Winter 2022

Healthcare Information Security Maturity Model Grande Ronde Hospital

Pallavi Agrawal
Portland State University

Riad Alharithi
Portland State University

Karthik Manjunath
Portland State University

Kamal Thapa
Portland State University

Eric Ingersoll
Portland State University

See next page for additional authors

Citation Details

Agrawal, Pallavi; Alharithi, Riad; Manjunath, Karthik; Thapa, Kamal; Ingersoll, Eric; and Rajagopal, Sujitha, "Healthcare Information Security Maturity Model Grande Ronde Hospital" (2022). *Engineering and Technology Management Student Projects*. 2322.
https://pdxscholar.library.pdx.edu/etm_studentprojects/2322

Authors
Pallavi Agrawal, Riad Alharithi, Karthik Manjunath, Kamal Thapa, Eric Ingersoll, and Sujitha Rajagopal

ETM
ENGINEERING & TECHNOLOGY MANAGEMENT

Healthcare Information Security Maturity Model
Grande Ronde Hospital

Course Title: Decision Making
Course Number: ETM 530
Instructor: Dr. Tugrul Daim
Term: Winter
Year: 2022
Author(s): Pallavi Agrawal, Riad Alharithi, Karthik Manjunath, Kamal Thapa, Eric Ingersoll, Sujitha Rajagopal

Introduction

Technology offers significant advantages in improving the delivery of healthcare to patients. The technology creates electronic data associated with each patient. The data journey starts from the collection point, through the data warehouses that store the data, the application that processes the data, and the medium that transfers the data throughout the patient's life.

Data collection starts with patients filling out web forms on a provider's website. This information is stored for the Healthcare organization in remote servers managed by developers and is shared with healthcare specialists, hospitals, labs, pharmacists, insurance providers, and billing software among many other healthcare workers.

Each of these players receives the data via the internet and stores it on their remote servers or internal computers.

Many regulations and laws are issued to improve the security of the data that is collected, transferred, and stored across these data users. Unlike reissuing a credit card or closing a bank account when compromised, patients' health records cannot be changed, and the data breach is permanent. Consequently, the security of the data while being collected, stored, and transferred is extremely important.

Patients will likely visit multiple healthcare facilities as they age. Each facility has its own cybersecurity system to meet the laws and regulations as a baseline. How do we assess the system's maturity to build a baseline of its conditions then prepare a roadmap to constantly improve the existing conditions based on the objectives set by the facilities' decision-makers?

This report used the Hierarchical Decision Model (HDM) method that Dr. Bridget Barnes developed to assess the information security maturity level of the Grande Ronde Hospital in La Grande, Oregon.

Literature review

"Cybersecurity in Science and Medicine: Threats and Challenges" by Luh and Yen [1] provided an overview of the risk types associated with genomic research, medical devices, and wearable technology. Any loss or breach of data not only causes financial harm but also reputational damage. Unlike a stolen credit card or lost driver's license, there is no replacement or 'start over' with one genomic identity [1, p. 825]. Cybersecurity in the healthcare industry has grown to an alarming stage. Between 2009 and 2019, there were more than 3000 healthcare data breaches, involving at least 500 patients' records in each occurrence. Cyberattacks involved all types of organizations: hospitals, clinics, insurance providers, etc. and the overall number of hacked medical records has been staggering [1, p. 826]. Cybersecurity has been involved with genomic research by preventing hacking of personal and genomic patient data from research institutions, and from medical devices such as intravenous infusion pumps and implantable cardiac pacemakers. Wearable technology and mobile health Apps have also been subject to hacking. Smartphones and Google Glass can be compromised through unsecured Wi-Fi, operating system flaws, and malicious Apps, collecting personal and health data from this wearable technology. Improving healthcare requires technology; but this same technology is subject to hacking and exposes the patients' data to organized hackers' activities. Consequently, it is imperative to improve the cybersecurity of all healthcare technologies listed above. This requires changes in the investment strategy of each healthcare organization. While financial institutions allocate 15% of their budget to cybersecurity, the healthcare industry allocates 4-7% of their budget [1, p. 827].

Evaluating the Security Impact of Healthcare Web Applications Through Fuzzy Based Hybrid Approach of Multi-Criteria Decision-Making Analysis by Agrawal et al. [2] discussed the threats associated with the web-based healthcare applications. It defined the model to evaluate these applications against security threats. The authors developed a multi-criteria decision methodology to perform that evaluation. The MCDM is an integrated hybrid model of Fuzzy Analytical Hierarchy Processes-Technique for Order of Preference by Similarity to Ideal Solution (Fuzzy AHP-TOPSIS). First, the authors solicited from 101 experts the factors that affect the development of the web-based application and, consequently, their vulnerability to cyberattacks. These factors are confidentiality, integrity, availability, scalability, interoperability, accountability, and accessibility [2].

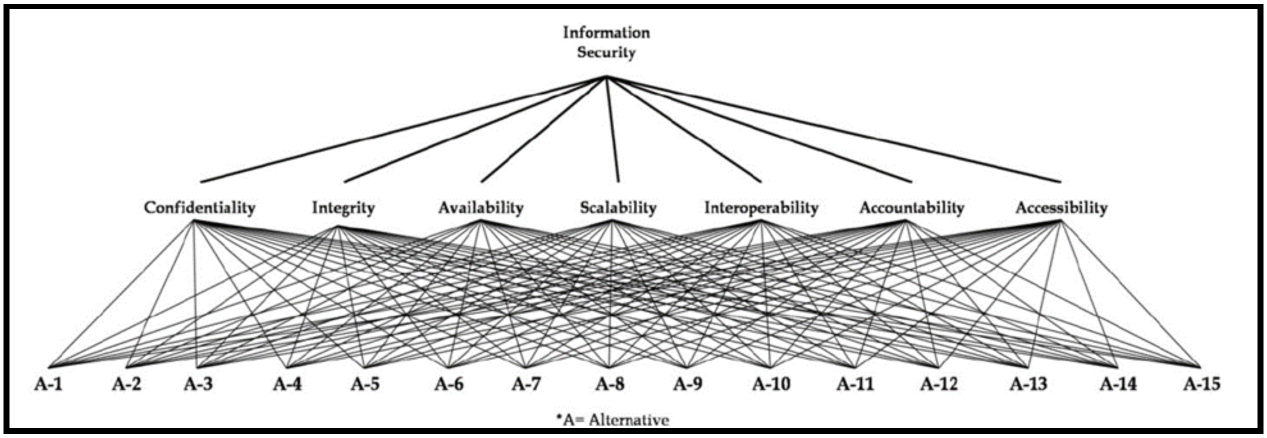


Figure 1: Criteria definitions of the Model

Authors performed analysis on these criteria to first focus on the most relevant factors that will assure high-end security and secondly would reduce both time and resources invested in analyzing and accurately evaluating the efficacy of the web application. The authors explained that AHP is the most effective method of the MCDM approaches. However, AHP does not account for the accountability factor; consequently, the fuzzy and AH with TOPSIS methodology is more effective in this scenario. Figure 2 shows the authors' model map and the introduction of the fuzzy factors in the model. The authors compared the classical AHP-TOPSIS and Fuzzy AHP-TOPSIS and showed the advancement of their model in evaluating the importance of integrity and accountability against cyber-attacks. In other words, when a developer and a healthcare organization focuses on these two factors in building the web application, they gain significant security against attacks [2].

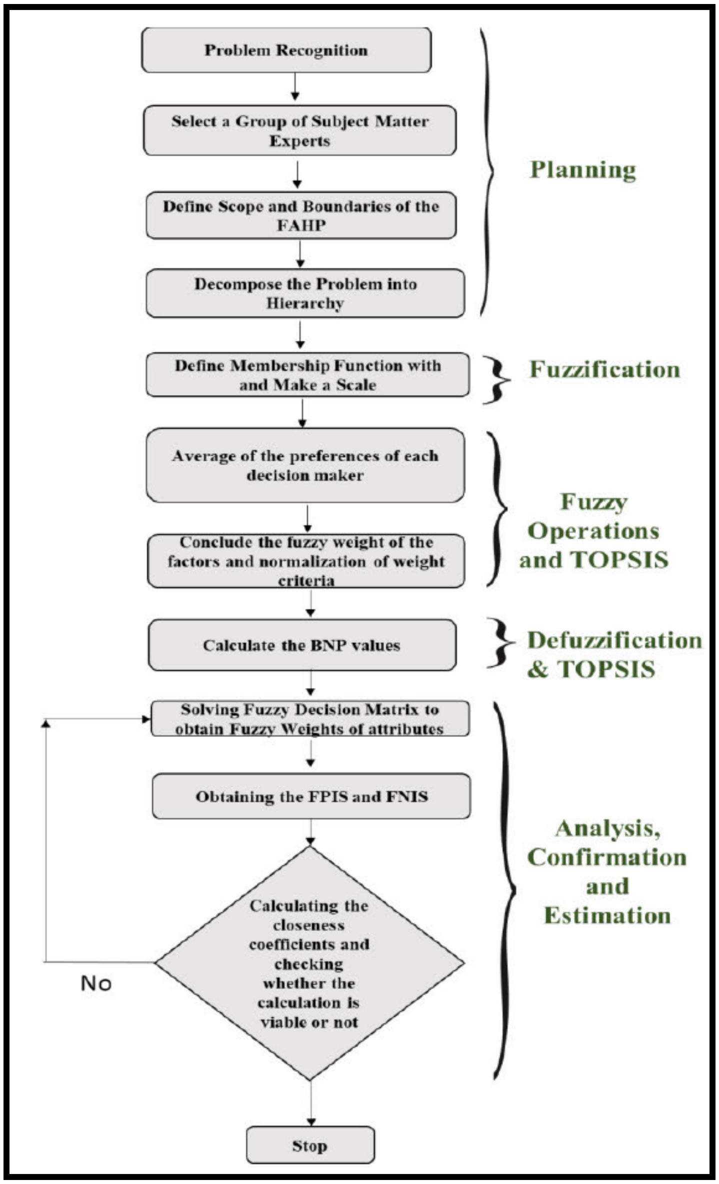

Problem Recognition
Select a Group of Subject Matter Experts
Define Scope and Boundaries of the FAHP
Decompose the Problem into Hierarchy
Planning
Define Membership Function with and Make a Scale
Fuzzification
Average of the preferences of each decision maker
Conclude the fuzzy weight of the factors and normalization of weight criteria
Fuzzy Operations and TOPSIS
Calculate the BNP values
Defuzzification & TOPSIS
Solving Fuzzy Decision Matrix to obtain Fuzzy Weights of attributes
Obtaining the FPIS and FNIS
Calculating the closeness coefficients and checking whether the calculation is viable or not
No
Analysis, Confirmation and Estimation
Stop

Figure 2: Methodology flow chart and the addition of the fuzzy steps in the process

Seh et al. [3] examined and investigated the trend of healthcare data breaches and their cost. According to the authors, the advent of the Internet of Medical Things, Smart Devices, Information Systems, and Cloud Services have led to a digital transformation of the healthcare industry. With this, digital healthcare services have paved the way for easier and more accessible treatment, thus making lives far more comfortable. However, the modern-day healthcare industry has also become the main target of data breach as data from the healthcare industry is regarded as being highly valuable. Unsurprisingly, the healthcare industry has faced the highest number of breaches among all industries which is represented by tables below [3]:

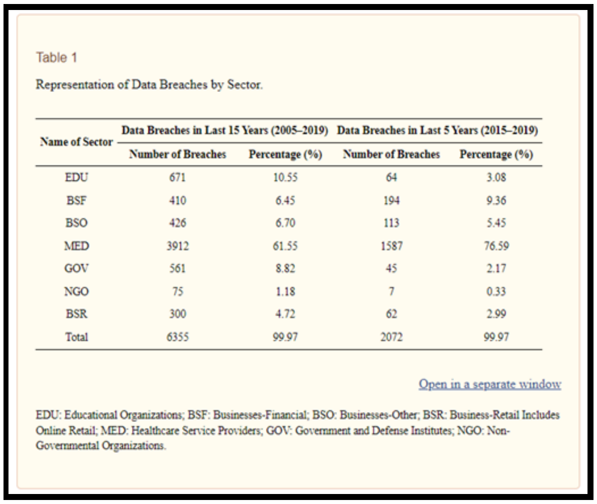


Table 1

Representation of Data Breaches by Sector.

Name of Sector	Data Breaches in Last 15 Years (2005–2019)		Data Breaches in Last 5 Years (2015–2019)	
	Number of Breaches	Percentage (%)	Number of Breaches	Percentage (%)
EDU	671	10.55	64	3.08
BSF	410	6.45	194	9.36
BSO	426	6.70	113	5.45
MED	3912	61.55	1587	76.59
GOV	561	8.82	45	2.17
NGO	75	1.18	7	0.33
BSR	300	4.72	62	2.99
Total	6355	99.97	2072	99.97

Open in a separate window

EDU: Educational Organizations; BSF: Businesses-Financial; BSO: Businesses-Other; BSR: Business-Retail Includes Online Retail; MED: Healthcare Service Providers; GOV: Government and Defense Institutes; NGO: Non-Governmental Organizations.

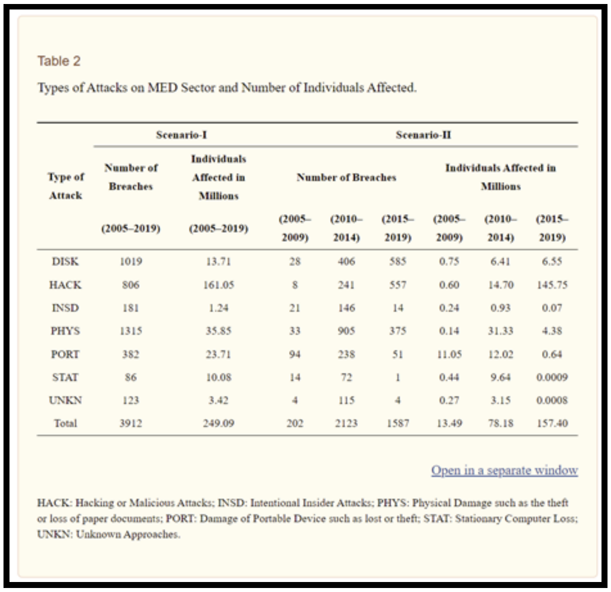


Table 2

Types of Attacks on MED Sector and Number of Individuals Affected.

Type of Attack	Scenario-I		Scenario-II					
	Number of Breaches	Individuals Affected in Millions	Number of Breaches			Individuals Affected in Millions		
	(2005–2019)	(2005–2019)	(2005–2009)	(2010–2014)	(2015–2019)	(2005–2009)	(2010–2014)	(2015–2019)
DISK	1019	13.71	28	406	585	0.75	6.41	6.55
HACK	806	161.05	8	241	557	0.60	14.70	145.75
INSD	181	1.24	21	146	14	0.24	0.93	0.07
PHYS	1315	35.85	33	905	375	0.14	31.33	4.38
PORT	382	23.71	94	238	51	11.05	12.02	0.64
STAT	86	10.08	14	72	1	0.44	9.64	0.0009
UNKN	123	3.42	4	115	4	0.27	3.15	0.0008
Total	3912	249.09	202	2123	1587	13.49	78.18	157.40

Open in a separate window

HACK: Hacking or Malicious Attacks; INSD: Intentional Insider Attacks; PHYS: Physical Damage such as the theft or loss of paper documents; PORT: Damage of Portable Device such as lost or theft; STAT: Stationary Computer Loss; UNKN: Unknown Approaches.

Key findings from Seh et al. can be summarized below:

- More than 10 billion records were exposed from different sectors from 2005 to 2019.
- There have been 3912 confirmed data breach cases in the healthcare sector alone. Nearly 43.38% of health data was compromised from 2005 to 2019, the highest among all sectors.
- As per HIPAA reports, 255.18 million were affected from 3051 healthcare data breach incidents from 2010 to 2019.
- The main types of attacks used to breach protected health data are Hacking/IT incidents, unauthorized access/ internal disclosure, Theft/loss, or Improper disposal.
- Hacking/IT incidents have increased by 73.4% in 2019 from 2018.
- Email and network servers are the most common places for confidential healthcare data breaches.
- In the healthcare industry at present, the average cost of data breach is $6.45 million, up from $3.92 million in 2019.

When private data is breached, it is impossible to restore privacy or reverse psychosocial harm because these records contain private data such as name, date of birth, insurance and health provider information, as well as health and genetic information. Dias et al. [4] carried out a comprehensive literature survey to investigate risk management focusing on identifying requirements and best practices for healthcare data security systems. The healthcare industry was thought to be immune to cyber-attacks, and protective measures were not taken into consideration in the past. In recent decades, this sector has focused its efforts on medical care, scrapping its devices to protect against cyber-attacks. As recent statistics show about 90 percent of health organizations have been victims of cybersecurity violations, this has highlighted the several factors that contributed to the sector becoming one of the main targets of cyber-attacks. Moreover, data shows that the healthcare industry in the United States experiences four data breaches in a week, making it the most vulnerable sector to digital security breaches [3][4][5]. Through a system literature review, they proposed to answer two questions: what are the minimum requirements, and what are the best risk management practices applied for a cybersecurity system in healthcare? While presenting five major research gaps, authors offered healthcare institutions parameters to be used in the fight against cybercrime, investigating risk management focused on identifying requirements and best practices for healthcare data security systems. If cybersecurity issues in healthcare institutions are not addressed promptly, the consequences might be disastrous and result in sociotechnical issues. Although there is no 100% effective approach to prevent system breaches by cybercriminals, cybersecurity should be a part of management procedures in healthcare organizations that strive for cyber resilience [4].

Gap Analysis

For any organization, especially healthcare organizations, gap analysis is a key part of performance management which is vital for delivering the highest quality care and outcomes.

Gap analysis is an iterative process as shown in the diagram below. It is important to perform a gap analysis to justify the necessity for the educational activity and to guide you to select the appropriate teaching and evaluation methods. Ultimately, this is the justification for why you are putting on this activity.

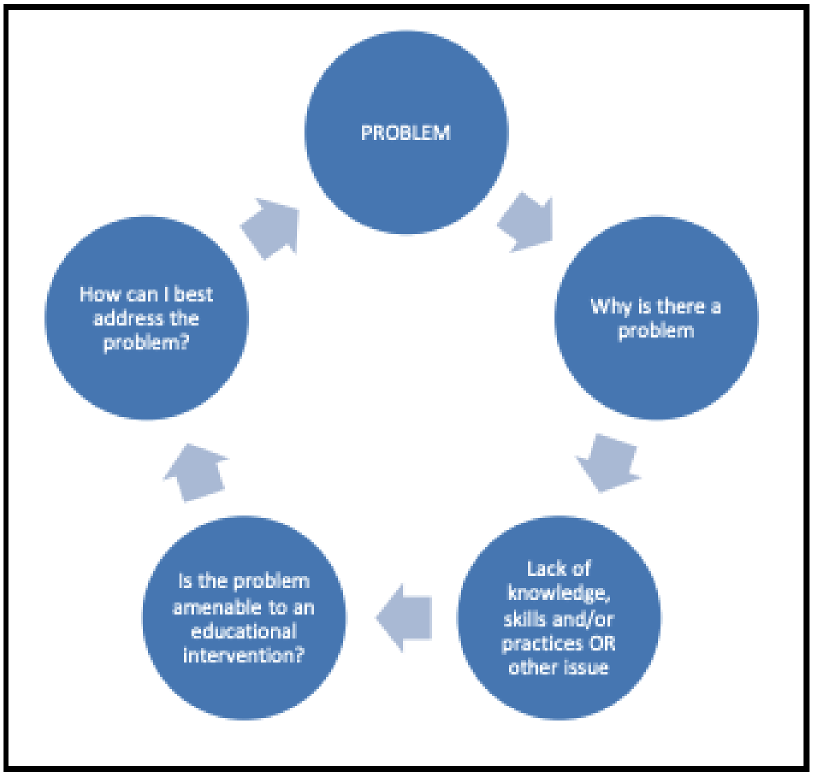

PROBLEM
Why is there a problem
Lack of knowledge, skills and/or practices OR other issue
Is the problem amenable to an educational intervention?
How can I best address the problem?

Figure 3: GAP analysis for healthcare industry

Based on our interviews with Parhez Sattar, the chief information officer at Grande Ronde hospital, Oregon we found these gaps in the organization:

Current state	Desired state	Identified Gap	Gap due to knowledge, skill and/or practice
The organization hosts limited (e.g. small groups) or inconsistent security awareness events.	The organization hosts regular security awareness events that are well attended by small groups of organizational members.	Not enough awareness is being spread across the organization in terms of the potential and news security threats	The lack of practice is the main reason since most of the core technical team follows this process internally
The organization has some documentation related to information security procedures.	The organization has well documented procedures related to information security and practiced among major technical teams	Lack of practice seems to be a major Gap here. Since policies and standards are followed through legacy rather than referring to it.	Practice as well as lack of Knowledge of the existence seems to play important roles for this Gap.
The organization has some tools, process or staffing to support limited asset management	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).	Lack of dedicated resources to manage these Physical and virtual assets	Lacks the Skill needed to maintain these resources which can be mitigated by adding more resources and knowledge sharing.

Table 3- GAP analysis for Grand Ronde Hospital

Key points:

- Limited awareness of security events across organizations. The desired state is to be at a stage where everyone is aware of the events and attends based on their interests. The gap here is the lack of practice.
- Documentation and information security procedures are mostly word of mouth. Desired state would be to have most of it documented and well maintained and make it available to organization personnel. Part of the reason for this is the lack of knowledge of these documents being in existence
- Asset management is another gap we found. The desired state is for us to have the organization with comprehensive tools, processes and staffing to support full life cycle management related to all physical and virtual technology assets (hardware and software).The gap is the lack of dedicated resources in this case.

Research Approach

Implementing and maintaining high-functioning information security infrastructures is becoming increasingly difficult for healthcare businesses. Threats to information security continue to exist. Increasing the focus on information security is important. Given the growing investment in information security by healthcare organizations, decision support systems that clearly describe the strategies that will have the greatest influence on improving performance will enable objective and transparent decision making.

The objective of this research is to evaluate the information security maturity assessment at Grande Ronde hospital. The validation and testing of the HDM model as part of the case study was our primary focus which aids organizations in the development of strategic, practical, and effective information security behaviors. In this way, Healthcare organizations can benefit not just from the findings of a single assessment, but also from the experiences of others in similar or different organizations that are dealing with similar information security issues.

This research includes the following steps:

1. Examine strategic decisions a multi-criteria decision-making process that are being applied
2. Break down complex problem into key components
3. Obtain expert viewpoints in order to make decisions. In this case, the Healthcare Information Security Maturity Model(HISMM) interview tool assessment at Grande Ronde hospital
4. Results are validated using sensitivity, disagreement, and inconsistency analysis

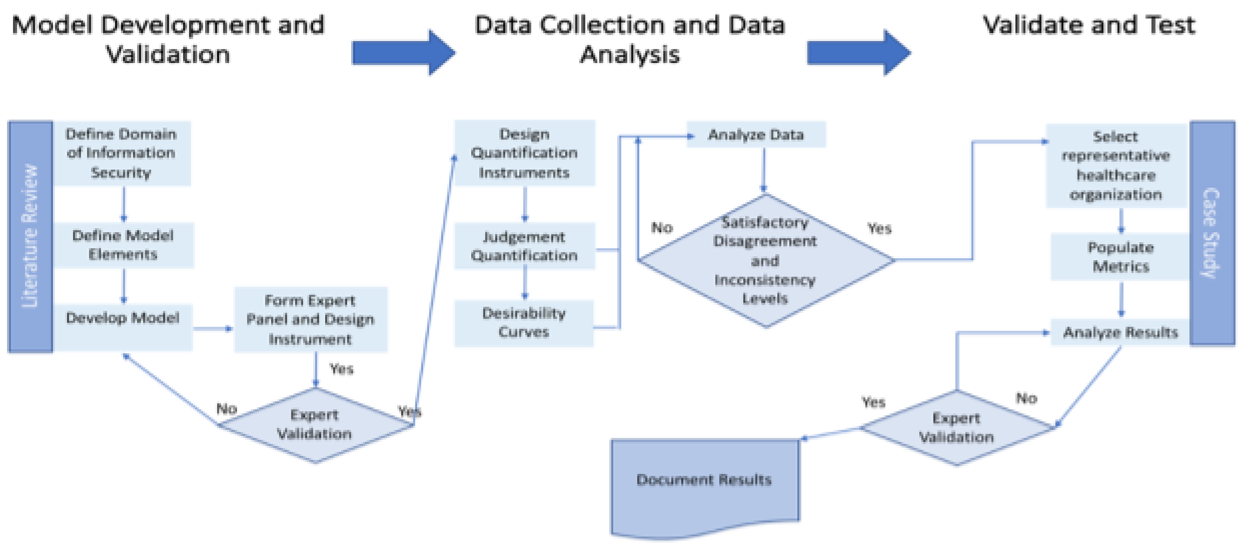
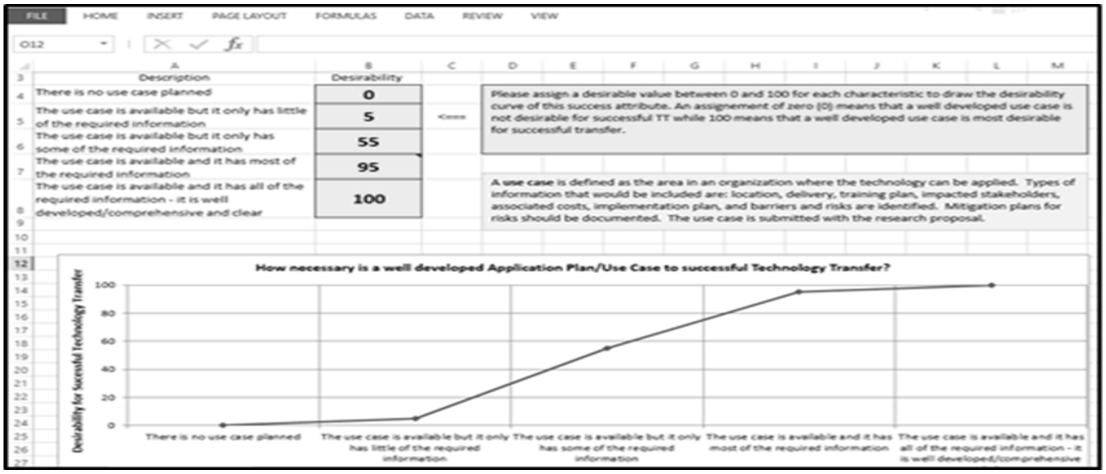

Model Development and Validation
Data Collection and Data Analysis
Validate and Test
Literature Review
Define Domain of Information Security
Define Model Elements
Develop Model
Form Expert Panel and Design Instrument
Yes
No
Expert Validation
Yes
Design Quantification Instruments
Judgement Quantification
Desirability Curves
Analyze Data
No
Satisfactory Disagreement and Inconsistency Levels
Yes
Select representative healthcare organization
Populate Metrics
Analyze Results
Case Study
Yes
No
Expert Validation
Document Results

Figure 4: Research steps- Flowchart

Research steps are represented in this flowchart. The steps include Model Development and Validation, Data collection and Data Analysis, Validate & Test and Finally producing the Document Results.

For each element in the HDM model, the expert feedback was translated into a Desirability Curve, resulting in a scale of relative importance for each criterion/goal. It is a method for translating qualitative or quantitative data for a model element to a scaled numerical value. This allows experts to normalize findings across all model elements. When HDM is combined with desirability curves, decision-makers can better understand the tools and techniques that can be utilized to improve the maturity of the information security environment.


FILE
HOME
INSERT
PAGE LAYOUT
FORMULAS
DATA
REVIEW
VIEW
O12
fx
<===
How necessary is a well developed Application Plan/Use Case to successful Technology Transfer?
Desirability for Successful Technology Transfer
100
80
60
40
20
0
There is no use case planned
The use case is available but it only has little of the required information
The use case is available but it only has some of the required information
The use case is available and it has most of the required information
The use case is available and it has all of the required information - it is well developed/comprehensive

Description	Desirability
There is no use case planned	0
The use case is available but it only has little of the required information	5
The use case is available but it only has some of the required information	55
The use case is available and it has most of the required information	95
The use case is available and it has all of the required information - it is well developed/comprehensive and clear	100

Please assign a desirable value between 0 and 100 for each characteristic to draw the desirability curve of this success attribute. An assignement of zero (0) means that a well developed use case is not desirable for successful TT while 100 means that a well developed use case is most desirable for successful transfer.

A **use case** is defined as the area in an organization where the technology can be applied. Types of information that would be included are: location, delivery, training plan, impacted stakeholders, associated costs, implementation plan, and barriers and risks are identified. Mitigation plans for risks should be documented. The use case is submitted with the research proposal.

Figure 5: Eg.,Desirability Curve

MCDM and HDM

The hierarchical decision model (HDM) is built on the concept that decisions are based on criteria that must be weighted according to their importance to the organization’s mission and goals. The model is presented in the following hierarchy: mission, objectives, goals, strategies, and action (MOGSA).

Typically, decisions must be made to choose from specific alternatives presented to the organization's leadership. Generally, this begins by having management review the criteria which is then validated by experts who also provide opinions on the criteria to get a weight, then a mathematical model is run to provide the recommendations. Attention should be given to the evaluation of the criteria method. In this case, the criteria are placed in pairs, and one criterion is evaluated against the other to determine its value: this is known as a pair-wise comparison. HDM results include disagreement, inconsistency, and sensitivity to validate the reliability of the final model. The alternatives that the leaders need to decide on is whether to use cloud computing or non-cloud computing.

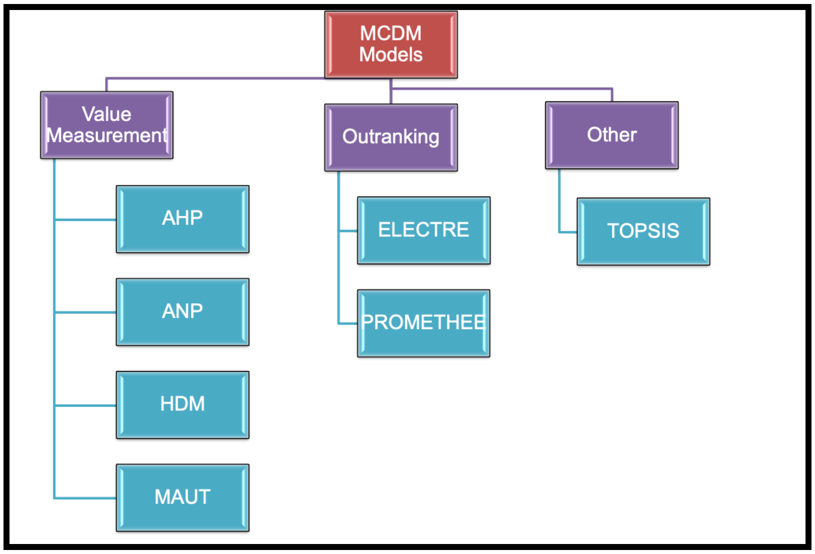


Figure 6: MCDM Classification

Why HDM?

HDM proves to be a reasonable tool for prediction outcomes as it provides the following advantages to both decision-makers and the subject matter experts.

For Decision-makers:

- Provides Comprehensive Abstraction of a problem under considerations
- Illustrates multi-level relationships among elements of the model
- Aggregates the opinions in an easy to digest way for decision-makers
- Structures both qualitative and quantitative data in a single view
- Allows variability of value for each criterion within the model

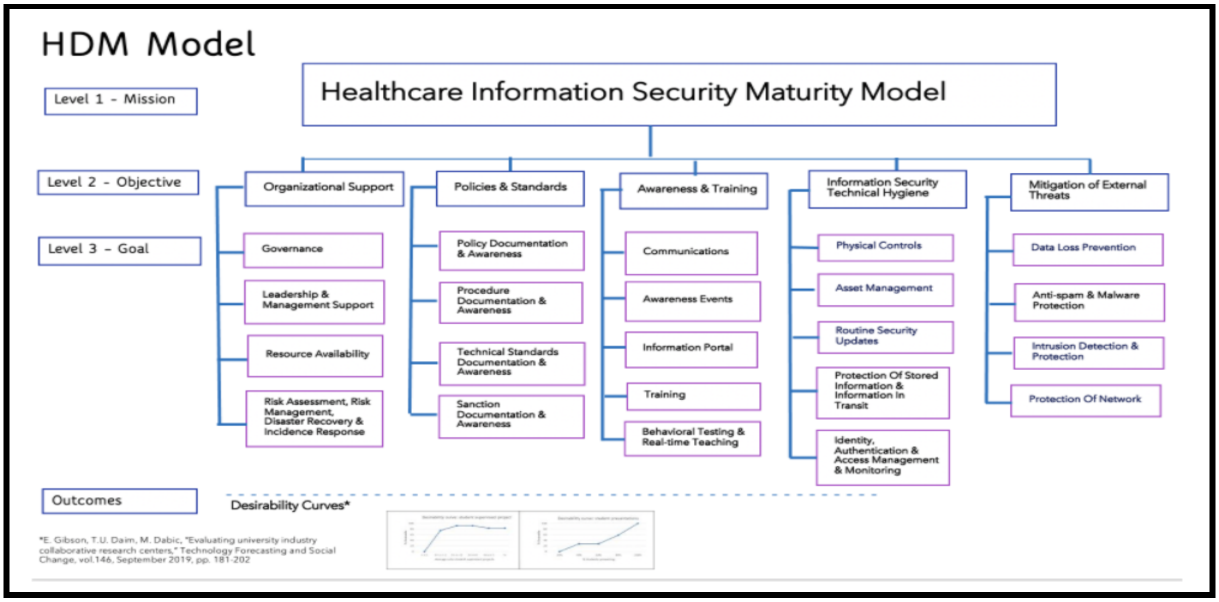
For Experts

- Allows experts to express a 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 level of effort level

HDM Model for Grande Ronde Hospital

The overall anatomy of the model that developed by Dr. Barnes and which we used:

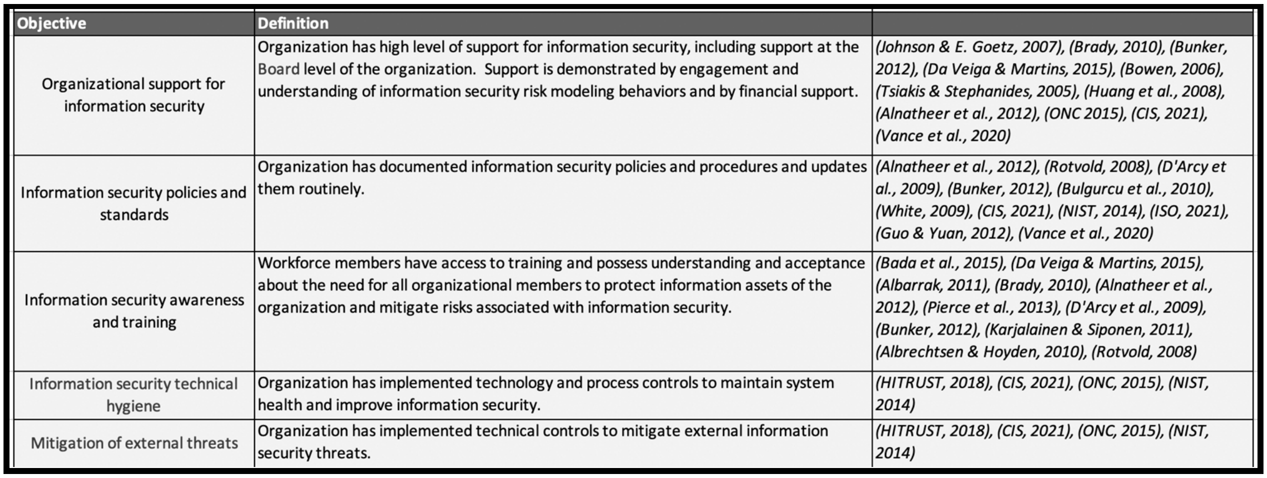
- Mission: Assess the maturity level of the Security framework that is being implemented at the hospital
- Objectives: are derived from cybersecurity literature survey and validated by cybersecurity experts
- Measurable Goals are the basic blocks that construct each objective
- Outcomes: a number that describes the current status of the existing framework maturity


HDM Model
Level 1 - Mission
Healthcare Information Security Maturity Model
Level 2 - Objective
Level 3 - Goal
Organizational Support
Policies & Standards
Awareness & Training
Information Security Technical Hygiene
Mitigation of External Threats
Governance
Leadership & Management Support
Resource Availability
Risk Assessment, Risk Management, Disaster Recovery & Incidence Response
Policy Documentation & Awareness
Procedure Documentation & Awareness
Technical Standards Documentation & Awareness
Sanction Documentation & Awareness
Communications
Awareness Events
Information Portal
Training
Behavioral Testing & Real-time Teaching
Physical Controls
Asset Management
Routine Security Updates
Protection Of Stored Information & Information In Transit
Identity, Authentication & Access Management & Monitoring
Data Loss Prevention
Anti-spam & Malware Protection
Intrusion Detection & Protection
Protection Of Network
Outcomes
Desirability Curves*

*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

Figure 7: HDM Model

The objectives of the model are:



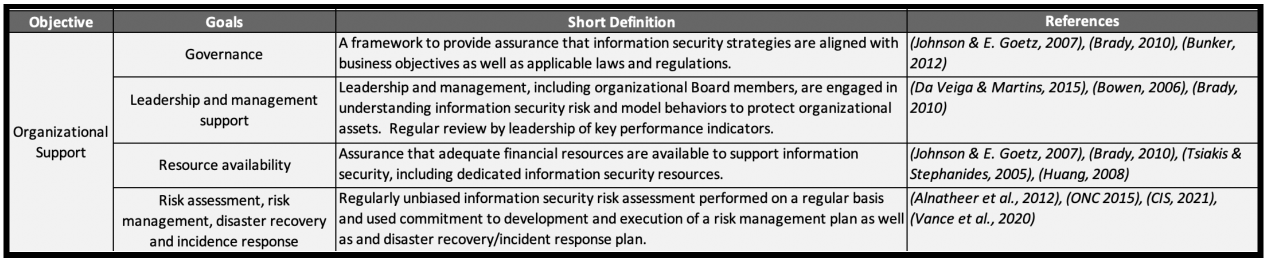
Objective	Definition	
Organizational support for information security	Organization has high level of support for information security, including support at the Board level of the organization. Support is demonstrated by engagement and understanding of information security risk modeling behaviors and by financial support.	*(Johnson & E. Goetz, 2007), (Brady, 2010), (Bunker, 2012), (Da Veiga & Martins, 2015), (Bowen, 2006), (Tsiakis & Stephanides, 2005), (Huang et al., 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 et al., 2010), (White, 2009), (CIS, 2021), (NIST, 2014), (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), (Albarrak, 2011), (Brady, 2010), (Alnatheer et al., 2012), (Pierce et al., 2013), (D'Arcy et al., 2009), (Bunker, 2012), (Karjalainen & Siponen, 2011), (Albrechtsen & Hoyden, 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, 2014)*
Mitigation of external threats	Organization has implemented technical controls to mitigate external information security threats.	*(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2014)*

Figure 8: Model objectives

- Organization support: includes Board and leadership level support to the cybersecurity unit of the Information Technology Department by providing funds to the program.
- Policies and Standards: documented policies and standards in place and the effort to keep them updated and accessible to all staff at all levels.
- Awareness and training: training program in place, especially for the new hires.
- Information security and technical hygiene: security system in place that prevents accidental or intentional exposure of information to outsiders, and system maintenance to minimize exposure to security risks.
- Mitigation of external factors: having an in-place system to prevent security breaches and hacking such as malware protection and anti-spam applications.

HDM Model - Objective Definitions

Organizational Support:



Objective	Goals	Short Definition	References
Organizational Support	Governance	A framework to provide assurance that information security strategies are aligned with business objectives as well as applicable laws and regulations.	*(Johnson & E. Goetz, 2007), (Brady, 2010), (Bunker, 2012)*
	Leadership and management support	Leadership and management, including organizational Board members, are engaged in understanding information security risk and model behaviors to protect organizational assets. Regular review by leadership of key performance indicators.	*(Da Veiga & Martins, 2015), (Bowen, 2006), (Brady, 2010)*
	Resource availability	Assurance that adequate financial resources are available to support information security, including dedicated information security resources.	*(Johnson & E. Goetz, 2007), (Brady, 2010), (Tsiakis & Stephanides, 2005), (Huang, 2008)*
	Risk assessment, risk management, disaster recovery and incidence response	Regularly unbiased information security risk assessment performed on a regular basis and used commitment to development and execution of a risk management plan as well as and disaster recovery/incident response plan.	*(Alnatheer et al., 2012), (ONC 2015), (CIS, 2021), (Vance et al., 2020)*

Figure 9: Organizational support

Grande Ronde hospital had the following responses in regards to Governance, Leadership and management support, Resource availability and Risk assessment, risk management plan, and disaster recovery and incident response.

Governance

The organization has well established information security governance which includes routine monitoring and measurement of performance associated with a defined strategic plan.

Leadership and management support

The organizational leaders participate actively in the information security governance process, policies, and procedures, ensuring that they are aligned with business goals.

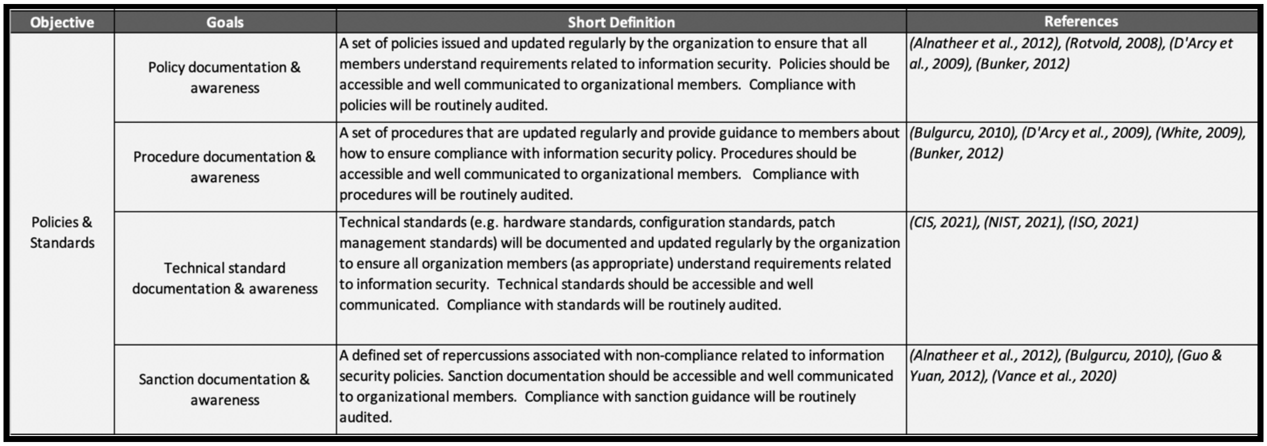
Resource availability

The organization has a dedicated information security team for providing training every month for new employees, every quarter all employees training and weekly Phishing expeditions

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

The organization conducts risk assessments once a year and has developed a risk management plan.
However, organization-wide planning is required and it is not yet accomplished.

Policies and Standards



Objective	Goals	Short Definition	References
Policies & Standards	Policy documentation & awareness	A set of policies issued and updated regularly by the organization to ensure that all members understand requirements related to information security. Policies should be accessible and well communicated to organizational members. Compliance with policies will be routinely audited.	*(Alnatheer et al., 2012), (Rotvold, 2008), (D'Arcy et al., 2009), (Bunker, 2012)*
	Procedure documentation & awareness	A set of procedures that are updated regularly and provide guidance to members about how to ensure compliance with information security policy. Procedures should be accessible and well communicated to organizational members. Compliance with procedures will be routinely audited.	*(Bulgurcu, 2010), (D'Arcy et al., 2009), (White, 2009), (Bunker, 2012)*
	Technical standard documentation & awareness	Technical standards (e.g. hardware standards, configuration standards, patch management standards) will 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.	*(CIS, 2021), (NIST, 2021), (ISO, 2021)*
	Sanction documentation & awareness	A defined set of repercussions associated with non-compliance related to information security policies. Sanction documentation should be accessible and well communicated to organizational members. Compliance with sanction guidance will be routinely audited.	*(Alnatheer et al., 2012), (Bulgurcu, 2010), (Guo & Yuan, 2012), (Vance et al., 2020)*

Figure 10: Policies and standards

Grande Ronde's responses were:

Policy documentation and awareness

The organization has well documented policies related to information security but they are not well known to organizational members.

Procedure documentation and awareness

The organization has good documentation related to non-security documents but still lacks security related documents. Their procedures are mostly word-of-mouth and well handled.

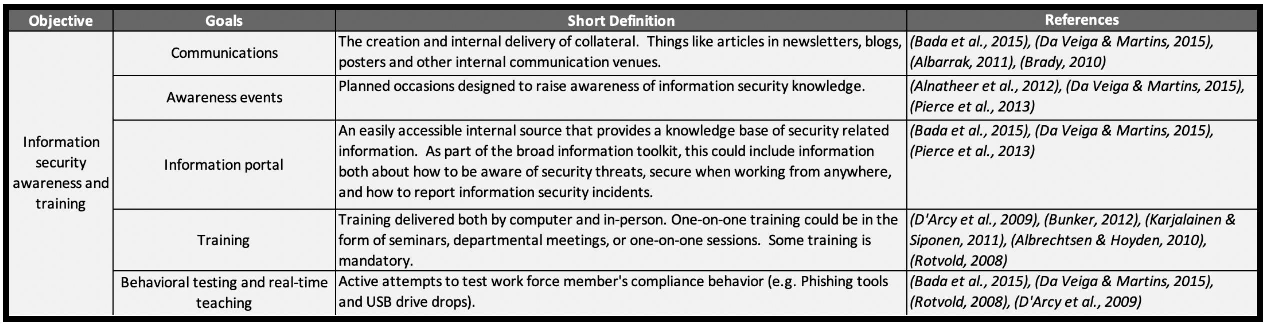
Technical standard documentation and awareness

The organization has some documentation related to their information security technical standard but hoping to be well documented in the future.

Sanction documentation and awareness

The organization has decent documentation which is followed, but could improve.

Information Security Awareness and Training



Objective	Goals	Short Definition	References
Information security awareness and training	Communications	The creation and internal delivery of collateral. Things like articles in newsletters, blogs, posters and other internal communication venues.	*(Bada et al., 2015), (Da Veiga & Martins, 2015), (Albarrak, 2011), (Brady, 2010)*
	Awareness events	Planned occasions designed to raise awareness of information security knowledge.	*(Alnatheer et al., 2012), (Da Veiga & Martins, 2015), (Pierce et al., 2013)*
	Information portal	An easily accessible internal source that provides a knowledge base of security related information. As part of the broad information toolkit, this could include information both about how to be aware of security threats, secure when working from anywhere, and how to report information security incidents.	*(Bada et al., 2015), (Da Veiga & Martins, 2015), (Pierce et al., 2013)*
	Training	Training delivered both by computer and in-person. One-on-one training could be in the form of seminars, departmental meetings, or one-on-one sessions. Some training is mandatory.	*(D'Arcy et al., 2009), (Bunker, 2012), (Karjalainen & Siponen, 2011), (Albrechtsen & Hoyden, 2010), (Rotvold, 2008)*
	Behavioral testing and real-time teaching	Active attempts to test work force member's compliance behavior (e.g. Phishing tools and USB drive drops).	*(Bada et al., 2015), (Da Veiga & Martins, 2015), (Rotvold, 2008), (D'Arcy et al., 2009)*

Figure 11: Information Security Awareness and Training

Grande Ronde's responses were:

Communications
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.

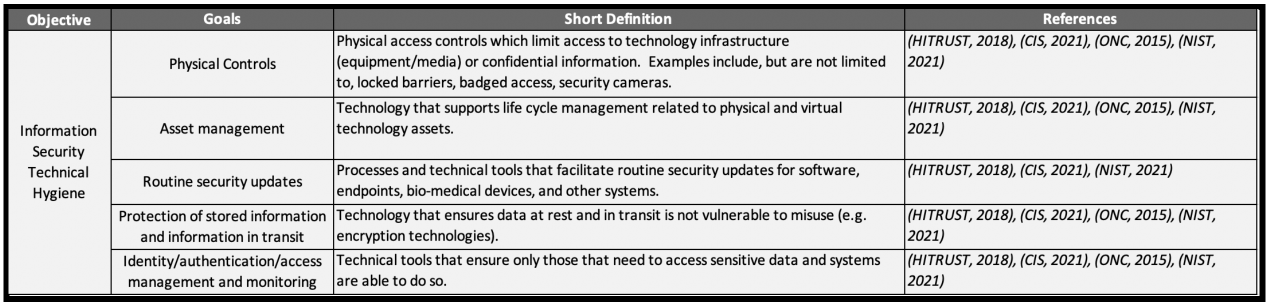
Awareness events
The organization hosts limited (e.g. small groups) or inconsistent security awareness events.

Information portal
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. Most of the time they get calls to the front office to get things done.

Training
The organization provides security training and 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
The organization regularly and frequently tests members compliance with information security policies, procedures, and best practices. Tests are conducted through a variety of delivery mechanisms (e.g. phishing tests, USB drop, Pen testing and social engineering). Results of individual tests are shared with individual organizational members privately to avoid shaming and encourage learning. Organizational members who repeatedly fail behavioral tests are offered personal coaching.

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)*

Figure 12: Information Security Technical Hygiene

Grande Ronde's responses were:

Physical Controls
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. They have all physical controls needed for maintaining a high level of security.

Asset Management

The level of asset management for physical and virtual technology assets is established at the organization. Their organization has some tools, processes or staffing to support limited asset management capabilities for physical and virtual technology assets (hardware and software). Pahrez highlighted that they have the tools and processes identified but they don't have enough dedicated resources yet.

Routine security updates

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, and bio-medical devices. They have a lot of biomedical devices which can't be updated based on FDA notice. Non-medical devices do get maintained regularly but some are owned by vendors and need to wait until they get the updates from them. We had a follow up question on his response that during covid, were the security alerts/updates maintained. He mentioned that for bio equipment, there are no new releases. They have most of their devices from Philips and GE, and at least they didn't have any updates. Vendors have to get permissions and verified before patching.

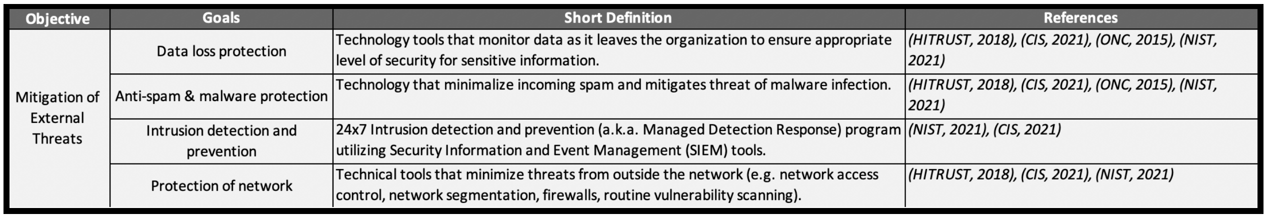
Protection of Stored Information and Information in Transit

The organization has comprehensive tools to support stored information and information in transit for applications and systems that are on-premise. They are not yet associated with cloud computing platforms.

Identity/Authentication/Access Management and Monitoring

The organization is between having some tools to support identity, authentication and access management capabilities, and having 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. Since it's a mix of both cloud and non-cloud access control mechanisms being used, the organization was listed as having "some tools" and not "all comprehensive tools".

Mitigation of External Threats



Objective	Goals	Short Definition	References
Mitigation of External Threats	Data loss protection	Technology tools that monitor data as it leaves the organization to ensure appropriate level of security for sensitive information.	*(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)*
	Anti-spam & malware protection	Technology that minimalize incoming spam and mitigates threat of malware infection.	*(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)*
	Intrusion detection and prevention	24x7 Intrusion detection and prevention (a.k.a. Managed Detection Response) program utilizing Security Information and Event Management (SIEM) tools.	*(NIST, 2021), (CIS, 2021)*
	Protection of network	Technical tools that minimize threats from outside the network (e.g. network access control, network segmentation, firewalls, routine vulnerability scanning).	*(HITRUST, 2018), (CIS, 2021), (NIST, 2021)*

Figure 13: Mitigation of External Threats

Grande Ronde's responses were:

Data Loss Protection

The organization has comprehensive tools to support data loss protection for applications and on-premise systems. There is currently no monitoring for Cloud systems, but has been identified as a goal. They have backup monitoring as well as email backups.

Anti-spam and malware protection

The organization has some tools to support both anti-spam and malware protection capabilities. On-premises systems are well maintained but cloud solutions are maintained by vendors.

Intrusion detection and prevention

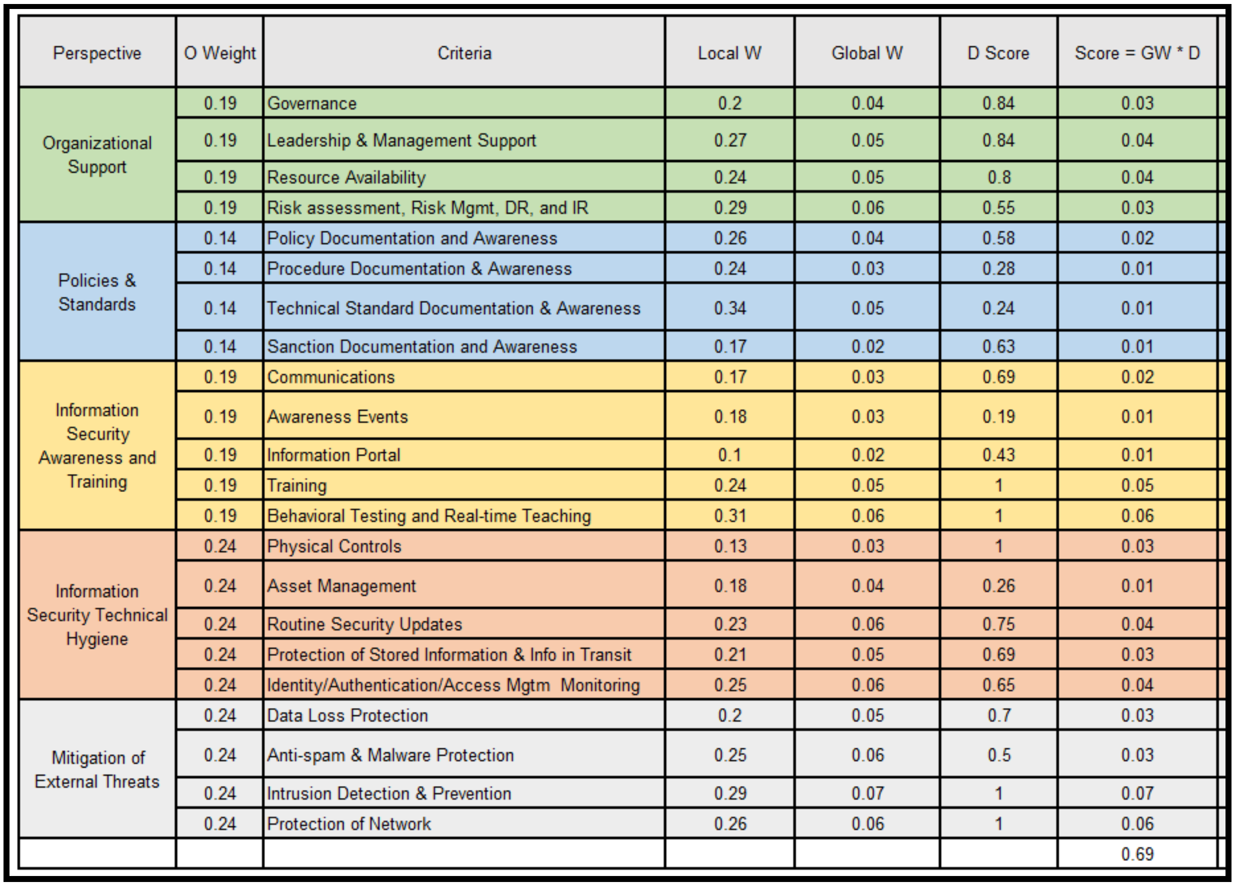
The organization has comprehensive tools and staffing to support 24x7 Intrusion detection and prevention via Managed Detection Response system utilizing a Security Information and Event Management system.

Protection of network

The organization has comprehensive tools which are actively monitored by information security professionals to support protection of the network. Remote monitoring and firewalls are in place and they have segmented networks combined with 24/7 active monitoring.

Quantification of HDM Model - Results

Based on our discussion with Parhez Sattar, CIO at Grande Ronde Hospital, we came up with the D-score, which determines the current level of maturity, and the overall score for each objective. We had the local weight and the objective weight determined for each criterion from Dr. Barnes dissertation, which gave us the Global weight. And further we calculated the D-score and overall score. The analysis of the D-score helped us determine the strong and weak areas of the organization.

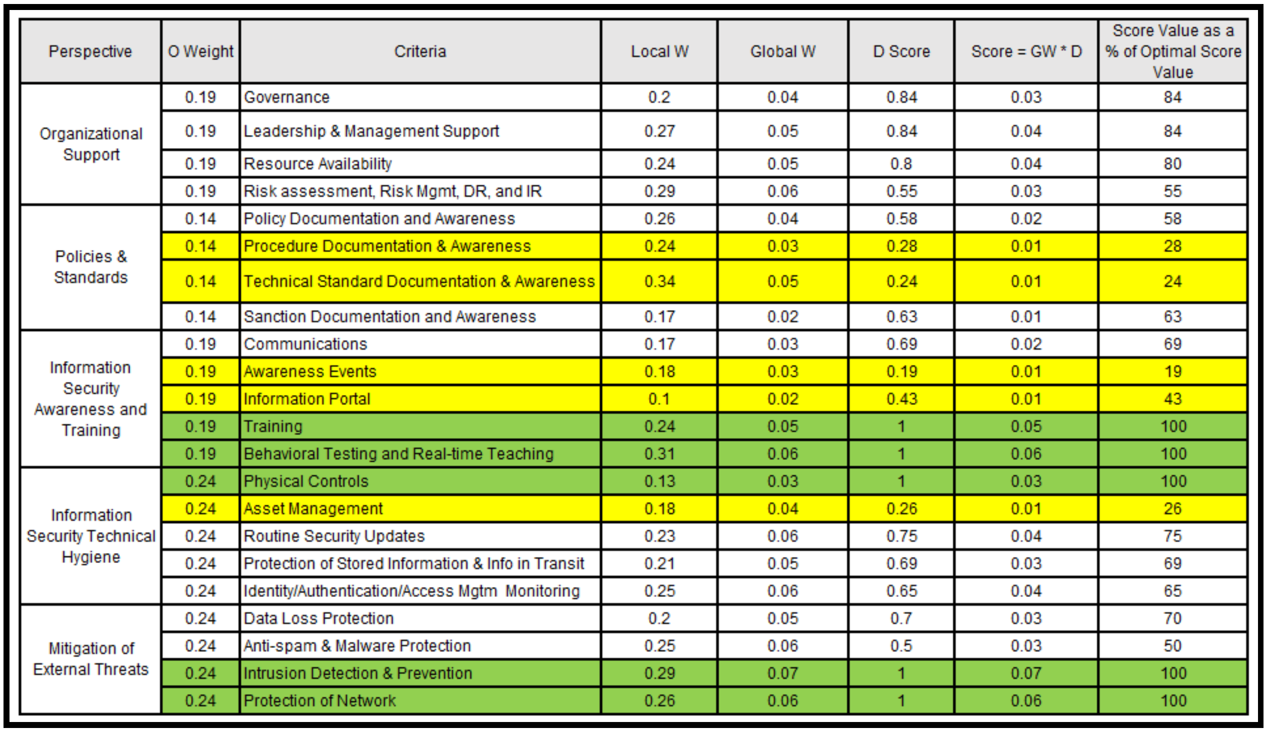


Perspective	O Weight	Criteria	Local W	Global W	D Score	Score = GW * D
Organizational Support	0.19	Governance	0.2	0.04	0.84	0.03
	0.19	Leadership & Management Support	0.27	0.05	0.84	0.04
	0.19	Resource Availability	0.24	0.05	0.8	0.04
	0.19	Risk assessment, Risk Mgmt, DR, and IR	0.29	0.06	0.55	0.03
Policies & Standards	0.14	Policy Documentation and Awareness	0.26	0.04	0.58	0.02
	0.14	Procedure Documentation & Awareness	0.24	0.03	0.28	0.01
	0.14	Technical Standard Documentation & Awareness	0.34	0.05	0.24	0.01
	0.14	Sanction Documentation and Awareness	0.17	0.02	0.63	0.01
Information Security Awareness and Training	0.19	Communications	0.17	0.03	0.69	0.02
	0.19	Awareness Events	0.18	0.03	0.19	0.01
	0.19	Information Portal	0.1	0.02	0.43	0.01
	0.19	Training	0.24	0.05	1	0.05
	0.19	Behavioral Testing and Real-time Teaching	0.31	0.06	1	0.06
Information Security Technical Hygiene	0.24	Physical Controls	0.13	0.03	1	0.03
	0.24	Asset Management	0.18	0.04	0.26	0.01
	0.24	Routine Security Updates	0.23	0.06	0.75	0.04
	0.24	Protection of Stored Information & Info in Transit	0.21	0.05	0.69	0.03
	0.24	Identity/Authentication/Access Mgtm Monitoring	0.25	0.06	0.65	0.04
Mitigation of External Threats	0.24	Data Loss Protection	0.2	0.05	0.7	0.03
	0.24	Anti-spam & Malware Protection	0.25	0.06	0.5	0.03
	0.24	Intrusion Detection & Prevention	0.29	0.07	1	0.07
	0.24	Protection of Network	0.26	0.06	1	0.06
						0.69

Table 4 - D-score calculation for Grand Ronde

The Total Maturity Score for Grande Ronde Hospital came out to be 0.69 which means that the company is 69% mature in their information security and there is little scope for improvement (The expected Optimal Maturity model score is 1.0). Our main criterion for ranking was the availability of resources for the desired goal. So we can conclude that the site least likely to have sufficient resources has the lowest score, and the site most likely to have sufficient resources has the highest score. This analysis was mainly based on expert feedback from Parhez Sattar at Grande Ronde Hospital for results reflecting Assessment of Current Maturity Level. There is still opportunity for further research, which we will discuss in the next section.

HDM Model- GRH, Strengths & Opportunities



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	0.2	0.04	0.84	0.03	84
	0.19	Leadership & Management Support	0.27	0.05	0.84	0.04	84
	0.19	Resource Availability	0.24	0.05	0.8	0.04	80
	0.19	Risk assessment, Risk Mgmt, DR, and IR	0.29	0.06	0.55	0.03	55
Policies & Standards	0.14	Policy Documentation and Awareness	0.26	0.04	0.58	0.02	58
	0.14	Procedure Documentation & Awareness	0.24	0.03	0.28	0.01	28
	0.14	Technical Standard Documentation & Awareness	0.34	0.05	0.24	0.01	24
	0.14	Sanction Documentation and Awareness	0.17	0.02	0.63	0.01	63
Information Security Awareness and Training	0.19	Communications	0.17	0.03	0.69	0.02	69
	0.19	Awareness Events	0.18	0.03	0.19	0.01	19
	0.19	Information Portal	0.1	0.02	0.43	0.01	43
	0.19	Training	0.24	0.05	1	0.05	100
	0.19	Behavioral Testing and Real-time Teaching	0.31	0.06	1	0.06	100
Information Security Technical Hygiene	0.24	Physical Controls	0.13	0.03	1	0.03	100
	0.24	Asset Management	0.18	0.04	0.26	0.01	26
	0.24	Routine Security Updates	0.23	0.06	0.75	0.04	75
	0.24	Protection of Stored Information & Info in Transit	0.21	0.05	0.69	0.03	69
	0.24	Identity/Authentication/Access Mgtm Monitoring	0.25	0.06	0.65	0.04	65
Mitigation of External Threats	0.24	Data Loss Protection	0.2	0.05	0.7	0.03	70
	0.24	Anti-spam & Malware Protection	0.25	0.06	0.5	0.03	50
	0.24	Intrusion Detection & Prevention	0.29	0.07	1	0.07	100
	0.24	Protection of Network	0.26	0.06	1	0.06	100

Table 5 - GRH Strengths and Opportunities

Strengths

Based on our Analysis using Dr. Barnes' HDM model we have identified top 5 strengths and areas of opportunities to manage the technologies and resources better. Top 5 strengths for Grande Ronde hospital which they should maintain are:

1. **Training** - Great training alignment within the technology department. In person presentations are well organized and targeted training for different departments happens frequently. Ad-hoc training is in place as well to educate individuals who need to upgrade their skills.
2. **Behavioral Testing & Real-time Teaching** - Highlights of the training program include, but are not limited to, a no shaming policy and people who need help are provided one-on-one training they require. Different types of testing is in-place to assess behavioral testing and real-time teaching, such as USB drops, pen testing, phishing, and social engineering.
3. **Physical Controls** - Grande Ronde Hospital has taken all physical measures to protect information and sensitive data within the organization by having dedicated resources to protect the premises.
4. **Intrusion Detection & Prevention** - They have MDR implemented and monitored 24/7.
5. **Protection of Network** - Remotely monitored networks and firewalls are in place. utilization of network segments streamlines problem identification and resolution.

Opportunities

Moving to opportunities for improvement, it is shown that Grande Ronde Hospital does not seem to score well in the following areas:

1. **Procedure Documentation and Awareness:** Grande Ronde has good documentation related to non-security documents, but lacks documents related to information security procedures instead opting for word of mouth dissemination of information, and therefore receives a 27.75% maturity level as illustrated in the desirability curve below. Unsurprisingly, there is a lot of room for improvement. In order to get fully matured on this criterion, they will need to have a comprehensive set of information security procedures which are regularly updated and well understood by members of the organization.

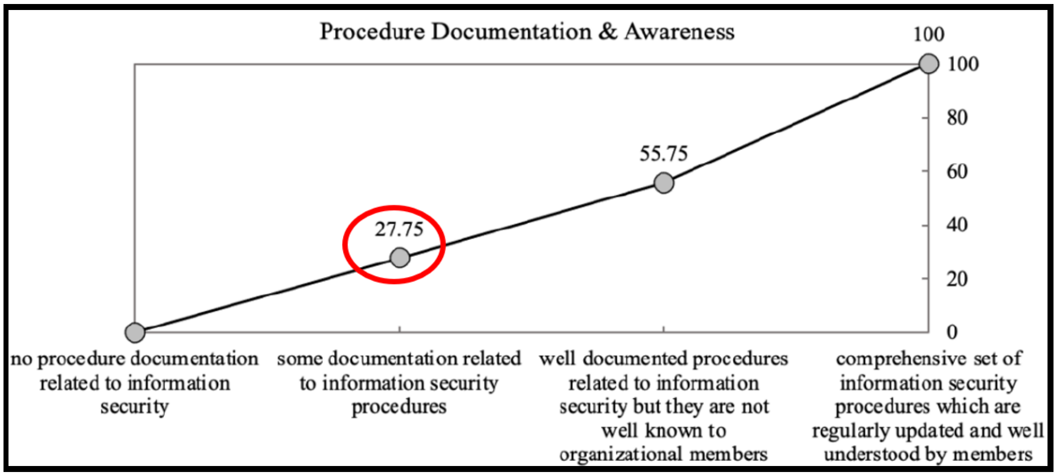


Figure 14: Procedure Documentation & Awareness

2. **Technical Standards Documentation & Awareness:** Grande Ronde has some documentation related to information security technical standards however, a majority are left undocumented. The desirability curve for this metric shows a maturity level of 23.75% which is still at its fledgling stage. For full maturity in this criterion, they should have a comprehensive set of information security technical standards which are regularly updated and well understood by the members of this organization.

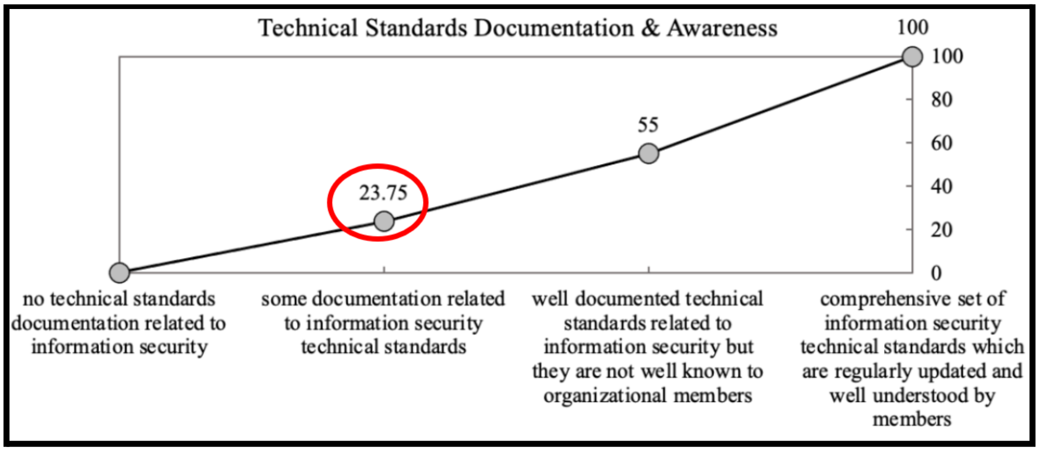


Figure 15: Technical Standards Documentation & Awareness

3. **Awareness Events:** Information security awareness events at Grande Ronde are currently limited to small IT groups and this has not been adopted as a company-wide approach. Reflecting this on the desirability curve, their maturity in this criterion stands at 18.75%. If they strive to be fully mature in this area, they should host regular security awareness events, some of which may be uniquely designed to appeal to discrete stakeholders while others could be well attended by large numbers of organizational members.

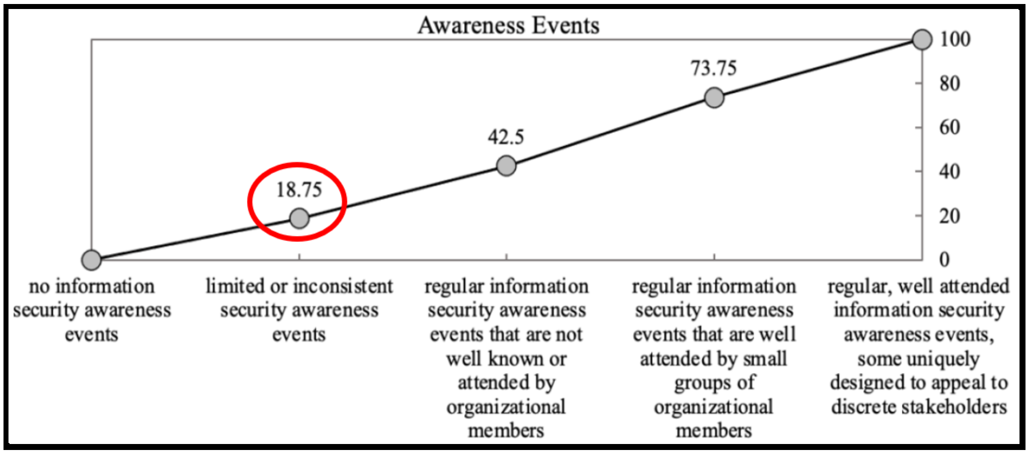


Figure 16: Awareness Events

4. **Information Portal:** Grande Ronde has an established information portal, however it is not well known to organizational members. Even though resources are available very few people in the hospital know about it and mostly call the front desk to get things done. Quantifying this, they can be scaled at 42.5% maturity level in desirability curve. Further, if they can have a well-established information portal that provides comprehensive information related to information security and should be actively used by organizational members.

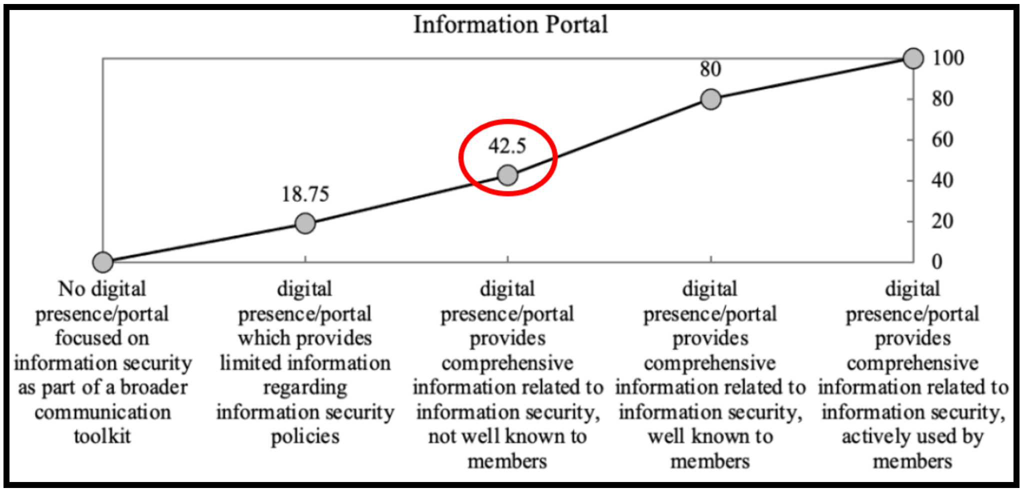


Figure 17: Information portal

5. **Asset Management:** Regarding asset management, Grande Ronde has some resources to support limited asset management capabilities for physical and virtual assets. While they lie at 26.25% maturity level in the desirability curve, they should have comprehensive tools, processes and staffing to support full life-cycle management for all physical and virtual technology assets in order to fully mature in this criterion.

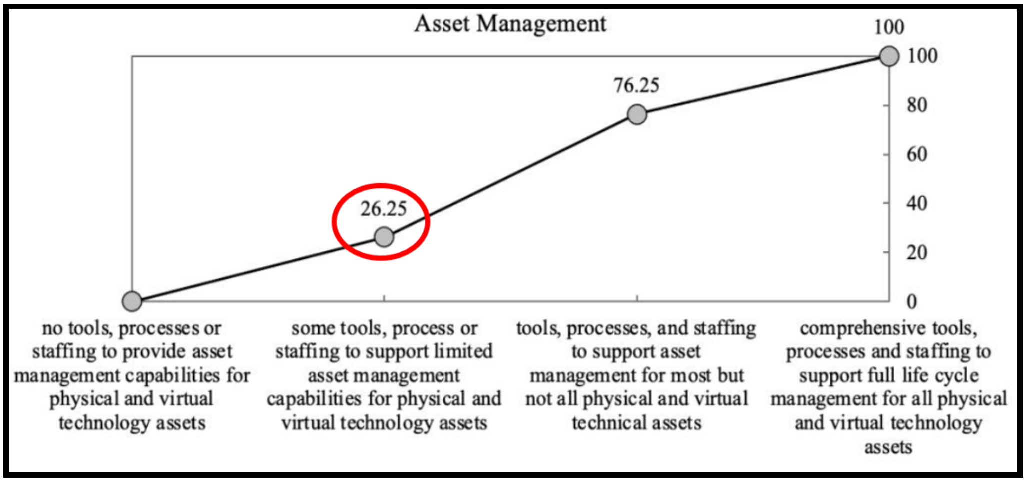
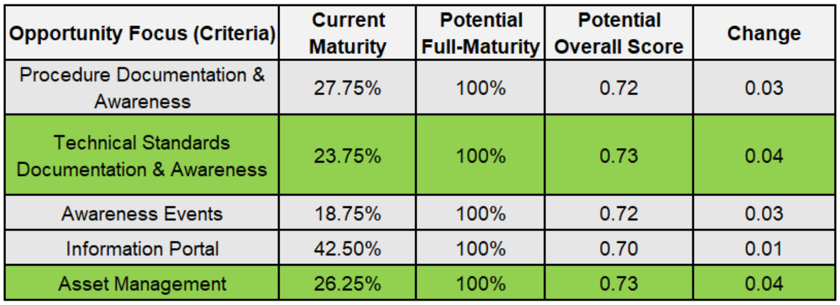


Figure 18: Asset Management

Opportunity Analysis

The table below represents how the overall maturity of Grande Ronde Hospital would change in response to the change in maturity level of criteria we listed as opportunities for improvement. Full maturity in the Information Portal would contribute an increase of 0.01 in overall maturity score. If they concentrated on either Procedure Documentation & Awareness or Awareness Events and raised them to 100% Maturity score, the overall score would increase up to 0.72, an improvement of .03. Finally, this healthcare organization could significantly improve its overall maturity score provided that they fully improve in one of these two criteria: Technical Standards & Awareness or Asset Management, to a total increased score of .04. It is because of the higher weighted values of these two criteria that they hold a greater impact on overall maturity score than others.



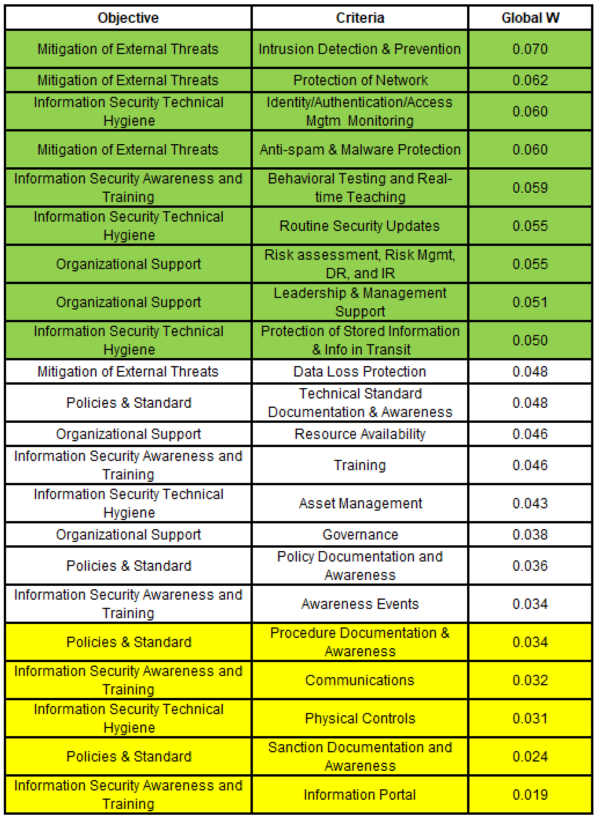
Opportunity Focus (Criteria)	Current Maturity	Potential Full-Maturity	Potential Overall Score	Change
Procedure Documentation & Awareness	27.75%	100%	0.72	0.03
Technical Standards Documentation & Awareness	23.75%	100%	0.73	0.04
Awareness Events	18.75%	100%	0.72	0.03
Information Portal	42.50%	100%	0.70	0.01
Asset Management	26.25%	100%	0.73	0.04

Table 6 - Opportunities focus

Criteria Ranking

We can see a visual representation of criteria ranking by global weight in the adjoining table. The top criteria are greater than 0.05, and the bottom 5 are less than 0.035, which we calculated based on overall objective weight and local criteria weight which were achieved as a result of expert feedback through the quantification and validation process. Interestingly, 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. Hence, this criteria ranking helps decision makers realize two things:

1. Some criteria have greater impacts in improving the overall information security maturity score.
2. Technology solutions alone are not enough to create a mature information security environment.



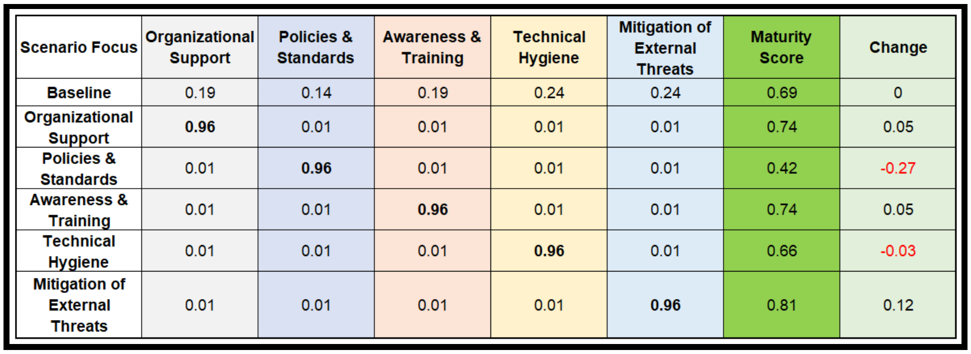
Objective	Criteria	Global W
Mitigation of External Threats	Intrusion Detection & Prevention	0.070
Mitigation of External Threats	Protection of Network	0.062
Information Security Technical Hygiene	Identity/Authentication/Access Mgtm Monitoring	0.060
Mitigation of External Threats	Anti-spam & Malware Protection	0.060
Information Security Awareness and Training	Behavioral Testing and Real-time Teaching	0.059
Information Security Technical Hygiene	Routine Security Updates	0.055
Organizational Support	Risk assessment, Risk Mgmt, DR, and IR	0.055
Organizational Support	Leadership & Management Support	0.051
Information Security Technical Hygiene	Protection of Stored Information & Info in Transit	0.050
Mitigation of External Threats	Data Loss Protection	0.048
Policies & Standard	Technical Standard Documentation & Awareness	0.048
Organizational Support	Resource Availability	0.046
Information Security Awareness and Training	Training	0.046
Information Security Technical Hygiene	Asset Management	0.043
Organizational Support	Governance	0.038
Policies & Standard	Policy Documentation and Awareness	0.036
Information Security Awareness and Training	Awareness Events	0.034
Policies & Standard	Procedure Documentation & Awareness	0.034
Information Security Awareness and Training	Communications	0.032
Information Security Technical Hygiene	Physical Controls	0.031
Policies & Standard	Sanction Documentation and Awareness	0.024
Information Security Awareness and Training	Information Portal	0.019

Table 7 - Criteria analysis and ranking

Scenario Analysis

We did a scenario analysis with the results for the overall maturity score based on the responses we received. To do this, we tested the sensitivity of the model and validated our findings by testing through extreme values by artificially weighing the objective levels differently than their actual value. For each scenario, we increased the objective level weights to 0.96 and kept all others at 0.01. The results showed that there is significant reduction in overall score when the focus is on **Policies and Standards**. Looking back to our responses from the interview, it makes sense that the organization is not mature enough in this particular objective segment and hence the reason for significant reduction in the overall score when the objective level weight is increased. This same approach applies to **Technical Hygiene** as well.

On the other hand, there is an increase in overall score when the focus is on **Mitigation of External Threats, or Awareness and Training, or Organizational Support**. It is because the organization is more mature in this segment which validates the results we received and the response we obtained from the interview.



Scenario 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	0.69	0
Organizational Support	**0.96**	0.01	0.01	0.01	0.01	0.74	0.05
Policies & Standards	0.01	**0.96**	0.01	0.01	0.01	0.42	-0.27
Awareness & Training	0.01	0.01	**0.96**	0.01	0.01	0.74	0.05
Technical Hygiene	0.01	0.01	0.01	**0.96**	0.01	0.66	-0.03
Mitigation of External Threats	0.01	0.01	0.01	0.01	**0.96**	0.81	0.12

Table 8 - Scenario focus

Recommendations

Based on our findings, the organization is not mature enough in two specific areas and an additional section that could use minor improvement:

Policies & Standards (Not Mature)

Even though there are documented policies and standards, most of them are followed through word of mouth practices. An improvement would be if those were distributed via training and, preferably, an online knowledge base for easy reference. Utilization of online portals can be effective for communication, awareness and training and ultimately lead to better problem solving. Internal policy should direct both Information Technology and general hospital staff to the knowledge base as the first source of information as opposed to calling in.

Awareness and Technical Hygiene (Not Mature)

Security awareness events are limited to specific groups which could be expanded to larger, more general groups based on the application and necessity. Physical asset management is solid but due to lack of resources, the virtual asset management is a little behind which can be mitigated by internal training or starting small on newer resources and expanding as policies and procedures are built up alongside virtual assets.

Mitigation of External Threats (Minor Improvement)

The organization has a good maturity in this regard, as long as they keep maintaining the same standards along with additional employee training, that will help them achieve a greater overall maturity score.

All in all, Grande Ronde is doing fairly well in regards to data security, but more focus should be directed toward the human factor of the organization, mainly disbursement of documentation regarding policies, standards, and security awareness and the reasoning behind why these are important and exist.

Conclusion

It is becoming more obvious year-over-year that information security controls need to improve across the US Healthcare industry. Current trends show data breaches will only become more frequent. By using Dr. Barnes HDM Maturity Model, organizations should be able to better predict where they need to focus their resources before an incident occurs and create a better security environment for their organization, especially those who are unfocused or those which have smaller budgets for their information security.

References

[1] F. Luh and Y. Yen, “Cybersecurity in Science and Medicine: Threats and Challenges,” *Trends in Biotechnology*, vol. 38, no. 8, pp. 825–828, Aug. 2020, doi: 10.1016/j.tibtech.2020.02.010.

[2] A. Agrawal *et al.*, “Evaluating the Security Impact of Healthcare Web Applications Through Fuzzy Based Hybrid Approach of Multi-Criteria Decision-Making Analysis,” *IEEE Access*, vol. 8, pp. 135770–135783, 2020, doi: 10.1109/ACCESS.2020.3010729.

[3] A. H. Seh *et al.*, “Healthcare Data Breaches: Insights and Implications,” *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[4] F. M. Dias, M. L. Martens, S. F. de P. Monken, L. F. da Silva, and E. D. R. Santibanez-Gonzalez, “Risk management focusing on the best practices of data security systems for healthcare,” *International Journal of Innovation*, vol. 9, no. 1, pp. 45–78, Apr. 2021, doi: 10.5585/iji.v9i1.18246.

[5] S. T. Argaw *et al.*, “Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks,” *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, Jul. 2020, doi: 10.1186/s12911-020-01161-7.