

**Developing Security Metrics Scorecard for Health Care  
Organizations**

by

Heba Elrefaey

Msc, Cairo University, 2001

Bsc, Ain Shams University, 1995

A Thesis Submitted in Partial Fulfillment  
of the Requirements for the Degree of

Master of Science

in the School of Health Information Science

© Heba Elrefaey, 2015

University of Victoria

All rights reserved. This thesis may not be reproduced in whole or in part, by  
photocopy or other means, without the permission of the author.

## **Supervisory Committee**

Developing Security Metrics Scorecard for Health Care Organizations

by

Heba Elrefaey

Msc, Cairo University, 2001

Bsc, Ain Shams University, 1995

Supervisory Committee

Dr. Elizabeth Borycki, School of Health Information Science

Supervisor

Dr. Andre Kushniruk, School of Health Information Science

Departmental Member

## **Abstract**

Supervisory Committee

Dr. Elizabeth Borycki, School of Health Information Science Supervisor

Supervisor

Dr. Andre Kushniruk, School of Health Information Science

Departmental Member

Information security and privacy in health care is a critical issue, it is crucial to protect the patients' privacy and ensure the systems availability all the time. Managing information security systems is a major part of managing information systems in health care organizations. The purpose of this study is to discover the security metrics that can be used in health care organizations and to provide the security managers with a security metrics scorecard that enable them to measure the performance of the security system in a monthly basis. To accomplish this a prototype with a suggested set of metrics was designed and examined in a usability study and semi-structured interviews. The study participants were security experts who work in health care organizations. In the study security management in health care organizations was discussed, the preferable security metrics were identified and the usable security metrics scorecard specifications were collected. Applying the study results on the scorecard prototype resulted in a security metrics scorecard that matches the security experts' recommendations.

## Table of Contents

Developing Security Metrics Scorecard for Health Care Organizations .....	i
Supervisory Committee.....	ii
Abstract .....	iii
Table of Contents .....	iv
List of Tables.....	vii
List of Figures .....	viii
Chapter 1 Introduction.....	1
1.1 Background.....	1
1.2 Security Objectives in Health Care.....	4
1.2.1 Confidentiality.....	4
1.2.2 Integrity .....	5
1.2.3 Availability.....	5
1.2.4 Accountability .....	6
1.3 Security Metrics .....	7
1.4 Security Metrics in Health care Organizations .....	8
1.5 Significance and Purpose of the Study .....	9
1.6 Research Questions.....	10
Chapter 2 Background and Theory on Security Metrics in Health Care Organizations	11
2.1 Introduction.....	11
2.2 Principles and Policies .....	12
2.3 Patient Privacy in Shared Data Environment.....	15
2.4 Hospitals Integration Case Studies .....	17
2.5 Risk Analysis Studies .....	20
2.6 Security Metrics Outside of Health Care .....	23
Chapter 3 Security Metrics Scorecard Background and Design .....	30
3.1 Balanced Scorecard (BSC) .....	30
3.1.1 Financial perspective.....	31
3.1.2 Customer perspective .....	31
3.1.3 Internal perspective .....	31
3.1.4 Learning and growth perspective .....	31
3.2 Security Metrics Visualization.....	32
3.3 Human Computer Interaction and Usability Engineering .....	36
3.3.1 Cognitive Theory and Assessing User Needs .....	37
3.3.2 System Evaluation and Usability Testing .....	38
3.4 Applying Usability Methodologies to Security Metrics .....	38
3.5 Prototype Design Recommendations.....	39
3.6 Security Metrics Scorecard.....	41
3.6.1 Score Card Audience.....	41
3.6.2 Major Organization’s Objective.....	41
3.6.3 Areas of Interest .....	41

3.6.4	What Metrics? .....	42
3.7	CIS Suggested Metrics.....	42
3.8	Metrics Groups.....	43
3.8.1	Incident Management .....	43
3.8.2	Vulnerability Management.....	44
3.8.3	Application Security .....	44
3.8.4	Financial Metrics .....	44
3.8.5	Management Metrics .....	44
3.8.6	Operational Metrics .....	45
3.9	Scorecard Design .....	45
3.10	Impact Metrics .....	46
3.10.1	Number of Incidents .....	47
3.10.2	Cost of Incidents.....	47
3.10.3	Mean-time between Security Incidents .....	47
3.10.4	Mean-time to Incident Recovery .....	47
3.11	Operations Metrics.....	48
3.11.1	Number of Applications .....	48
3.11.2	Number of Systems with No Known Severe Vulnerabilities.....	48
3.11.3	Vulnerability Scanning Coverage .....	48
3.11.4	Number of Known Vulnerability Instances.....	49
3.11.5	Mean-time to Mitigate Vulnerabilities .....	49
3.11.6	Mean Cost to Mitigate Vulnerabilities .....	49
3.12	Financial Metrics .....	49
3.12.1	IT Security Spending as Percentage of IT Budget .....	50
3.12.2	IT Security Budget Allocation .....	50
3.13	Scorecard Visualization and Prototype Development .....	50
Chapter 4	Study Design and Research Approach.....	53
4.1	Methodology .....	53
4.2	Participants.....	53
4.3	Recruitment.....	54
4.1	Setting .....	55
4.2	Data Collection .....	56
4.2.1	Demographic Questionnaire.....	56
4.2.2	Interviews .....	57
4.2.3	Usability Study .....	57
4.3	Materials .....	58
4.4	Procedure .....	58
4.5	Data Analysis .....	59
4.6	Ethics Approval .....	60
Chapter 5	Study Findings .....	61
5.1	Introduction.....	61
5.2	Characteristics of the Participants in this Study .....	61
5.3	Semi-structured Interview Data .....	63
5.4	Managing Security in Health Care.....	64

5.4.1	Technical Security .....	65
5.4.2	Information Security.....	66
5.4.3	Standards and Guidelines .....	68
5.5	Security Metrics Scorecard .....	70
5.5.1	Security Metrics .....	70
5.5.2	User Acceptability and Usability .....	72
5.5.3	Audience Oriented.....	73
5.6	Security Metrics Evaluation.....	74
5.6.1	Impact Metrics (Security Breaches and Incidents).....	74
5.6.2	Operation Metrics (Vulnerabilities) .....	79
5.6.3	Financial Metrics .....	83
5.7	General Recommendations for Improvements .....	84
5.7.1	What Metrics are Good?.....	84
5.7.2	What Metrics are Irrelevant.....	85
5.7.3	Additional Metrics Suggested .....	87
5.7.4	Visualization and Structure .....	91
5.8	Conclusion .....	92
Chapter 6	Discussion.....	94
6.1	Introduction.....	94
6.2	Security Management in Healthcare.....	94
6.3	Using Security Metrics in Health Care .....	97
6.4	Security Metrics Scorecard.....	99
6.5	Human Computer Interaction and Usability Testing.....	101
6.6	Suggested Recommendations for Security Metrics Scorecard .....	102
6.7	Modified Scorecard Prototype .....	104
6.7.1	Incident Metrics.....	104
6.7.2	Financial Metrics .....	106
6.7.3	Training Metrics .....	106
6.7.4	Selective Follow-up Metrics .....	107
6.8	Research Limitations .....	110
6.8.1	Limited Sample Size .....	110
6.8.2	Inability to Apply Additional Iteration of the Study. ....	111
6.9	Future Research .....	112
6.10	Security Metrics and Health Informatics Education.....	113
6.11	Study Contribution to Health Information Practice .....	113
Chapter 7	Conclusion .....	114
References	.....	117
Appendix A	.....	122
Appendix B: Demographic Questionnaire	.....	123
Appendix C Interview guide	.....	125
Appendix D	.....	127
Appendix E	.....	132
Appendix F Website Post	.....	134
Appendix G	.....	135

## List of Tables

Table 1 Metric categories (CIS, 2010, p. 4) .....	25
Table 2 vulnerability metrics quarterly (example of table illustration).....	35
Table 3 Summary of participant demographics. ....	62
Table 4 Categories of semi-structured interview findings. ....	63
Table 5 Summary of participants' feedback about the scorecard.....	93
Table 6 Definitions appear in Security metrics scorecard (modified) page 2 .....	109

## List of Figures

Figure 1 Number of weak passwords by department (bad visualization example).....	34
Figure 2 Number of weak passwords by department (good visualization example) ....	34
Figure 3 an example of time series chart.....	35
Figure 4 A sample of using small multiples.....	36
Figure 5 An example of a clear graph from The Economist (2013) .....	40
Figure 6 Interview Diagram .....	55
Figure 7 Security Metrics scorecard (modified) page 1 .....	108



## Chapter 1 Introduction

### 1.1 Background

In health care organizations, risk management and security control are crucial. Controlling security implies protecting babies from being kidnapped, keeping drugs safely locked away and preventing unauthorized access to secure areas and records. The use of electronic health records (EHR) is widely spreading in health care. The EHR is a comprehensive record for a specific individual that incorporates selected information from every health care encounter (Nagle, 2007). As the EHR holds personal information that needs to be private, a greater emphasis will need to be placed on data security measures that touch all aspects of health care organizations. In 1999, the Canadian Medical Association (CMA) conducted a survey, which found that “11% of the public held back information from a health care provider due to concerns about whom it would be shared with or what purposes it would be used for”. The number did not change in 2007 survey (BCMA British Columbia medical Association, 2009, p. 1).

Health care organizations are rapidly moving toward the adoption and integration of EHRs. This facilitates information sharing between groups (i.e. regional health authorities), but this kind of sharing is opening up new venues for risk (Matthews, 2007). To promote patient safety and the appropriate availability of health information such access to patient information must be combined with controls that prevent access to sensitive data by unauthorized individuals. Sharing health data ensures information is available when needed, but can affect the security of that data. External data security related attacks on health care organizations have increased by 85% between January 2007

and January 2008 in the USA (Counter Threat Unit, 2008). Compared with other industries, health care has the highest percentage of Internet vulnerabilities, an average of 61.07% compared to an average of 27.37 % across all other industries (Wimalasiri, Ray & Wikon, 2005). In the last four years (2010-2014) the number of criminal attacks targeting health care information increased by 100 % according to a study on 91 health care organizations (Ponemon Institute, 2014). Another expert mentioned in an article posted on August 2014 that he saw a 600% increase in attacks on health care organizations during the last 10 months (j.p. Mello, 2014).

In Canada, the case is not different. Jim Forbes, the CTO (chief technology officer) at shared information management services (SIMS), the primary information technology provider for the Toronto-based University Health Network (UHN) and seven other institutions, stated he has not seen any increase in the number of hacker attacks on patient records.

“but I don’t see any reason why it would differ (from the U.S.) We certainly use the same technology from the same providers. I don’t think we would be any better off” (Sutton, 2008, Para. 12).

Forbes thinks that the number of attacks and vulnerabilities in health care organizations in Canada are expected to be in the same range as the USA. The increasing number of attacks and vulnerabilities has to be faced by more security controls to overcome their effects.

Another statistic showed that, in the period between January 2007 and end of August 2009 in the USA and Canada, there were 115 breaches that happened involving 2.7 million patient records (Pascal, Elemam & McCarrey, 2009).

As health care organizations possess personal patients' information, a data breach occurs when that information falls into the wrong hands or is extracted, viewed, or captured by unauthorized individuals. Medical information theft is not discovered as fast as credit card numbers, which give hackers the opportunity to use such data more efficiently, and this makes health data more profitable. According to Don Jackson, director of threat intelligence at PhishLabs, a cybercrime protection company; hackers sell health credentials for a 10-20 times the price of credit card numbers (C. Humer & J. Finkle, 2014). For example in November 2007, a consultant working for the Provincial Public Health Laboratory in Newfoundland and Labrador unplugged a computer and took it home with him. An anonymous tipster claiming to be a security consultant called after the computer was removed and said they were able to access patient health data over the Internet. Another incident happened in January 2007, when a laptop containing 2,900 patient records from the Hospital for Sick Children in Toronto was stolen from a physician's van (Sutton, 2008). These two incidents showed how one breach can lead to a leak of a huge amount of patient's personal information (which may affect the safety of these patients). The number of records breached in attacks can vary from hundreds or thousands records -as in the case happened in breaching BC Pharmanet and 1600 accounts breached in July 2014 (cbc, 2014) - to millions as the attack happened in US community Health System Inc. in August 2014 that lead to revealing 4.5 million patients' data (C. Humer & J. Finkle, 2014).

Health care organizations such as regional health authorities must take the appropriate technical and organizational measures to maintain confidentiality, integrity, availability and accountability of information. This means protecting patients' data against

destruction, or loss, and any form of unauthorized processing (such as access, alteration, and communication of patient information). These technical and organizational measures shall ensure an appropriate level of security is provided for sensitive medical data and the evaluation of potential risks takes place (Ilioudis & Pangalos, 2001). In order to confront security issues in health care, organizations should have a successful security management and planning process, which cannot be achieved without a clear set of security metrics.

## **1.2 Security Objectives in Health Care**

Information Security has changed from being a technical initiative towards a broader business focused concern (for the protection of information in all of its forms across the organization). Information Security managers aim to deliver real business benefits by both protecting and yet facilitating the controlled sharing of information and managing the associated risks across a changing threat environment (Ashenden, 2008). This expansion in health care organizations promotes the need for more work focused on the specific security issues found in a health care environment. Health information systems are expected to provide accurate information at the proper time and place, and to the right people (Kokolakis, Gritzalis & Katsikas, 1998). Thus, health information systems should preserve the confidentiality, integrity, availability and accountability of the EHR.

### **1.2.1 Confidentiality**

Confidentiality means the assurance that patient data are not made available or disclosed to unauthorized individuals (Van der Haak et al., 2003). When patients know their information is treated confidentially, they are willing to share it with health care

professionals, resulting in improved health care. Thus, preserving confidentiality benefits both individuals and society. Threats to confidentiality include economic abuses or discrimination by a third-party. Third parties can be payers, employers, and others who take advantage of the burgeoning market in health data. Another threat to confidentiality is insider abuse, or record snooping by hospital or clinic workers and hackers.

Coworkers might not be directly involved in a patient's care but examine a record out of curiosity or for blackmail. Hackers are people who, via networks or other means, copy, delete, or alter confidential information (Shortliffe & Cimino, 2006). Confidentiality can be achieved through secure connections and authorization techniques.

### **1.2.2 Integrity**

Integrity can be defined as ensuring that data cannot be changed or deleted by unauthorized individuals or parties (Van der Haak et al., 2003). Avoiding medical errors represents a major challenge for health care organizations as evidenced by the Institute of Medicine's report "To Err is Human" (HIMSS, 2005). Unauthorized and incorrect changes to a patient's medical record or data in medical equipment (i.e. breaches of integrity) yield medical errors with potentially disastrous consequences for health or life (HIMSS, 2005). Integrity can be achieved through the use of digital signature techniques (Van der Haak et al., 2003).

### **1.2.3 Availability**

Availability means that, data can be accessed and used by authorized people upon demand (Van der Haak et. al., 2003). Health care information should always be available when needed to provide patient care and avoid medical errors. The Institute of Medicine

emphasizes the role of unavailable information in causing medical errors (HIMSS, 2005). Ensuring the availability of information includes data replication as well as a disaster recovery strategy. An example of an availability breach incident occurred in London in November of 2008: 4,700 PCs were infected by a worm at three hospitals and this led to shutting down these computers till they were cleared of the infection (Kirk, 2009).

#### **1.2.4 Accountability**

Accountability refers to the actions of a person, especially the modifications that he/she performs on data stored in the system that can be traced (Van der Haak et al., 2003). Accountability can be ensured by means of so-called audit trail logs or file logs. These trail logs store the user's identification, date and time of the session, documents used, changes in files or documents made by the user and other important data that are needed to reconstruct the way a change of data has taken place.

To build a security system in a health care organization one needs to achieve the above four objectives (i.e. confidentiality, integrity, availability and accountability) through policies and security mechanisms so the patient's information is kept confidential and cannot be altered by an unauthorized individual. Also, there is a need to ensure medical information is unconditionally available when needed and any modifications to the patient's EHR can be traced. After establishing the security of the system, managers need to evaluate the performance of the system and recommend improvements when needed, and this can be done by studying and analyzing the security metrics of the system.

### 1.3 Security Metrics

According to Jaquith (2007) a metric is a consistent standard of measurement, and it is anything that quantifies a problem space and results in value for an organization. The primary goal of metrics is to translate the data of the organization into meaningful numbers to help managers evaluate organizational performance. Metrics and measurements are two different things. Measurements are specific values recorded in a specific time, while metrics are results from analyzing the measurements over a specific period of time (Savola, 2007).

Using metrics in the field of security provides a tool to measure the security level in the organization, it can clarify how far the organization applied the security policy and how effective the security controls work, by answering the managers questions about security they can understand the current status and take right decisions about investments to improve it (Wang, 2005). More importantly, metrics enable managers to continue watching and understanding security status regularly, which will lead them to improving overall organizational security (Ravenel, 2006).

According to Wayne (2009), using security metrics can help managers who are making decisions that affects organizational security improvements in the future. Using security metrics also, enables managers to check if the system complies with the required policies and reflects the effectiveness of the security system. Gathering and analyzing security status in the form of metrics enables business leaders to understand, evaluate and plan for better security. Most importantly, as stated by Ravenel (2006):

“because security is being measured, it can be managed and continuous improvement can ensue.”

Research has shown: there are many successful cases of implementing and using security metrics (Qu & Zhang , 2007).

Good metrics are “SMART - specific, measurable, attainable, repeatable, and time dependent” (Nichols & Sudbury, 2006). For Jaquith (2007) a good metric should be consistently measured, cheap to gather, expressed as a cardinal number or percentage and expressed using at least one unit of measure such as defects, hours, or dollars. Therefore, security metrics are used to measure the security of a system, which aids in organizational decision making and helps to determine compliance with security requirements, or to support organizational quality assurance processes.

#### **1.4 Security Metrics in Health care Organizations**

As the importance of ensuring security in health care organizations increases, security spending continues to grow and so does the need to manage and understand the impact of security programs. This cannot be done without security metrics that give quantifiable information (e.g. numbers show how many attacks happened during a specific period). These metrics should be illustrated in a clear and easy to understand form.

Security management is a general problem that exists in wide range of organizations so the research about this area is also general except some cases about IT and banking. For the special nature of the security requirements in health care organizations, there is a need for in depth studies. These studies should investigate what kind of metrics are needed by health care organizations to help high level leaders who are managing, planning and improving the security programs. Some examples of studies related to the health care field will be reviewed in in the next chapter.



The main problem addressed in this study was to find a description of security metrics that can be applied effectively in health care organizations to guide managers through controlling security issues. To verify the usability of the proposed set of metrics delivered via scorecards, the researcher applied human computer interaction and usability engineering approaches.

### **1.5 Significance and Purpose of the Study**

The results of this work contributed to activities that aid in facilitating security management in health care organizations by providing a metrics scorecard prototype. It is hoped the scorecard that arose from this research will help with managing security within organizations and will improve their security level. Also, the scorecard may make communication between health care organizations easier, if they are using the same metrics' technique. It is hoped this study will encourage more research in the area of security management and related issues such as introducing new policies for different parts of information systems in health care organizations. The outcomes of this study might also promote research related to security requirements and new standards specific to health care.

The purpose of this study was to develop a security metrics scorecard that could be used in health care organizations and help security managers in this field. These metrics were introduced in the form of a scorecard. The proposed scorecard needed to be acceptable and usable to health care security managers. The research was conducted by interviewing a group of experts who work in the area of security in health care organizations. The work involved testing the usability of the scorecard with these individuals while they were checking it. The researcher collected their feedback about

the suggested scorecard prototype, then analyzing the results to extract their preferences and recommendations in order reach an acceptable form.

## **1.6 Research Questions**

The research questions in this work were:

- 1) How do health care organizations currently manage information security?
- 2) What security metrics can be used in health care organizations?
- 3) What do security managers think about using security metrics scorecard in health care organizations?
- 4) What are the specifications for usable and effective security metrics scorecard?

The answers to these questions provides a clear view of using security metrics in health care organizations, and what metrics are more important and have to be monitored. There are also recommendations for the preferred design and specifications for creating a usable and effective scorecard.

## **Chapter 2 Background and Theory on Security Metrics in Health Care Organizations**

### **2.1 Introduction**

In order to find out how the topic of “security metrics in health care organizations” appears in the literature, a search was undertaken of the Pubmed database and key industry journals including the Journal of the American Medical Informatics Associations, the Journal of Biomedical Informatics, International Journal of Medical Informatics, Methods of Information in Medicine, and IEEE proceedings. The keywords used in the search were ”security metrics”, “security metrics in health care”, “information security management” and “data security in health care”. Excluding articles that addressed cyber security systems (only as they are limited to one type of application which is out of the scope of this work) and articles that study security in a setting other than hospitals, for the same reason. And then included articles dated 1998 to 2014. Due to the relatively few articles that directly address the research area of “security metrics in health care” the researcher decided to extend the search to get a clearer picture about the status of research related to information security in health care organizations in general and, in addition to the research related to security metrics in health care organizations Looking at information security in health care in general as a research area the researcher can find that, research has some major foci, which include:

1. The importance of security management and the policies needed to verify security.
2. The importance of patient privacy in an environment of shared data between organizations.

3. Case studies from hospitals related security issues.
4. Risk and threat analysis in health care settings.

In this section, the articles mentioned in the above research areas will be discussed. In addition to reviewing some relevant research related to security metrics visualization and how to apply usability engineering approaches to security metrics.

## **2.2 Principles and Policies**

Many articles aim to study security principles and policies in the health care environment. For example, the study by Buckovich, Rippen and Rozen (1999), who collected a set of principles on privacy, confidentiality, and security from ten different sources, the sources mentioned in the study were: the Secretary of the Department of Health and Human Services, the Koop Foundation, the Center for Democracy and Technology, the Association of American Medical Colleges, the draft Model Privacy Law of the National Association of Insurance Commissioners, the Medical Privacy and security Protection Act, the discussion draft of the Medical Information Protection Act of 1998, the National Research Council, the Computer-based Patient Record Institute and the American Society for Testing and Materials

The authors listed extracted principles from these organizations and analyzed them to identify the most supported principles by these entities. The result was eleven primary principles that are commonly supported in all sources as mentioned in (Buckovich et al., 1999), :

“1) Individuals have a right to the privacy and confidentiality of their health information.

2) Outside of the doctor–patient relationship, health information that makes a person identifiable shall not be disclosed without prior patient informed consent and/or authorization.

3) All entities with exposure or access to individual health information shall have security/privacy/ confidentiality policies, procedures, and regulations (including sanctions) in place that support adherence to these principles.

4) Individuals have a right to access in a timely manner their health information.

5) Three entities have exceptions to the right to access, for specific state law requirements or for the protection of individuals have a right to control the access and disclosure of their health information and to specify limitations on a period of time and purpose of use.

6) Employers have a right to collect and maintain health information about employees allowable or otherwise deemed necessary to comply with state and federal statutes. However, employers shall not use this information for job or other employee benefit discrimination.

7) All entities involved with health care information have a responsibility to educate themselves, their staff, and consumers on issues related to these principles (e.g., consumers' privacy rights).

8) Individuals have a right to amend and/or correct their health information. One of the ten organizations has an exception and refers to the exception as 'under certain circumstances'.

9) Health information and/or medical records that make a person identifiable shall be maintained and transmitted in a secure environment.

10) An audit trail shall exist for medical records and be available to patients on request.

11) Support for these principles needs to be at the federal level." (p. 127)

Bakker (1998) discussed the importance of the CIA-triad (confidentiality, integrity and availability) in health care. As it was in the early period of using computer systems in health care, Bakker (1998) shed light on the importance of having a clear security policy and applying security measures at both the technical and organizational level, in addition to the importance of educating people working in the field of health care about information security.

In another example Kolkowska, Hedström and Karlsson (2008) defined information system security (ISS) goals in the formal system of a Swedish hospital then related the ISS goals to the traditional objectives of ISS (Confidentiality, Integrity and Availability) known as the CIA triad. To identify formal ISS goals the authors began with document

analysis. Analyzed documents were then related to documents from the county council and from formal hospital documents. Analyzing the documents resulted in a list of goals; the authors organized and classified them into main goals and goals. These processes resulted in seven formal goals in the hospital studied, which were

“Complete confidentiality, Available information, Traceability, Reliable information, Standardized information, Follow ISS laws, rules, and standards and Informed patients and/or family” (Kolkowska et al., 2008, p. 6).

The authors discussed how only three of these goals were covered by confidentiality, integrity and availability, and other goals ‘Follow ISS laws, rules and standards,’ ‘Traceability,’ ‘Standardized information’ and ‘Informed patients and/or family’ remained uncovered, which meant that the three traditional security goals are not enough in a hospital setting to ensure the desired security.

Other types of policies were also discussed by Behlen and Johnson (1999). The researchers described the principles and considerations that should be taken into account while building a multicenter research database to keep the security of the patient’s data verified according to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The authors studied the interests of the patients who expect their data to be treated confidentially and used to benefit their care, and explained how the regulations and state laws support these interests. Federal regulations in the United States have empowered Institutional Review Boards (IRBs) to protect patients’ interests in accordance with federal regulations set forth in the Federal Policy for the Protection of Humans.

The authors also studied the research institute’s interests in ensuring that research systems have security mechanisms sufficient to prevent abuse in order to avoid liability.

They stated that strict adherence to Institutional Review Board procedures is the best protection from this risk. For multicenter research projects, an IRB approved research procedure is required at each site and, thus, a responsible principal investigator is required at each site as well. This protects the interests of each site institution while satisfying public policy requirements for the protection of the interests of patients.

In this section, the reviewed studies were displaying how the researchers demonstrated security principles or policies that can be applied in health care organizations as in Buckovich, Rippen and Rozen (1999) and Bakker (1998). Other researchers gave recommendations to help in creating such policies as Behlen and Johnson (1999); another type was studying the information system security goals as in Kolkowska, Hedström and Karlsson (2008).

### **2.3 Patient Privacy in Shared Data Environment**

Sharing the EHR between health care institutions raises a number of issues. In Van der Haak et al., (2003) the authors described possible ways for meeting the legal requirements based on German and EU law (as a part of a research project at the Department of Medical Informatics of the University of Heidelberg). The project goal was to develop a cross-institutional EHR for the Thoraxklinik-Heidelberg and the department of clinical radiology of the University Medical Center of Heidelberg.

In this article, the authors clarified different types of security measures such as:

- measures needed in the case of a cross-institutional EHR to ensure confidentiality through secure connections (e.g. firewalls) and through authorization concepts,
- measures for ensuring authentication (by means of specific cryptographic algorithms),

- measures for ensuring integrity (by using electronic signatures),
- measures for ensuring availability specially in emergency cases like providing redundant storage for the data and;
- measures for ensuring accountability (using audit trail logs).

The security issues related to exchanging information between health care organizations appear in van der Linden, Kalra, Hasman, and Talmon (2009). The authors created a scenario about shared care. The scenario was divided into steps. Each step is an action that involves information exchange. The authors formulated questions related to security and privacy issues, like

“How should a patient be identified reliably across organizations? and, How should health professionals be identified reliably across organizations? How should organizations be reliably identified?” (van der Linden et al., 2009, p. 145).

They grouped the questions to view the underlying issues (i.e. Authorized access, Confidentiality, Patient consent, Relevancy, Ownership of information, Infrastructure, Audit log, archiving). After discussing these security issues, they found that a solution for one issue could cause additional problems for another one. They suggest a paradigm shift from storing all incoming information in a local system to retrieving information from external systems when needed for patient care. The information sharing requires cooperation between the organizations and consensus on the restrictions and rules across organizations. Audit logs must be trusted to enable regeneration of past interactions.

The above section illustrated some studies about how to maintain the patients' privacy while data are being shared in the health care environment. The studies provide the measures needed to ensure privacy (van der Haak et. al., 2003), the underlying security issues that appear during communication in health care organizations and the



recommendations to maintain security while allowing for data sharing (van der Linden et. al., 2009).

## **2.4 Hospitals Integration Case Studies**

In this section, the researcher discusses several case studies related to hospital information systems integration and the effect of this integration on the information security. The first case study appears in Matthews (2007). Matthews discussed integrating eight health facilities in a regional health authority in Ontario. The goal of the program discussed in the case study was to create an efficient security system that works invisibly in all participating hospitals and was planned to be done in three years. The challenge in that project was to set a standard for security across the group so that each hospital's staff felt comfortable sharing information while each IT department in the group worked independently. The plan was to make an assessment for each enterprise according to a common security standard, to study the regional security strategy and to implement a security program in each enterprise. The region created a Federated Information Risk Management Organization. A regional information security officer (RISO), who manages the security management framework in all participating hospitals, supervises this organization. Each hospital's security staff is charged with complying with the policies and tools within the organization (i.e. the organization's requirements for integration). The integration between hospitals helped IT managers to benefit from using inter-related tools at a low cost, enabled access to many tools and received more support from vendors. Working as a group enabled the managers in each hospital to know the best practices across the region and to lower the cost of maintenance and training as well (Matthews, 2007).

The second case study is the one studied by Ravera, Colombo, Tedeschi, and Ravera, (2004), and is about a multispecialty private hospital named Istituto Clinico Humanitas (ICH) in Rozzano (Milan, Italy) which has 437 beds, 18 operation theatres and 110 outpatient consulting rooms, in addition to biomedical and biotechnological research, and also a university teaching centre. The ICH hospital is part of “Humanitas” project, a project aimed at constructing and managing private health care. All the departments in ICH are fully computerized. The authors explained how the information system in the hospital ensures integrity, availability and confidentiality as is the main objective in any information system. In the hospital the information management department provides a strong backup and data recovery system and implements component redundancy or fault tolerance programs to minimize the downtime of the system (they use passwords and authentication techniques, they use biometric technology to verify the users’ identity through fingerprints, encryption and firewalls).

In the third case study Collmann and Cooper (2007) in their research described an incident, where there was a security breach, involving Kaiser Permanent’s (KP) Internet Patient Portal. Kaiser Permanente (KP) functions as an integrated health delivery system. The security breach caused by a program written by two programmers led to revealing personal patient’s information in concatenated e-mails sent to 800 persons instead of separating them. The authors investigated the incident by interviewing KP staff, reviewing incident reports and media reports in addition to applying root cause analysis. After investigating all the related information the authors found that the breach occurred for number of reasons. Firstly, the architecture of the information system contributed to the breach. The application used at Kaiser is a complex interconnected

information technology and the complexity of the system led to transforming errors becoming cascading accidents. When the programmers placed the flawed program into the production environment, messages flowed through the KP Online system without interruption. The second reason was the motivations of individual staff members (as training was not sufficient to prevent the accident). The third reason was the differences among the subcultures of individual groups, as each group was working separately and with different priorities and ideologies; for example, the operation group was working according to disciplined standards and procedures while the development group adopted a fluid work process with a few standards and procedures. The last reason for the incident was the technical and social relations across the Kaiser IT program. The incident showed how the groups worked in isolation rather than consolidating masses of expertise.

In this section, several case studies about security issues relating to large hospitals or integrated multi-hospital systems were discussed. The integration between hospitals raises the need for standards, policies and guidelines to be followed by organizations verifying the security of systems and reducing the effects of security incidents if they occur (Matthews, 2007). The second case study was about the security measures applied in a large multispecialty hospital to ensure the integrity, availability and confidentiality of the patient information. The last case study investigated an incident involving a security breach (Collmann & Cooper, 2007) to develop lists of learned lessons and recommendations to avoid the repetition of such an incident. Although the studies described specific cases, they provided some general information that can be applied to implementing security in other health care settings.

## 2.5 Risk Analysis Studies

Another branch of information security related studies in the health care setting is risk analysis studies that study threats in a system and analyze them trying to find ways to deal with threats in order to overcome or minimize their effects. One of these studies involves conducting a risk analysis of a mobile instant messaging application (Bønes, Hasvold, Henriksen, & Strandenaes, 2007). The instant messaging application showed the usefulness of instant messaging (IM) in health care. The researchers proposed a secure IM architecture (MedIMob) with a detailed risk analysis covering the risks related to the mobile messaging while dealing with sensitive data. The authors discussed technical and non-technical risk reduction measures.

Huang, Bai and Nair (2008) studied the application of security metrics in health care by using the SSE-CMM “The Systems Security Engineering Capability Maturity Model” but changing it to match the patient centered health care domain instead of the process area it was originally designed for. The mapping between the two domains helped in developing a complete set of metrics for security and privacy risk assessment of EHR systems. The mapping process was based on HIPAA regulations that have five major regulation standards including Administrative Safeguards; Physical Safeguards; Technical Safeguards; Organization Requirement; Policies and Procedures and Documentation Requirements. The standards in each safeguard are mapped into SSE-CMM process areas. The authors focused on the 11 security engineering process areas in SSE-CMM because they define security-specific practices and have a close relationship with HIPAA standards and requirements. The 11 process areas are: Administer Security Controls, Assess impact, assess security risk, Assess threat, Assess vulnerability, Build

Assurance Argument, Coordinate Security, Monitor Security Posture, Provide Security Input, Specify Security Needs, Verify and Validate Security.

HIPAA regulations do not cover all the privacy issues in a health care environment, so Huang et al., (2008) used a scenario-based approach to identify the uncovered security and privacy issues. From these scenarios, the authors suggested solutions for the uncovered issues, and then provided a mapping for these solutions in SSE-CMM process areas. Huang et al., (2008) introduced an overall risk assessment process for patient centered health care systems.

Cavalli, Mattasoglio, Pinciroli, and Spaggiari, (2004) explained a case study of a multispecialty hospital in Italy and how the security and privacy are verified through that hospital. Cavalli et al., (2004) explained the design, implementation, management, and auditing of information security inside a multi-specialty provincial Italian hospital. In that research the authors explained how ISO 17799, the standard for information security management, can be applied to health care information systems. This standard is focused on businesses, and does not deal with particular privacy concerns that naturally arise when dealing with personal and sensitive medical data. Therefore, the authors needed to integrate ISO 17799 with CEN/ENV12924 (a standard for security categorization and protection for health care information systems) to cover the different security requirements in the health care sector. The researchers used four phases to achieve information security and management: Plan, Do, Check and Act, but they focused on the planning phase by doing threat assessments and risk assessment which is similar to threat assessment but takes into consideration the existing safeguards. They dealt with information security as a management process.

In summary, researchers in the above studies about risk analysis are trying to reduce risks by applying risk management measures. These measures have been developed from risk analyses of projects or by mapping from a well known standard as SSE-CMM as in (Huang et al., 2008), or by using standards as ISO 17799 and CEN/ENV12924 and do an integration between them to cover security requirements in health care as discussed in Cavalli et al. (2004).

Another example of security metrics based on ISO/IEC 27001 standard, found in (Azuwa, Ahmad, Sahib, & Shamsuddin, 2012) these standards were developed by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) for information security matters.

The authors reviewed the definitions of information security metrics and measures from multiple researches and then they came up with their own definition as

“information security metrics is a measurement standard for information security controls that can be quantified and reviewed to meet the security objectives” (Azuwa et. al, 2012).

The main idea in that paper was to introduce how to build a technical security metrics model to measure the effectiveness of the network security controls in compliance with the ISO/IEC 27001 standard, to do that they followed the plan, do, check, and act phases. The plan phase works on selecting controls from 133 controls suggested by ISO/IEC 27001 standard. In the “Do” phase the authors expressed the security of network in three network dimensions (Vulnerability, Exploitability, and Attackability) or the VEA-ability score. The check phase is about comparing the measurements with the target or the standards, then the Act phase begins, when the metrics will be validated by the organization in order to be used by the management team (Azuwa et. al, 2012).

Jafari, Mtenzi, Fitzpatrick and O'Shea (2009) proposed a security metrics approach to assess security posture for e-health care organizations; the security posture is the status of security in the organization. The purpose of this approach is to compare the security of different organizations in order to allow data exchange between them. The proposed approach constitutes five elements: technology maturity analysis, threat analysis and modeling, requirements establishment, policies and mechanisms and system behavior. By measuring those elements, the resulting metrics can be used to compare security posture in different organizations.

In reviewing security management in health care organizations as explained in the previous sections, some articles were found to be related to the principles and the policies needed for establishing secure information systems, other articles discussed how to keep the patient's privacy while allowing for data sharing. In addition to reviewing case studies about security issues related to data sharing, and related to risk analysis and security breaches. Few articles examined how security metrics are applied in health care organizations. More research is needed in the area of administrative policies and requirements to address additional security and privacy concerns. Researchers need to obtain feedback from industry experts for more applicable results. Case studies provide limited information and need to be fully examined for their applicability to different settings.

## **2.6 Security Metrics Outside of Health Care**

From outside the domain of health care, security management using security metrics appears in the literature in different ways. The studies in this work focused on:

1. how to build a security metrics system,

2. evaluation and classification of security metrics, and
3. industry oriented studies.

In Sanders (2014) the author pointed out the importance of security metrics and the different types of metrics (organizational, technical and operational security metrics). The author discussed the need to develop tools for quantitative assessment of security metrics that will make those metrics more usable and enable making better decisions throughout the system life cycle starting at design, and through to implementation, configuration, operation, upgrade or modification.

A general research study that resulted in a set of basic security metrics that can be used in a wide range of organizations was conducted by the Center of Internet Security (CIS) in 2010. CIS formed a team of one hundred experts with different backgrounds “consulting, software development, audit and compliance, security research, operations, government and legal” (p. 1). These metrics provided a basic set of indicators that cover six business functions: “Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics” (p. i). The purpose of developing these metrics is to help enterprises to improve security levels. Each organization can add more metrics as needed.

The basic metrics are selected and depend on the data that are collected in most organizations to encourage adoption of security metrics in organizations and improve the security systems. Working towards a standard security metric will make vendors modify the security products to comply with these metrics. All these steps will make organizations’ integration easier and safer. Table 1 from (CIS, 2010, p. 4) shows the metrics categorized according to their purpose and audience.



<b>Metric categories</b>	<b>description</b>	<b>Metrics</b>
Management Metrics	Provide information on the performance of business functions, and the impact on the organization. Audience: Business Management	Cost of Incidents Mean Cost of Incidents Percent of Systems with No Known Severe Vulnerabilities Patch Policy Compliance Percentage of Configuration Compliance Percent of Changes with Security Reviews IT Security Spending as % of IT Budget
Operational Metrics	Used to understand and optimize the activities of business functions. Audience: Security Management	Mean Incident Recovery Cost Mean-Time to Incident Discovery Mean-Time Between Security Incidents Mean-Time to Incident Recovery Mean-Time to Mitigate Vulnerabilities Mean Cost to Mitigate Vulnerabilities Mean Cost to Patch Mean-Time to Patch Mean-Time to Complete Changes Percent of Changes with Security Exceptions IT Security Budget Allocation
Technical Metrics	Provide technical details as well as a foundation for other metrics. Audience: Security Operations	Number of Incidents Vulnerability Scanning Coverage Number of Known Vulnerability Instances Patch Management Coverage Configuration Management Coverage Current Anti-Malware Compliance Number of Applications Percent of Critical Applications Risk Assessment Coverage Security Testing Coverage

**Table 1 Metric categories (CIS, 2010, p. 4)**

The authors explained for each metric what data needed to be collected, how to calculate the suggested frequency for collection (e.g. hourly, weekly, monthly) and the best way for visualization of the metrics. The document is designed to be a manual to start a security metric program.

Weiß, Weissmann and Dressler (2005) proposed a method to evaluate the security of organizations by calculating the percentage of lost assets during a period of time, so the

organization will be considered more secure when it loses less assets than another for the same time interval. The authors applied their approach on a university department showing steps of application.

Another way to assess the performance of a security system has been discussed by Breu and Innerhofer–Oberperfler (2008). They proposed a quantitative assessment for a security system in an enterprise. The assessment was designed based on an enterprise modeling framework created by the authors in a previous work. They used this modeling framework to build a security model for business security objectives (e.g. prevent frauds) in banking. By using these models, they illustrated how to conduct a security assessment and find out the causes of failures.

Breu and Innerhofer–Oberperfler’s (2008) quantitative assessment used measures that quantify the ratio of attacks which result in successful breaches of security requirements, the propagation effect of successful attacks and the losses for the organization. Although the example that was used in the article is based on the banking system, the same approach can be applied to different types of organizations. The authors stated in their future work section that they will apply the proposed approach to analyzing the security of a distributed cross-institutional health data record network.

Ravenel (2006) published an analysis of a survey about “collecting effective security metrics” conducted by the Robert Frances Group (RFG). The survey asked about collected virus related metrics (i.e. a virus detected in user files and in e-mail messages). A large majority of respondents (84.6%) reported measuring invalid log-ins and intrusion attempts. Respondents indicated that they were measuring spam detection and filtering (76.9 %) and spam was not detected (38.5 %). The results of the survey illustrated how

most of the participants (60%) felt the metrics they collect were effective or very effective. Most participants collected and tracked metrics from products that make this process straightforward, such as virus and spam detection packages, but when participants were asked about the process of delivering the metrics (61.5%), they stated that the process is not automatic. The author discussed the benefits of automating the delivery of security metric reports. Minimizing human intervention leads to more accurate and reliable measurements that can be used to track and plot any organizational security trends.

Savola (2007) introduced a taxonomy to support the development of feasible security metrics for companies that produce information and telecommunication technology products, systems or services. Taxonomies are frequently used for classification of objects into a hierarchical structure, which is a tree structure of a classification. The author started the tree with the root node (i.e. the business-level security metrics) which then divided into five categories: Business level security metrics

- └ Security metrics for cost-benefit analysis –such as ROI (Return of Investment),
- └ Trust metrics for business collaboration,
- └ Security metrics for business-level risk analysis,
- └ Security metrics for information security management (ISM), and
- └ Security, dependability and trust (SDT) metrics for ICT products, systems and services.

The author took the last two branches under the first level of the taxonomy tree (Security metrics for information security management (ISM), and provided a detailed tree to show how to classify security metrics under defined categories related to the upper

level of the tree; for example, the security metrics for ISM were divided into three sub categories

#### ISM

- └ management

- └ operational

- └ information system technical security metrics

The information system technical security metrics included two sub categories

The information system technical security metrics

- └ technical security dependability

- └ trust metrics and technical control metrics

The author then suggested the use of this taxonomy to develop a feasible security metric which covers the policies of the management and the details of the products.

In the manufacturing industry Qu and Zhang (2007) studied how to get numerical values for security levels. The authors dealt with security management as a process and proposed a model for measuring security, and then they applied that model in a manufacturing factory with 6000 workers. The study demonstrated that an effective assessment of a security system could be a great assistance to improving the control of information risk. They favor the idea of dealing with information security as a management process and applying the management rules from business area.

Although security objectives are unique and tied to the goals and the purpose of an organization, similarities in high level security objectives do exist between organizations performing similar work. Few studies were found that mainly address organizational security metrics in specific detail based on organizational security objectives. In

summary, the security management process is highly important in all kinds of organizations and especially in health care organizations due to the highly sensitive nature of information. More work is needed in the area of using security metrics in health care organizations.

## **Chapter 3 Security Metrics Scorecard Background and Design**

Managing security can be done using a definite set of values that determine how secure the system is at a specific point of time and how secure it was at another point of time and how the change happened through a period of time. Managers need to follow up with these changes in system performance to be able to reach decisions about how to improve the system. To verify this they need a tool that tells them clearly and easily all the information they need to know. This can be done using balanced scorecards (Jaquith, 2007).

### **3.1 Balanced Scorecard (BSC)**

Evaluation of a security system in order to verify its effectiveness requires measuring the performance of the system using metrics, and then arranging these metrics in a clear form. This can take the form of a scorecard or a balanced scorecard. A balanced scorecard (BSC) is a performance measurement system based on organizational strategy. The BSC was developed by Robert Kaplan and David in 1990 (Kaplan, 2008). Before, BSC organizational performance was measured mainly by financial metrics, but financial metrics display only the final results, not how these results are achieved. BSC's are called balanced because they show metrics from four different perspectives (Voelker, Rakich and French, 2001).

### **3.1.1 Financial perspective**

The financial perspective is about how to maintain the organizational goal by analyzing the financial metrics. In the case of security metrics, a BSC might show IT security spending as a percent of IT budget (CIS, 2010).

### **3.1.2 Customer perspective**

The customer perspective is about customer satisfaction, and in security management case it is concerned with data security and availability as the patient can be considered as customer. An example of metric related to this area is the number of incidents.

### **3.1.3 Internal perspective**

This type of metric considers the effectiveness of internal processes. An example of a metric related to this area is risk assessment coverage as it shows how effective is the process in assessing risks.

### **3.1.4 Learning and growth perspective**

This perspective is about the employees' development, training and improvements in the workplace. In case of security metrics, it might refer to security training programs efficiency, or frequency. The mentioned four perspectives are those that were introduced by Kaplan and David in 1990 (Kaplan, 2008). They were introduced as a framework, so each organization can modify, add or remove perspectives according to their needs, and then select the appropriate metrics that fit under each perspective in a way that will support these needs (Jaquith, 2007).

### 3.2 Security Metrics Visualization

As seen in the previous section selecting and managing security metrics is not always an easy process as it is not systematic, and there are no rigid rules surrounding it. The difficulty does not exist only in selecting and collecting security metrics, it also exists in designing the end-user tool that illustrates the security status of the organization to decision makers (e.g. scorecards). The visualization of measured data in security scorecards directly affects the usability of such tools. If a scorecard is not clearly displayed, data may be confusing and leads to wrong decisions. In this section, different ways of effectively illustrating data will be discussed and how this can be applied to scorecard design.

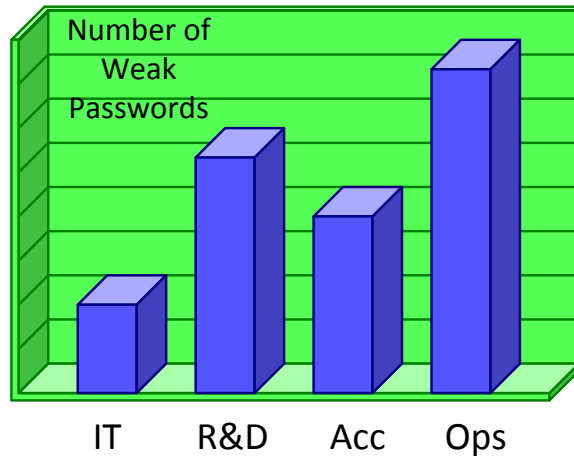
Security metrics data is quantitative in general. Quantitative data is primarily communicated in the form of graphs and tables (Few, 2004). Although graphics are a good way to present data, it depends on how and when graphics should be used. For example, Pie charts take a large space relative to the data they show. In addition, they tend to include only a single metric or data range. The usage of Pie graphs is always criticized and it is always recommended to avoid using them when possible, but designers use them because they are attractive to the user (Stabina, 2005). Bar charts like pie charts usually present only one metric, but they do not take the same large space. For line charts to be used, there must be 3 or more points to display and 5 or less lines (metrics) to view on one graph for readability purposes (Stabina, 2005). Traffic lights that show the status of a metric as one of three possible cases are a very simple way to present data. Unfortunately, they do not easily present quantified data (Jaquith, 2007).



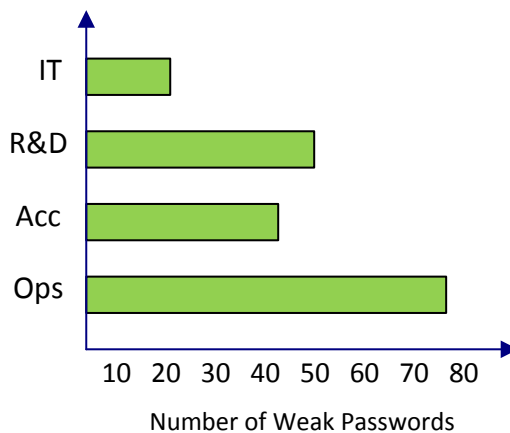
Stabina (2005) discussed the basic principles that need to be considered when designing a graphic display, while Jaquith (2007) outlined the basic design principles to make visualization of metrics effective. Based on the previous two sources the following points need to be considered while designing a security metrics scorecard:

- 1) The purpose of the visualization is to show the data clearly. It is important to keep the design simple so it will not overcome the clarity.
- 2) Simplicity is the key to a clear, easy read of graphs, which results in a more readable and usable scorecard.
- 3) Using 3-D graphs will reduce a scorecard's clarity, and make it harder to read the data (Jaquith, 2007; Stabina, 2005).
- 4) It is better to avoid lines in charts other than the x- and y-axes, even the grid lines can be muted. The data is the only element that should be clear in the graph (Jaquith, 2007), (Stabina, 2005).
- 5) Using saturated colors (Jaquith, 2007), fills and patterns (Stabina, 2005) can distract the user and can reduce the readability of the graph.
- 6) Labeling a graph will help the reader in knowing what it is about (Jaquith, 2007). Also the use of grids should be limited to cases where the text is longer than can be fitted in the graph. In this case it should be as close to the data as possible. It is also helpful to have the units of measures clear and the axis labelled (Stabina, 2005).

Figure 1, shows how a graph can present data in a complex unclear way. Figure 1 has 3-D without labeling the axis. In Figure 2, the data is presented in a simpler way with all the needed data but in a clear form.



**Figure 1** Number of weak passwords by department (bad visualization example)



**Figure 2** Number of weak passwords by department (good visualization example)

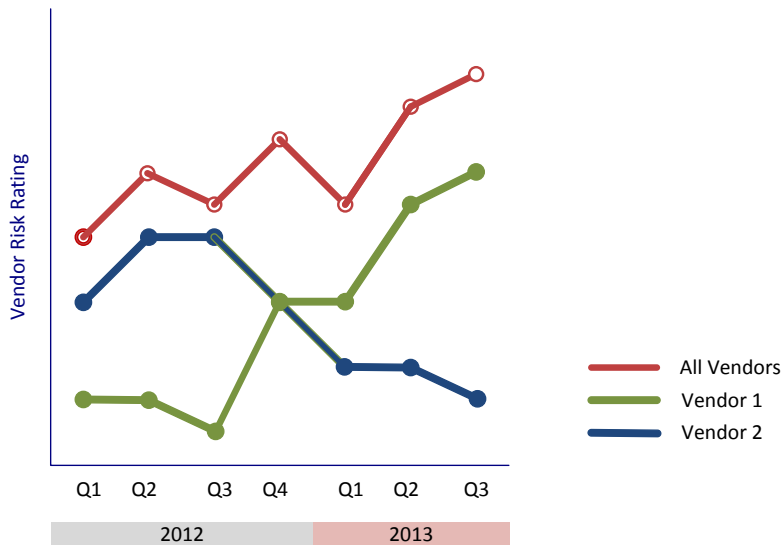
CIS (2010) discussed three different visualization types for security metrics. These types are simple visualization, graphical visualization and complex visualization. Simple visualizations can be represented as a table showing metric results for an organization

with each row displaying a value as a selected time period (each week or each month). Columns can include the value of metrics, like different vulnerability severities (e.g. Low, Medium, High) in the case of displaying vulnerability management, table 2 illustrates this case.

Month	Systems with no known severe vulnerability	Mean time to mitigate vulnerabilities	Number of known vulnerabilities
June	L	M	H
July	M	H	L
August	L	L	H
September	M	M	L

**Table 2 vulnerability metrics quarterly (example of table illustration)**

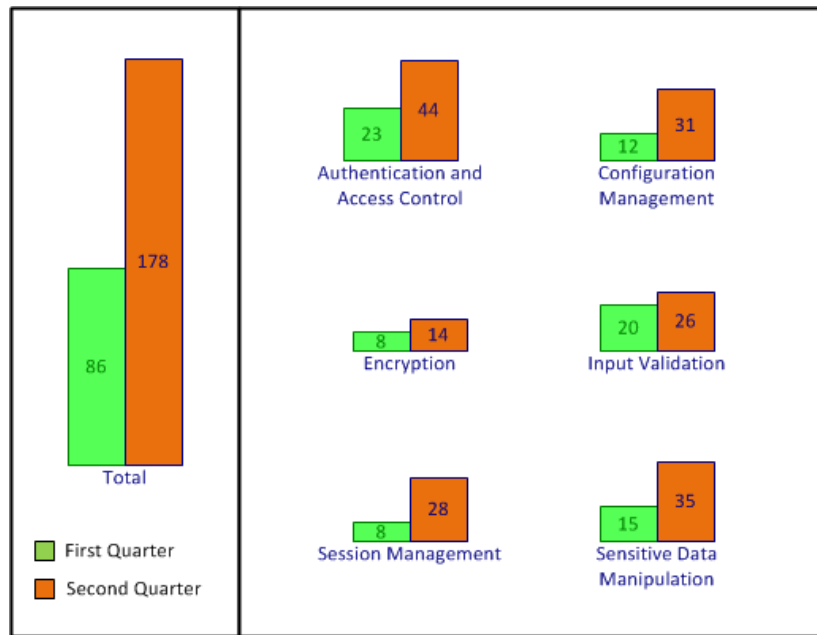
An example for graphical visualizations is the time-series chart, where the metric result is plotted on the vertical axis and time periods are displayed on the horizontal axis (e.g. month, years, and quarters). Figure 3 is an example of time series chart.



**Figure 3 an example of time series chart.**

Complex visualizations are needed when viewing a metric value in different business units. A form of these complex visualizations is the small multiples that could be used to

compare a number of high severity vulnerabilities across business units (CIS, 2010) A sample graph of using small multiples shown in Figure 4.



**Figure 4 A sample of using small multiples**

In this section, visualization methods for security metrics are discussed by reviewing recommendations for designing a graph display in general as declared by Stabina (2005) and for designing a security metrics tool as in Jaquith (2007), and then various ways of presenting data are presented and different designs are compared.

The design recommendations aim to help in reaching a clear graph and this will improve the usability of security metrics scorecard.

### 3.3 Human Computer Interaction and Usability Engineering

The study of human-computer interaction (HCI) is concerned with the human, social, organizational, and technical aspects of the interaction between human and machines.

Research in HCI lies at the intersection of a number of disciplines including: cognitive and social psychology, computer science, anthropology, sociology, the design sciences, and engineering (Kushniruk & Borycki , 2008). To include human computer interaction in design, users need to be involved as much as possible to make sure the designer knows what their requirements are. Software designers also need to integrate knowledge and expertise from different disciplines. As well, they need to be highly iterative when designing such systems until they reach a result that satisfies user needs (Preece, Rogers, & Sharp, 2004). In this section, the concepts of human computer interaction in design and evaluation will be used for security metrics tools, to ensure effectiveness and acceptability.

### **3.3.1 Cognitive Theory and Assessing User Needs**

HCI can be considered largely cognitive in that it involves processing of information by humans, in close conjunction with computer systems. Therefore, the application of ideas, theories and methods emerging from the field of cognitive psychology are highly relevant to the design and implementation of more effective health care information systems from the perspective of human users, for whom systems are designed to support and serve (Kushniruk & Borycki, 2008). There are a number of ways for applying human cognitive processing theories to improve the use of computer systems that can be applied to improve the use of a security metrics scorecard. This involves determining how easily the user can read and understand the scorecard data and use it effectively in managing security and taking decisions that affect organizational performance positively, in addition to pointing out the difficulties or misleading information in order to overcome them (Kushniruk & Borycki , 2008).

### **3.3.2 System Evaluation and Usability Testing**

There are a number of specific methods associated with usability engineering and foremost among these is usability testing. Usability testing refers to the evaluation of information systems that involves testing of participants who are representative of a target user population, as they perform representative tasks using an information technology. During the evaluation, all user–computer interactions are typically recorded (i.e, video recordings are made of all computer screens or user activities and actions) (Kushniruk & Patel, 2004). These techniques generally include the collection of “think aloud” reports, involving the recording of users as they verbalize their thoughts while using information systems.

Usability testing can be used as a part of the system development life cycle in rapid prototyping methods. This method typically involves the development of prototypes (defined as partially functioning versions of a system) which may be shown to users early in development process in order to assess the systems usability and functionality. The assessment can be done through the usability testing methodologies. Such work can be applied to security metrics scorecards to show users how the metrics will appear as well as learn about users’ reaction to designs in order to improve it.

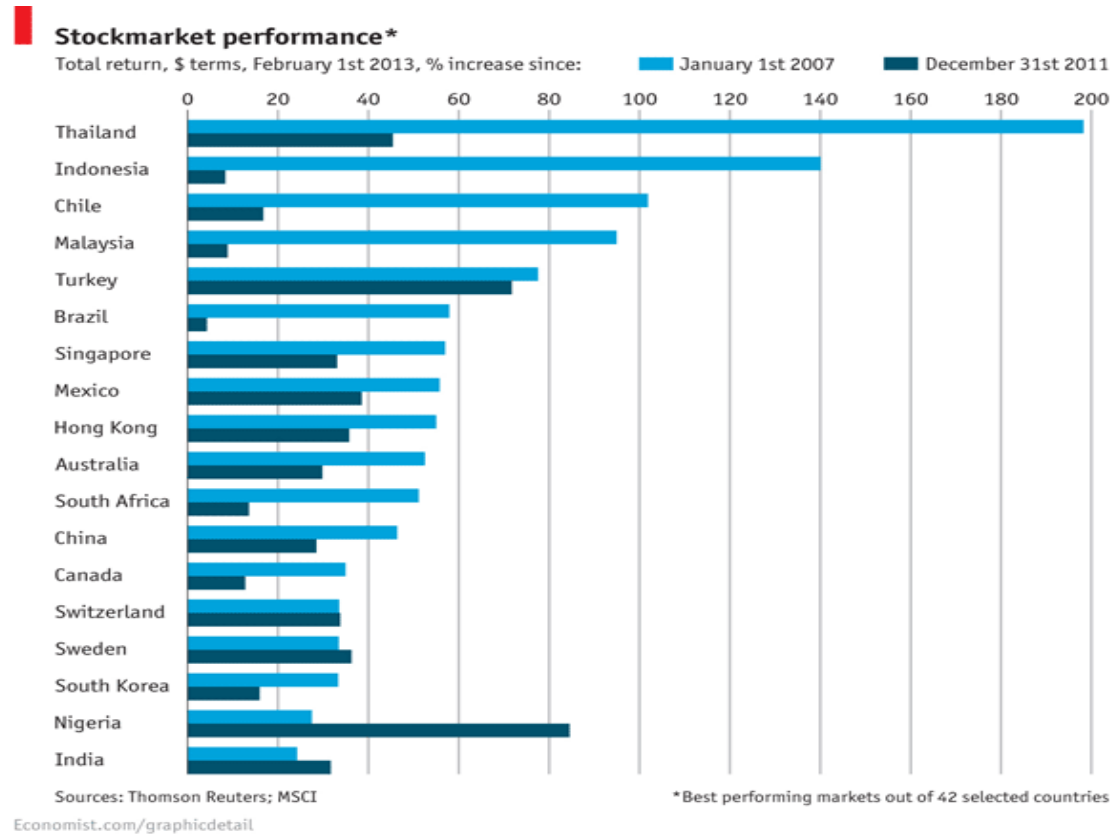
### **3.4 Applying Usability Methodologies to Security Metrics**

Developing security metrics tools is not a straightforward task because the requirements are not clear and the end users (decision makers) can have variant interests. Not all metrics matter to readers. Chief financial officers (CFOs) will want to know about cost and risk. Chief executive officers (CEOs) care about impact on reputation and profit. Chief strategy officers (CSOs) worry about all of these things and more. To cover

the needs of senior management, it is recommended that balanced scorecards include metrics that cover the four areas (Financial, Customer, Internal Process, Learning and Growth) to be useful and interesting for managers. Not only metrics selection important but also there is a need to consider how metrics are presented in the development process. This is done to obtain feedback from the users during development. This can be done using the rapid development cycle and involves prototyping and iterative usability testing (Jaquith, 2007).

### **3.5 Prototype Design Recommendations**

The visualization and design recommendations mentioned above should be applied during the prototype design. Jaquith (2007) gave some recommendations to create effective “mock-up” prototypes for scorecards. He recommended using a small number of metrics (20 to 25 maximum) that will fit on a single sheet of paper, with a simple design to enable users to understand them well without confusion. A good example is the style used in stockmarket graphs (see Figure 5). Jaquith (2007) recommended using the basic BSC perspectives (Financial, Customer, Internal Process, Learning and Growth), and general metrics that most people will use under each perspective. In the design there should be mixing between data and graphics with large white areas. It is also necessary to declare that this is a prototype and not the final scorecard by labeling the sheet clearly.



**Figure 5 An example of a clear graph from The Economist (2013)**

After preparing a prototype one can use low cost rapid usability engineering techniques to test the prototype. For testing usability, Kushniruk and Borycki (2006) introduced a low cost rapid usability method which depends on using a low cost and portable lab which consists of: (1) a computer to run the system under study on, (2) screen recording software which allows the computer screens to be recorded as movie files (with audio input of subject's "thinking aloud" captured using a standard microphone plugged into the computer), and (3) a digital DVD camcorder on a tripod or a ceiling mounted camera to video record user's physical interactions. The researcher shows the prototype to the participant and records participant's reactions and comments using the portable lab to get feedback about the prototype.



### **3.6 Security Metrics Scorecard**

A security metrics scorecard is a tool that helps managers in measuring security performance. The tool gives a clear view of how secure is the organization at a certain time and how secure it is, compared with other times or other organizations. Before starting to design the scorecard some information will need to be collected and clarified as outlined below.

#### **3.6.1 Score Card Audience**

Determining the audience helps in selecting specific metrics that will be useful for the user. In this work the audience is the information manager in the organization and are concerned about the security level of the organization and its impact on the overall performance as CIOs (chief information officers) and CFOs (chief financial officers).

#### **3.6.2 Major Organization's Objective**

After defining the audience the organization's objectives or the part of them that is related to security needs is determined, the suggested objective in this study will be (keeping the patients' data (PHI and PI) safe all the time and available when needed).

#### **3.6.3 Areas of Interest**

Security scorecards must be designed to ease the concerns of health care organizations regarding security. According to eHealth Ontario (2010) risk management is a main component in security programs. Risk management aims to minimize the likelihood of security incidents; it is concerned by determining vulnerabilities and how to mitigate them before causing any breach. (eHealth Ontario, 2010 ). The research of Park et al., (2010) proved that concept; after analyzing security programs in five hospitals they found

that vulnerabilities need to be determined and reviewed regularly, as well as incidents to prevent them and to overcome their impact on the system.

#### **3.6.4 What Metrics?**

Before designing the scorecard, the metrics that will be used need to be identified, as concluded from the previous point the main concerns in security programs in health care are the vulnerability (a weakness in system security) and incidents. Managers need to follow up on both statuses regularly. In eHealth Ontario (2010) there are definitions of the roles and responsibilities for information security employees; one of the responsibilities for information security managers is reporting threats and incidents, reporting threats can be done by reporting vulnerabilities that can enable these threats in the system. For information technology managers they need to report incidents and vulnerabilities. According to the audience selected, selected metrics need to be interesting for them and able to answer their questions, to help in decision making process. Metrics will be selected from the set suggested by CIS (CIS, 2010).

#### **3.7 CIS Suggested Metrics**

The CIS Security (CIS, 2010) established a consensus team of one hundred industry experts and put a set of twenty eight standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes. They gave metric definitions for six important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. In this work, metrics were selected to form a desired scorecard. CIS metrics were selected because they offer clear practical

definitions of security metrics based on data most organizations are collecting. This will make it easier, faster, and cheaper to implement a metrics program that supports effective decision-making. If many organizations adopt these metrics, they will be used as a standard and this will ease comparing security levels.

After reviewing the suggested security metrics and according to eHealth Ontario (2010), the two functions (incident management and vulnerability management) found to be directly related to the risk management process in addition to other metrics from different functions that support the security objectives. The metrics mentioned in CIS (2010), were classified into groups according to business functions (incident management, vulnerability management, patch management, configuration management, change management, application security and financial metrics); another classification for metrics was classifying metrics according to audience (management, operational and technical metrics).

### **3.8 Metrics Groups**

Metrics can be classified under the following groups, according to their business functions as outlined below.

#### **3.8.1 Incident Management**

Incident management describes the status of dealing with incidents by detection, identification, handling, and recovery. The collected metrics for this function are: number of incidents, mean time between security incidents, mean time to incident recovery and cost of incidents (CIS, 2010).

### **3.8.2 Vulnerability Management**

Vulnerability management describes the status of managing exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities. The collected metrics for this function are: percent of systems with no known severe vulnerabilities, vulnerability scanning coverage, number of known vulnerability instances, mean-time to mitigate vulnerabilities, mean cost to mitigate vulnerabilities. To make the scorecard more detailed additional business functions will be added which are application security and financial metrics as they include metrics related to the scope of the study as outlined in the next sections.

### **3.8.3 Application Security**

This function gives an indication of the efficiency of application security (CIS, 2010). The metrics that were collected are: number of applications, percent of critical applications and risk assessment coverage.

### **3.8.4 Financial Metrics**

Financial metrics show the details of spending on IT security. The metrics to be collected are IT Security Spending as percentage of IT Budget and IT Security Budget Allocation.

Classification of metrics according to audience will be as outlined below.

### **3.8.5 Management Metrics**

Metrics in this section are suitable for business management, as they display the performance of business functions and how this performance affects the organization.

The collected metrics for this function are: cost of incidents, mean cost of incidents, percent of systems with no known severe vulnerabilities, patch policy compliance, percentage of configuration compliance, percent of changes with security reviews and IT security spending as percent of IT budget.

### **3.8.6 Operational Metrics**

Metrics in this section are suitable for security management, as they display the activities of business functions, but may be too detailed for top management.

The collected metrics for this function are: mean incident recovery cost, mean-time to incident discovery, mean-time between security incidents, mean-time to incident recovery, mean-time to mitigate vulnerabilities, mean cost to mitigate vulnerabilities, mean cost to patch, mean-time to patch, mean-time to complete changes, percent of changes with security exceptions and IT security budget allocation (CIS, 2010).

## **3.9 Scorecard Design**

Comparing the first four functions in the previous section, and the last two functions, common metrics can be seen between the two groups. The common metrics are (cost of incidents, mean cost of incidents, mean incident recovery cost, mean-time to incident discovery, mean-time between security incidents, mean-time to incident recovery, percent of systems with no known severe vulnerabilities, mean-time to mitigate vulnerabilities and mean cost to mitigate vulnerabilities). These metrics were selected to be included in the scorecard in addition to other metrics if needed.

The scorecard was designed in the form of a balanced scorecard as it offers a well organized and comprehensive view for managers. The basic balanced scorecard (BSC)

includes four sections (financial, customer, internal, learning and growth) (Voelker et al., 2001). Thinking of these BSC sections in the terms of health care organizations, leads to the conclusion that it is better to keep the meaning of the sections, but to modify the names to be more acceptable and clear. CIS (2010) suggested other sections that they can make for a better alternative. For example, the term (Impact) in CIS (2010) means the effect of the security incidents on the organization which can replace the section customer in BSC as this effect will be directed towards the customers as well. Customers in health care situation may refer to patients, insurance companies and employees. The second and third sections are gathered under the name of (operations) and they display the performance of business functions by outcomes and by scope. These two sections form the internal part of the BSC. Finally, the (financial) part is kept under the same name. Learning and growth might be included in the financial part as spending on security personnel and training programs (Voelker et al., 2001).

In this work, the scorecard is designed based on the balanced scorecard system with some modifications, the four sections of the balanced scorecard mapped into three sections. These sections are impact, operations and financial. Those sections were selected in order to accommodate the needed metrics for security management in health care organizations as suggested by the researcher.

### **3.10 Impact Metrics**

In this part of the scorecard, the user will be able to see the effect of incidents on the organization in the current month and compare it with other months within a year. The metrics included in this section are described below.

### **3.10.1 Number of Incidents**

This metric gives the number of discovered incidents in the month of the scorecard, and as compared to the previous 11 months. It appears in the scorecard in the form of a single number for the current month and in the form of a time series chart for the monthly comparison (CIS, 2010).

### **3.10.2 Cost of Incidents**

This metric measures the total cost to the organization due to incident occurrence during the month (including the direct and indirect costs). It will appear in the scorecard as the number representing the cost of incidents in Canadian Dollars, and as a column chart for the costs that have happened during the last 12 months.

### **3.10.3 Mean-time between Security Incidents**

This metric measures the average time in days between security incidents. The unit is number of days (CIS, 2010).

### **3.10.4 Mean-time to Incident Recovery**

The mean time to recover from a security incident which is the time needed to analyze the incident, correct the system state to remove the harmful effect, and apply security controls to prevent the threat from happening again. The aim is to minimize this time as much as possible. The unit is in days. The last two metrics appear in one graph in the form of area chart indicating the mean time between incidents (blue) and mean time needed to recover from an incident (red) over the last 12 months. The more blue in the chart indicates a more stable system. The smaller red area represents more readiness to respond to security incidents in a timely manner (see Appendix A).

### **3.11 Operations Metrics**

This section of the scorecard shows how well business functions operate; the main function is vulnerability management as this one is of high importance to avoid any threats to the system and to keep the system working properly all the time, which is of high importance in health care as discussed earlier. Some metrics from the application security functions will be added as they provide a complete picture of the security status in addition to the vulnerability metrics (see Appendix A).

#### **3.11.1 Number of Applications**

This metric shows the number of applications in the system it helps the manager to understand the other metrics in the scale of the organization, viewed as a number (CIS, 2010).

#### **3.11.2 Number of Systems with No Known Severe Vulnerabilities**

The Number of systems that after vulnerability scanning that are found to not have severe vulnerabilities. The best value is equals to the number of applications, which means no systems have severe vulnerabilities (CIS, 2010). This metric appears in the scorecard as a number for the current month (see Appendix A).

#### **3.11.3 Vulnerability Scanning Coverage**

This metric shows the percentage of the systems that were covered by the vulnerability scanning process (CIS, 2010). The metric is classified as a technical metric but the researcher chose to include it as it might clarify for the managers how efficient is the vulnerability management in the organization, it appears in the scorecard as a percentage



for the reported month and as a time series in the monthly comparison area (see Appendix A).

#### **3.11.4 Number of Known Vulnerability Instances**

This metric counts the last known number of vulnerabilities in the system (CIS, 2010). The best value is zero, which means no known vulnerabilities in the system, or in other words, all known vulnerabilities were successfully mitigated. The metric appears in the form of a number in the current month area and as a bar chart in the monthly comparison area combined with the unmitigated vulnerabilities from previous month (see Appendix A).

#### **3.11.5 Mean-time to Mitigate Vulnerabilities**

This metric measures the average time taken to mitigate the known vulnerabilities of the system. The unit is hours or days per vulnerability and the best value is zero (CIS, 2010). It appears in the scorecard as a single number in the current month area (see Appendix A).

#### **3.11.6 Mean Cost to Mitigate Vulnerabilities**

This metric calculates the average cost needed to mitigate vulnerability and the unit is \$ CND per vulnerability (CIS, 2010). It appears in the scorecard as graph for cost per month (see Appendix A).

### **3.12 Financial Metrics**

The last part of the scorecard is the financial component, which shows the cost and allocation of the security budget, the selected metrics for this part are described below.

### **3.12.1 IT Security Spending as Percentage of IT Budget**

The part of the IT budget that was dedicated to security spending. It appears as four percentage numbers for four quarters of the year (CIS, 2010).

### **3.12.2 IT Security Budget Allocation**

This metric shows how the IT security budget is allocated to each category of spending. The categories included (products, services, training) in the scorecard and were selected as examples of the essential spending areas (CIS, 2010). Both metrics are recorded quarterly or annually according to the budget calculations in the organization, but they are included in the monthly scorecard for reference and guidance to improve planning and help in decision making.

## **3.13 Scorecard Visualization and Prototype Development**

The proposed scorecard should include all the metrics mentioned in the previous section. To present the metrics in a clear and attractive form, the researcher took into consideration the recommendations by Jaquith (2007) and Stabina (2005) reviewed in the section (prototype design recommendations) for visualization and design recommendations. In this section the design of the scorecard will be explained giving the reasons behind the selection of these design elements.

The balanced scorecard was chosen as a way of displaying security information as it arranges the metrics in groups, which makes it easier for the user to find the data easily and quickly. The balanced scorecard in this design consists of three major parts as described in the previous section: impact, operation and financial components. The scorecard is divided vertically in two sections the impact and the operation , and below

them appears the financial and comments. Horizontally, the impact and operation metrics appeared in two parts; the first part shows the metrics that describe the security status of the system in the current month as numbers for simplicity. The second part down shows a comparison for some metrics in the last 12 months. Each of these comparisons appears as a graph that displays the values of the metrics in the past 12 months. The graphs that are used are time series charts or column charts. The time series appears as simple lines and the column charts are 2-D with limited colors and lines for easier reading. Pie charts avoided in order to save space as well as to accommodate all metrics on one page.

Each one of the first four graphs (total cost of security incidents, number of security incidents, vulnerability scanning coverage and cost of mitigation) shows the way that the value of one metric changed during the last twelve months. The last two graphs show more than one metric. The first graph shows the mean time to incident recovery and the mean time between incidents. The two metrics are in the same graph and in the format of an area chart. The colors of the areas give an indication about security status, as it is better for the system to have a longer time between incidents (more blue in the graph) and shorter time to recover from incidents (less red in the graph). The other combined graph is the one that shows the known vulnerabilities and unmitigated vulnerabilities. The red part shows the unmitigated vulnerabilities so if the red color appears in large areas, the user should be alarmed. The last part is the financial part, and it is divided quarterly according to the budget. It shows in table form the percentage of IT budget allocated for security and how this budget is divided.

When users read the scorecard, they will be able to know the status of system security in the organization in the current month, how this status changed during the course of the

last year, and how the budget allocated for security has changed. This will provide the reader with information about any actions that have been undertaken to improve system status and the results of those actions.

## **Chapter 4 Study Design and Research Approach**

### **4.1 Methodology**

In this study, the researcher examined the acceptability and usability of a security metrics scorecard with number of experts working in health care organizations. The research method used was qualitative, as the researcher extracted the opinion of the participants about the scorecard and their views about security management in health care organizations (Jackson & Verberg, 2007). This qualitative research took place by interviewing participants and getting their reaction and feedback to the suggested scorecard.

### **4.2 Participants**

The main purpose of this study was to collect users' feedback and to test the usability of a security metrics scorecard. Individuals were invited to participate in the study if they were working in a health care organization and their work related directly to information security management in addition to being fluent in English. Based on Kushniruk and Patel's (2004) research the suggested number of participants is five to ten due to the law of diminishing returns as after this number saturation is reached. Saturation was reached when the usability tests and interviews no longer provided any additional information. In this work, eleven people participated in the study to reach saturation. The participants' job titles included : (director of clinical informatics, senior business analyst, director for

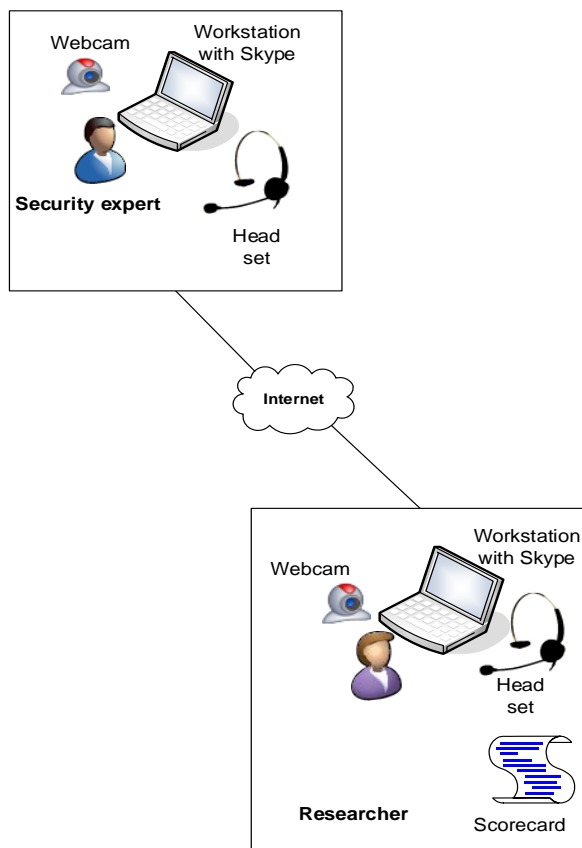
technology services and information privacy and security, nurse, system administrator, privacy officer, information technology, security information, communication, technology ISSM (information system security manager) and ISSO (information system security officer), clinical support person for training people on different issues including security, workflow improvement coordinator, information security officer, project manager and research ethics officer). The names of the participants and the organizations they work for were anonymized in this work for privacy and security purposes.

### **4.3 Recruitment**

To reach participants the researcher used a snowball sampling approach (Polit & Hungler, 1991). The researcher asked that an invitation email (Appendix E) be sent to the University of Victoria Health Information Science graduate student and Alumni listserv. In addition to this, the researcher posted information about the study on the Canadian Health Informatics Association (COACH) website and emails were sent to experts from the National Institute of Health Informatics (NIHI) website. When interested participants replied to the recruitment email expressing their interest in participating in the study, the researcher asked these individuals to pass on the study recruitment email to others, with instructions for those interested to contact the researcher directly about participating in the study (if they so wished). After receiving a reply from individuals expressing their intentions to participate in the study, the researcher emailed potential participants directly with information about the study, set-up a date and time for an interview and sent them a copy of the consent form (Appendix D).

## 4.1 Setting

The interviews were done using an Internet calling technology (i.e. Skype) as the subjects were located in different parts of the country. Therefore, on both sides (the interviewer side and the interviewee side), there was a need for a computer workstation connected to the Internet, a headset, and a webcam. The researcher used Skype features to share files as needed during the interview to share the questionnaire (Appendix B) and the scorecard prototype (Appendix A) to get the subject's feedback (see Figure 6). Also, the researcher used Camtasia Studio® to record the audio and video from the interviews, taking into consideration the consent signed by participants that stated clearly that the session will be recorded.



**Figure 6: Interview Diagram**

## **4.2 Data Collection**

After each participant replied to the invitation email (i.e. expressing an interest in the study, the researcher sent an email with the session details and attached the consent form (see Appendix D) asking the participant to sign it, scan it and send it back to the researcher. On the day of the interview, the researcher verified the consent with the participant and started the connection and recording. The first part of the session involved collecting information using the demographic questionnaire (see Appendix B). After this, a semi-structured interview (see Appendix C) about the usability of the system took place. The interview had three parts. The first part consisted of a set of general questions about the participants work experience in the field of security management in a health care organization. The second part involved usability testing of the scorecard prototype and then in the last part another set of semi-structured questions about the scorecard were asked.

### **4.2.1 Demographic Questionnaire**

The demographic questionnaire helped to obtain information about each participants' position and experience (Kvale, 2008). Collecting this kind of information contributed to the researcher's understanding of the differences in requirements based on differing user characteristics. The questions selected were in the form of closed ended questions as the participant selected only one answer from a suggested set of answers for each question (Salkind, 2006). The questions selected by the researcher were general demographic questions (GVU's, 1998), but adjusted to suit the purpose of the study. The



answer for question “What is your job?” was selected according to the classification of jobs related to the field of information security mentioned in Herrmann (2007).

#### **4.2.2 Interviews**

After completing the questionnaire, the researcher proceeded to the semi-structured interview with questions in the form of open-ended questions. The open-ended questions encouraged participants to give more specific and detailed answers and gave the interviewer the ability to add probes to the questions according to the received answers. Probes are the complementary questions that are not predetermined in the interview guide, but added by the interviewer according to the answers received to get more details about something in the answers (See Appendix C interview guide) (Given, 2008). The first part of the interview was about how security was being managed at the participants’ workplace, how they use metrics to measure security, and about the specifications of these metrics. After finishing Part 1 of the interview, the researcher proceeded to the usability study part of the study by sharing the scorecard prototype (Appendix A) with the participant.

#### **4.2.3 Usability Study**

In this phase of the study, the researcher explained the usability study by asking participants to walk through the scorecard prototype (Appendix A) pretending that they are checking it as part of their work. Participants were asked to think aloud and to give feedback, thoughts and suggestions for improvement. After finishing this part of the study, the researcher proceeded to the semi-structured interview and questions related to the scorecard (see Appendix C). The researcher asked what are the metrics the

participant thought were important, what are metrics that are not important and what should be added to the scorecard. The other benefit of asking the semi-structured interview questions was to get feedback about the format of the scorecard (i.e. to obtain information about users perspectives on the curves, tables, comparisons etc.)

### **4.3 Materials**

In this study the researcher used a questionnaire (see Appendix B) that was filled out by participants at the beginning of the session and a security metrics scorecard prototype (see Appendix A). The security metrics prototype was presented during the semi-structured interview component of the study. Both files (i.e. questionnaire and the prototype) were shared through the file sharing features in Skype (i.e. the Internet calling software). The researcher chose Skype because it is a popular, easy to use (even for people who have never used it) and free to call and share files and screens during the session. In some cases, this was an obstacle as some workplaces did not allow potential participants to use Skype. In such cases the participant used the technology from another site (i.e. from home). A questionnaire was used to collect demographic data about the participant's job and work experiences in the field. The scorecard used in the study was designed to be a general representation of a scorecard that included the basic metrics needed to know the security status of a health care organization.

### **4.4 Procedure**

The study steps were as follows:

- 1) Connect with the participant through Skype®.
- 2) Introduce the researcher, the study steps and verify the consent.

- 3) Share the demographic questionnaire and ask the participant to fill it in.
- 4) Start the semi-structured interview by asking the Part 1 questions (See Appendix C).
- 5) Share the scorecard prototype (see Appendix A) and ask the participant to think aloud while going through the prototype as they are pretending it is part of his or her daily work in checking on the security status of their organization.
- 6) Complete the interview questions in Part 2 (see Appendix C).
- 7) Finalize the session and disconnect.

#### **4.5 Data Analysis**

After finishing all interviews, the researcher collected the recordings of the sessions. Each session has data collected through the questionnaire questions, interviews and usability testing. The collected data were transcribed into a separate Microsoft® Word file for each session taking into consideration anonymizing any data related to the participants or their workplaces. The analysis of the collected data were done using a content analysis approach which is as the process implies coding the data and organizing the resultant codes into categories (Hsieh & Shannon, 2005). There are three different approaches to content analysis as described in Hsieh and Shannon (2005). Approaches vary according to the way the codes are selected. The one used in this work is the Conventional Content Analysis approach. This approach depends on extracting codes directly from data with no prior expectations or guidance (Hsieh & Shannon, 2005).

The coding process was done by extracting codes from the raw transcribed data, while reviewing these transcripts. The raw data was organized as answers to the interview questions in addition to the participants' thoughts in the part of the scorecard usability study, that resulted in codes related to the questions topics and to the design of the

scorecard, and this made the extracted codes follow the same pattern. After finishing the coding process, the occurrence of each code were counted to identify the emerging concepts.

#### **4.6 Ethics Approval**

The Human Research Ethics at the University of Victoria approved the request applied for this study on August 1<sup>st</sup> 2013 and assigned it Protocol Number 13-236. To reach more participants the researcher applied for modification to the approval from the Human Research Ethics at the University of Victoria to add the ability to email experts directly by sending the invitation email (Appendix E) to individuals who has the required experience and the modification approved on March 20<sup>th</sup> 2014. The researcher also applied for another modification to be able to ask specialized websites to publish a post about the research study on the website in order to reach more experts (Appendix F). That modification approved on April 25<sup>th</sup> 2014.

## **Chapter 5 Study Findings**

### **5.1 Introduction**

This chapter outlines the findings of the research study. The researcher will begin by presenting the analysis of the demographic data for the participants. Then the researcher will review the concepts and themes that emerged from analysing and coding the semi-structured interviews including direct quotes from participants to illustrate those concepts.

### **5.2 Characteristics of the Participants in this Study**

Eleven participants took part in the study. All participants were working in health care organizations and their work had a direct relation to information security management. Almost half of them, 45 % (n = 5), were females and 55 % (n = 6) were males. Their age is distributed as 27 % (n = 3) were between 26 to 40 years of age and 27 % (n = 3) were in the range between 40 to 50 years of age, 9 % (n = 1) was 50 to 55 years of age and the majority 36 % (n = 4) were more than 56 years of age.

Participants worked in the field of information security for differing numbers' of years: 18 % (n = 2) participants had less than 5 years of work experience in security, 45 % (n = 5) had experience in the range 5 to 10 years, and 36 % (n = 4) had more than 10 years. Similarly, in terms of their experience in the field of information security, while working in health care organizations, 18 % (n = 2) of participants had less than 5 years of experience, 55 % (n = 6) had experience between 5 and 10 years, and 27 % (n = 3) had experience of more than 10 years. Participants worked at differing levels of

management: 9 % (n = 1) worked in upper management, 27 % (n = 3) middle management, 18 % (n = 2) as support staff, 27 % (n = 3) administration staff and 18 % (n = 2) could not decide so they chose “Other”. Table 3 shows the participants demographics details.

Participant Demographics	Frequency (%)
Gender	
Male	6 (55)
Female	5 (45)
Age	
26-40	3 (27)
40-50	3 (27)
50-55	1 (9)
56>	4 (36)
Years in security	
< 5	2 (18)
5-10	5 (45)
>10	4 (36)
Years in security and health care	
< 5	2 (18)
5-10	6 (55)
>10	3 (27)
Role in industry	
Upper management	1 (9)
Middle management	3 (27)
Support staff	2 (18)
Administration staff	3 (27)
Other	2 (18)

**Table 3 Summary of participant demographics.**

For the participants’ jobs, it was hard for the participants to find the perfect match from the researcher suggested list, so most of the participants either chose other or chose more than one option from the list. The participants job titles included: “director of clinical informatics”, “senior business analyst”, “director for technology services and information privacy and security”, “nurse”, “system administrator”, “privacy officer, information technology, security information, communication, technology ISSM (information system

security manager) and ISSO (information system security officer)”, “clinical support person for training people on different issues including security”, “workflow improvement coordinator”, “information security officer”, “project manager” and “research ethics officer”. The majority of the study participants had considerable experience in the field of information security in health care organizations. See Table 3- Summary of participant demographics – for more details.

### 5.3 Semi-structured Interview Data

The eleven interviews were transcribed and analyzed using a content analysis approach. Data were coded using selected terms from the security management and scorecard literature. These codes were then grouped into thirteen categories, which were classified into four major themes as shown in table 4.

Themes	Categories
Managing Security in health care	Technical security Information security Standards and guidelines
Security metrics scorecard	Security metrics User acceptability and usability Audience oriented
Security metrics evaluation	Impact metrics (Security breaches and Incidents) Operation metrics (Vulnerabilities) Financial metrics
General recommendations for improvements	What metrics are good What metrics are irrelevant additional metrics suggested visualization and structure

**Table 4 Categories of semi-structured interview findings.**

The findings from the study will be discussed in the rest of this chapter in terms of how they were coded and classified according to the sections in the table (Table 4 Categories of semi-structured interview findings).

#### **5.4 Managing Security in Health Care**

The objective of information security management is to protect sensitive information while providing and delivering data at the proper time and place (Ashenden, 2008). In health care environments, sensitive information includes personal, medical and financial data. Some of this type of data may need to be available to and is necessary to saving lives. Some participants in this study worked only in health care organizations while others worked in other types of organizations before working in healthcare. All of the participants agreed that health care organizations should have a very strict security system that provides more security than other types of organizations.

More security means more information and more details about incidents as stated by participant 5:

“it need to be more secure more strict, more information, like in case of incident you need to know who’s affected , why is affected, and if anybody else involved, how to prevent it again in the future” (Participant 5).

Another participant described “security” in health care as “more granular”:

“more granular, like all organizations have access controls to the documents , but in health care not only access control to documents but also access control to information within documents so it’s more granular and more specific” (Participant 6).

Complexity is another property that makes health care organizations need stronger security systems.



“it’s too complex because there’s so many pieces and so many different systems all talk to one another now it’s so messy, It’s crazy, its horrible enormous and complex, I mean the whole , the security business is got busy and so difficult” Participant (7).

Many participants referred to consequences of incidents in health care that can be huge and can lead to dangerous results such as losing lives so avoiding these situations is a necessity. In analyzing the interview data about security management in health care organizations three main themes, which are technical management, information management and following standards, laws and guidelines emerged. The themes will be discussed next.

#### **5.4.1 Technical Security**

Technical security is the part of security management, which involves the servers, networks and devices used within the network. Most participants 82 % (n = 9) mentioned “management of servers and networks” as a main part of security management process in their organizations. This type of security management depends on monitoring networks for viruses and malware, setting up firewalls and checking the network to make sure it is available in every spot in the organization, and checking to see if there are any unknown wireless networks available.

“We do , monitor people’s workstations and computers they have access to it and everything, of course we monitor for ... , we have software on the computers to monitor for viruses , malware and that kind of stuff” (Participant 5)

This also includes monitoring the network traffic computers and internet usage:

“From a technical side they pay attention to traffic so even if you aren’t necessarily being attacked now , seeing changes in pattern of your traffic telling perhaps there is somebody is trying or thinking about attacking your system, I know they are paying attention to that” (Participant 9)

“Investigations of the usage of the internet and usage of access to files and documents on the network and so. These and computers as well, we do actually monitor the computer usage” (Participant 3)

To ensure confidentiality not only do the network and the computers connected to the network need to be monitored but also USB ports and CD's need to be disabled to prevent data copying.

“Another level of security and that is we turned off all the USB drives in all computers period. We also turned off the right to access for all the CDs so people couldn't write cd's of data and take it home” (Participant 7)

From the above discussion, it is clear that managing technical security is mandatory, it includes managing servers and networks, monitoring traffic and controlling personal devices.

#### **5.4.2 Information Security**

Information security involves the process of managing the security of information in the organization by having a clear policy and monitoring compliance with that policy throughout the organization (Sloms, 2004). To apply a policy, organizations need to enforce access control, and to check compliance. They have to audit information activities and monitor for breaches.

Participants referred to having security policies in their workplaces:

“there are policies coming from our organization that govern like a several security policies, and on regular basis we audit systems for access to information, and when we see a potential security breach we have a process to follow up on them” (Participant 1).

“we do have a privacy and security policy” (Participant 2).

“We have the documented policy procedures” (Participant 6).

As information sharing is vital in health care so is access control. Access control is important as it ensures the right information is available only to the right people. Role based access control can solve this problem. 73% (n = 8) of the participants referred to having access control which is based on the roles of the employees in the organization.

“what we have is role based access to that information.” (Participant 1)

“we need to do the least privilege the least access possible to do your job we keep an eye on that people change jobs and you need to change their privileges.” (Participant 9).

“the clinical system that I work with had quite few levels of security built in to them so just for instance you couldn’t get to any information unless you had a right to get there more importantly you couldn’t write orders or prescribe drugs unless you had a menu. Given various menus what is called user class.” (Participant 7)

To monitor the policy compliance and security of the information there must be an audit system that records transactions by system users. These audits are reviewed regularly to detect any inappropriate access to information as illustrated by the quotes below:

“On regular basis we audit systems for access to information, and when we see a potential security breach we have a process to follow up on them.” (Participant 1)

“At the health centers, who logged to the system what time what records did they view, how long they in the record this is an application level security and then we have network level security where who had accessed to the network, what time did they launch the application.” (Participant 6)

“We do lot of auditing and we use that auditing to make sure we don’t have holes.” (Participant 9)

Initial training for new employees and regular training for current employees was identified by participants as being essential to making sure they are aware of all the rules and restrictions. Security information system will never work well without an awareness program for the system users (Sloms, 2004). Sometimes there is a need for training after a security breach happens to avoid such incidents in the future. 46 % of the participants (n = 5) referred to training as an important part of security management in their organizations as people are the weakest link in the security systems. This is best illustrated by the quotes below:

“that training occurs at least yearly , there is people who keep track of that and again you can’t give people access unless you confirm their training updated.”  
(Participant 7)

“you need a training program for access for everybody uses the system.”  
(Participant 11)

“Typically that is the key thing in prevent the information security breaches and violations you need to make sure that your end users are educated appropriately.”  
(Participant 3)

“for example we require that everyone has to do initial training before granted access to the system they must maintain it annually.” (Participant 9)

According to participants, information security management in health care includes policy compliance, access control, regular reviewing of audit trails and continuous training for employees to ensure awareness.

#### **5.4.3 Standards and Guidelines**

Information security management is considered a process and process models and rules can be applied to such systems (Huang et al., 2008). This process should be governed by laws and regulations for privacy and information security, especially in the case of health

care due to the sensitive nature of the personal and medical content contained within these systems. In Canada there is PIPEDA ( Personal Information Protection and Electronic Documents Act) which is not specific to health care but for personal information in general, so health care organization security management teams apply more than PIPEDA by checking the governments' laws and acts related to health care information security as described by one participant in the below quote.

“There are applicable laws that can fit, PIPEDA doesn't specifically apply to health information we adopted a lot more than PIPEDA because it has gaps that data that PIPEDA does address so we did environmental scan. We looked across the country to see what different laws and regulations like BC. Primarily BC, Saskatchewan Ontario and Manitoba whatever the high standard was across the provinces or the federal, whatever the high standard that our standard we adopted.” (Participant 6)

In the United States there is Federal Information Security Management Act of 2002 (FISMA, 2002) and the National Institute of Standards and Technology) (NIST) 800 series (NIST, 2014), which is a set of publications that address these computer security topics.

“FISMA states what documentation we have to have in place a generic sort of set of standards because it's really hard to put into law that what technical standard is. As you know it is changing so rapidly, so the biggest thing is we generally follow NIST guidelines we pretty much the entire 800 series for how to create an information security plan, and how to do risk assessment , contingency plan, disaster recovery , all of this follows the 800 series.” (Participant 9)

In Canada it varies from one organization to another some use International Organization for Standardization (ISO) publications for security management (ISO/IEC 27000-series) and risk assessment (ISO 31000), in addition to recommendations from

organizations like Canada's Health Informatics Association (COACH). According to participants, security teams also apply provincial laws and recommendations. They also check for industry best practices to adopt what can be applied in their workplace. As described by two participants below:

“We based specifications on ISO guidelines also industry standards and organizations like COACH.” (Participant 1)

“The approach we take is different it is based on I suppose three main areas the OCIO (the office of the chief information officer) in the province. We follow the security standards which is online available publicly online all those based on ISO 27 and also all the related industry best practices, it can be a combination of thing.” (Participant 3)

Security and privacy of health care information is governed by general regulations such as PIPEDA, FISMA, ISO/IEC 27000-series and NIST. The selection of regulations depends on the governmental obligations and organizational preferences.

## **5.5 Security Metrics Scorecard**

In this section, the researcher reviews participants' ideas about security metrics and this includes what are metrics collected in their workplaces, and their first impression and general comments about the developed scorecard prototype introduced during the interviews.

### **5.5.1 Security Metrics**

To manage security there must be metrics collection and comparisons. By asking the participants about the metrics they collect regularly, their answers were not clear or specific which gave an indication that the term “metrics” is not widely used in their workplaces. After more discussion, while reviewing the scorecard sheet, participants

discovered other metrics they collect routinely or they came up with new metrics they would want to start collecting. Some participants referred to the audit review as part of metric collection as described below:

“On regular basis we audit systems for access to information, and when we see a potential security breach we have a process to follow up on them.” (Participant 1)

“who logged to the system what time what records did they view, how long they in the record this is an application level security and then we have network level security where who had accessed to the network, what time did they launch the application.” (Participant 6)

“I report metrics, like how many time be on a record how many times you find somebody who do something he shouldn’t you see running into malicious issue how many times people doing things that they shouldn’t, unless we don’t have incidents the result from that it’s just rolled up into general information security auditing and compliant.” (Participant 9)

Other participants were interested in breaches and violations. They wanted to know the details of breaches and violations, in addition to the audit tracking. This is best illustrated by excerpts from participant 2 and participant 3’s interviews below:

“Number of uses, number of sessions being used, the number of breaches, information security breaches and types and also description of them, these are probably the basic metrics that we capture for security, that also may be actually projects like sort of things being investigated in ongoing issues.” (Participant 2)

“The current security metrics which we collect regularly are typically around breaches and violations of a security policy. So that can be anything from a lost or stolen mobile computing devices, which is a lab-top or blackberry through to phishing attack and malware infection, so typically the metrics we collect around those types of incidents in general is what we collect on these areas. Another type of a metrics which is related to investigations of the usage of the internet and usage of access to files and documents on the network and so these and computers as well we do actually monitor the computer usage.” (Participant 3)

The initial description of security metrics in health care organizations by study participants was generally about reviewing audit and breach details. More in depth discussions about specific security metrics will be discussed in the following sections.

### **5.5.2 User Acceptability and Usability**

The general reaction from the participants was positive. Most of them liked the idea of having a scorecard for the workplace:

“Conceptually the idea of the scorecard is a great idea it gives you quick update on where things up.” (Participant 1)

“The idea of having a scorecard that reflects how secure your system are not a bad idea.” (Participant 8)

“My response will be: most management would love something like this, because it reduces it to thing they can grasp a little bit better.” (participant 9)

“It is nice, clear and precise, shows you exactly what you need to know.” (Participant 5)

“Visualization is good, I mean its simple managers like the pictures.” (Participant 6)

The participants liked the one page format, but to improve the usability of the scorecard they recommended having another page (maybe on the other side of the page) to include a clear definition of the terms used in the scorecard, so the user can find it easily whenever needed.

Other participants were worried about the accuracy of the data and the possibility of calculating some fields precisely. They asked for the data to be accurate and current so that managers can make the right decisions based on the scorecard data.

All major points from the participants’ comments will be discussed in the rest of this chapter.



### 5.5.3 Audience Oriented

To design an effective scorecard for an audience such as scorecard users'. The users' interests must be taken into consideration, (the researcher referred to that in section 3.7). While designing the prototype, the researcher oriented the scorecard towards a management focus with some operations metrics. This design lead to comments and more extensive discussion where the participants were concerned. Participants believed managers were interested in incidents and everything related to security breaches. Manager interest would also include cost, while technical people would be interested in operation metrics. Clinical people would want to see the effect of security incidents on patients. Participants considered financial and technical information irrelevant for example:

“Hi-level management are interested in the number of incidents, the type of incidents, the cost about incidents and the cost to mitigate as well and all auditors would be into and risk management folks will be interested in what is the residual risk after implementing mitigation strategies so what is the risk that left.”  
(Participant 3)

“well it depends who you are showing this to if for example the tech folks, chief technology officer may be very interested in the cost but for clinical side like clinical information achievement clinical informatics officers they are going to look at this and say it's useless it doesn't tell me anything, I think for an organization looking will be impact on patient care is far more meaning than statistics like if treatment were delayed or surgery were cancelled or mistakes were made, errors were reported I think that's far more important than the cost.”  
(Participant 1)

“you may need to design different scorecard for different people, so the manger would want to see something that probably the technical side not going to need to see.” (Participant 8)

The audience of scorecard defines the metrics needed. In this research the audience is the security managers, in the rest of the chapter, the favourite metrics for managers will be discovered.

## **5.6 Security Metrics Evaluation**

In this section, the researcher reviews the participants' feedback regarding the metrics suggested in the scorecard prototype. Feedback is categorized under three sections as they appear in the scorecard sheet in three sections (Impact, Operation and Financial).

### **5.6.1 Impact Metrics (Security Breaches and Incidents)**

The impact part of the scorecard was the most popular among participants as all of them showed interest in reporting incident details. Security Managers always need to know the status of incidents in the organization and the effect of these incidents on the assets and work. In healthcare, the effect on patients' health and privacy is crucial too as described by participant below:

“Definitely like the impact identification because it is important for an organization to understand what the impacts are especially in terms of financial impact.” (Participant 3)

Participants discussed the metrics in the impact section and asked for modifications and more related metrics as will be explained in the next section of the Findings chapter.

The impact section of the scorecard prototype is divided into two main parts (see Appendix A). The top part of the scorecard prototype contains the metrics that reflect the status of incidents in the organization for the current month. The lower part of the scorecard shows graphs that compare some metrics during the last 12 months. The first

part has four metrics; the participants' feedback about each metric will be discussed next part of this chapter

### ***Total Number of Incidents***

The total number of incidents is a main metric that every security manager needs to know, so it is already collected in organizations explicitly or as part of incidents in a detailed report as described by three participants below:

“number of incidents is fine that's not a problem as we already reporting that but really what is the outcomes is the biggest thing.” (Participant 1)

“Number of security incidents over each month yeah I think that's relevant.” (Participant 3)

“so the total number of incident , that is great we do as well.” (Participant 7)

Participants indicated that the total number of incidents is a metric that health care organizations collect.

### ***Total Cost of Incidents***

Total cost of incidents is one of the cost metrics that participants have different opinions regarding them. Most participants think it is good to know the cost of incidents while other participants who are interested more in the clinical side of security were against having cost in the scorecard, as they preferred to see metrics related to the incident's effect on patients rather than the cost of an incident as described below:

“Total cost of incidents its interesting I don't think we looked at that yet.” (Participant 2)

“Total cost of incidents is good I know the managers like to see numbers, money anyway.” (Participant 5)

Some participants were interested in the total cost of incidents but believed it would be hard to accurately calculate incident costs (incidents can happen during a specific month and can increase with time so the number of incidents might be misleading)

This is described by two participants in the below quotes:

“Another thing I see the total cost, the problem is you actually you don’t know the total cost until down the road a bit because you don’t know for instance.”  
(Participant 7)

“to me it would be very difficult to calculate cost I don’t know if that is of any value.” (Participant 8)

The solution to this problem can be adding the term current to “total cost” to become “current total cost” or to add a comment explaining that the total incident cost can change in the future.

### ***Mean Time***

“Mean time” is another metric. Mean time can be defined as the average time needed for specific event, for example the mean time between incidents is the total time between incidents divided by the number of incidents. That metric “mean time between incidents” was not clear to participants on the scorecard. The term “mean time” was not clear for some participants so they asked for clarification regarding the term. Also many participants asked to classify the incidents so in this case mean time between incidents must be modified to present different classes of incidents to improve clarity of understanding of the metric for participants. This is best illustrated in the quotes below:

“Mean time between incidents, I wonder if it is more to look at maybe on a given day maybe a whole bunch of incidents versus different data monthly so maybe more than monthly or weekly.” (Participant 2)

“an interesting statistic you have mean time between incidents so that is kind of interesting to me to understand you know how often something is happening and why.” (Participant 4)

The last metric in this part of the scorecard prototype is mean time to recovery. Many participants (46 % n = 5) provided positive feedback about this metric. Mean time to recovery represents the time needed to overcome the incident effect. Participants thought it is important to have this metric in a monthly scorecard as indicated by the excerpts from two participant interviews below:

“The meantime to recovery I think is really important.” (Participant 2)

“Meantime to incident recovery that is important.” (Participant 5)

Participant 7 was worried about accurately calculating the mean time to recovery (if the metric was included, the time needed to resolve human issues as law cases) and such issues related to security breaches in health care organizations as illustrated by the statement:

“mean time to recover that’s you have to have a longer view that’s what people don’t get it they don’t appreciate it, there’s long term issues here that can take a long time to sort themselves up.” (Participant 7)

All of the above metrics appear in the upper part of the scorecard, which shows the status of the security in the organization during the current month. The lower part of the impact section (see Appendix A) is about highlighting the change in some metrics through the latest twelve months. There are three graphs in this section. The first graph shows total cost of incidents in 12 months, and as participants found the “total cost of incidents” metric is important, they have the same opinion about the graph, as it will show the distribution of incidents over a period of months so the organization can find

patterns in the attacks if there are any. Participants found this part of the scorecard interesting and relevant as outlined below:

“the total cost graph is interesting.” (Participant 2)

“so the past 12 months telling me the total cost of security incidents, I like the breakdown on a monthly basis , so you can track the trend of the security incidents over a monthly basis so for instance times in a real organization where the incidents specially for incidents related to phishing attacks over summer and into the fall in our organization seems to be the highest months for phishing attacks so that chart in our organization would show more incidents through those months due to phishing attacks if you wanted to drill down into that and now you could trend that each year trying to understand where potentially which month present the most risk” (Participant 3)

The second graph on the scorecard provides information about the number of incidents in the last 12 months. In some cases participants asked for modifications to this graph such as showing the incidents using a classification system, or by adding the effects of the incident on patients to the graph as described in the following participant quotes:

“Number of security incidents over each month, yeah I think that’s relevant.” (Participant 3)

“So if you are able to match that to number of incidents with reported patient effect that will make a very strong scorecard.” (Participant 1)

The last graph is the one with two curves with a mean time to incident recovery and a mean time between incidents described (see Appendix A). Some participants thought it was confusing to have these two graphs together as illustrated by the below quotes:

“I can sort of see the bottom left mean time to incidents recovery mean time between security incidents. I have a suspicion that is not important, or just keep the incidents recovery one. I think for most people the number of incidents in a course of 3 months if the number is getting bigger or smaller that’s all you really need to know and you want to pay attention to, not necessarily in a chart form.” (Participant 9)

“I think on the bottom left there is mean time to incident recovery , mean time between security incidents are confusing statistics, maybe misleading, You don’t know what the long term effect of any given incident may be.” (Participant 7)

The participants worried that the calculation of recovery time might not be accurate according to the nature of the incidents’ impact and that the calculation may appear only after time has passed. A participant recommended adding a comment clarifying this point to avoid confusion for those using the scorecard.

### **5.6.2 Operation Metrics (Vulnerabilities)**

On the right side of the scorecard, the operation metrics appear (see Appendix A). These metrics might be of more importance to technical people as suggested by the interview data. For example, some participants thought it was totally out of scope of their interest to look at operations metrics while others chose to keep some of these metrics but not all of them as will be discussed in this section. The following participant quotes illustrate these differences of opinion regarding operations metrics:

“It looked to me what’s here is technical thing and not too much actual breaches or inappropriate access to information if I’m managing something it’s not really a concern of mine to know if the system is vulnerable because it is technical issue I’m more concerned about inappropriate access or inappropriate sharing of information.” (Participant 8)

As explained above, the impact side the operations part of the scorecard is divided into an upper part with the metrics values for current month and a lower part for comparison over a 12 month period (see Appendix A).

The first metric in the current month section is the number of applications, which is good for some participants as outlined in the below excerpts from the interviews:

“the operation number of applications, which is really cool.” (Participant 2)

“we probably want to identify number of systems not application , we prefer systems than applications.” (Participant 3)

“Number of applications in the system that would be interesting.” (Participant 4)

The next metric is the Number of Systems with No-Known or Severe Vulnerabilities which seemed to be of no importance to all participants. Rather, participants preferred to see the number of vulnerabilities that were present. Most participants thought that (Vulnerability Scanning Coverage) is a very technical metric and not suitable to be included in a scorecard for managers, as managers are not interested in the technical details. In addition, if the managers were more interested in the clinical side, this metric would be very irrelevant. These beliefs are described in the excerpts below:

“Vulnerability scanning coverage, not of reality in healthcare, we don’t have that today, and probably we wouldn’t in any case other organizations might be different but definitely in health care no.” (Participant 3)

“Vulnerability scanning coverage, it doesn’t stand out, for managers.” (Participant 5)

The Number of Known Vulnerabilities metric was not favorably viewed by most participants. Even so, some participants suggested classifying vulnerabilities according to severity or source of vulnerability as illustrated by the participant quotes below.

“We don’t record or track this kind of statistics number of known vulnerabilities.” (Participant 3)



“Total number of vulnerabilities that would be good too like a breakdown if its workstation vulnerabilities or intrusion like if the users themselves are doing something or its attacks coming in.” (Participant 5)

Most participants ignored the Mean-Time to Mitigate Vulnerabilities metric as it is a very technical area of health informatics work so they perceived it as irrelevant to the scorecard. The Total Cost of Mitigation was noted by some participants. Here, some participants tended to use the term as a way of thinking about how to mitigate incidents rather than vulnerabilities. While other participants wanted more details on the way money spent. Some participants worried about the accuracy of the numbers so these participants suggested that using the term “current cost” would instead give a better indication of the number shown (and how the number is not firm and can change in the future if there are new inputs) as described in the below quotes:

“I think the cost of mitigation when we do look at our incidents we do if any significant incidents do occur we have to go through incident management process and from there we build a recommendations for future mitigation and that could be either additional education, communications or it could be additional technology controls if it is additional technological controls if it is.” (Participant 3)

“total cost of mitigation, that’s really great to see what money is going like you buy more hardware or software or is it more people that you give to ease that sort of stuff again the question is doing hi level summary so this is great.” (Participant 2)

“computing the cost of mitigation I think can be very challenging and I would be skeptical when I look at that data want to be sure you considered all the variables and its hard you know health care specially it’s too complex.” (Participant 7)

“It’s a moving target you might need to say something like current number of vulnerability Current cost of mitigation.” (Participant 9)

The operation metrics as discussed above appear in the upper part of the scorecard that show the security status of the organization in the current month. The lower part of the scorecard has graphs that show how the metrics have changed in the last 12 months (see Appendix A).

The first graph in this part of the scorecard shows the metric (i.e. vulnerability scanning coverage), which is discussed earlier. Participants recommended this graph be omitted unless there is specific need to track this metric; for example, when the scorecard metric is changing rapidly from month to month for example

The second graph (cost of mitigation) is also based on a metric that appears at the top part of the scorecard. A participant found this useful as described by the following quote:

“Cost of mitigation a great chart definitely a good metrics, as it highlight the financial impact to mitigate the incidents been identified” (Participant 3)

The last graph provides information for two metrics (unmitigated vulnerabilities) and (known vulnerability). One participant recommended having only the unmitigated, as managers need to know the risk sources

“I think the chart with unmitigated and the known vulnerabilities, it’s better to know only the unmitigated and just watching that going up and down, In other words, I need to know what to worry about” (Participant 9)

The operation metrics part of the scorecard was very controversial. Operation metrics are technical in nature so it might not be interesting for managers. Some metrics were totally rejected by the participants like “vulnerability scanning coverage’ and some metrics were acceptable such as “number of applications” while other metrics were

considered to be more useful such as “cost of mitigation”. Here, participants suggested using this metric as the cost of mitigating incidents instead of vulnerabilities.

### **5.6.3 Financial Metrics**

The financial metrics in this scorecard consists of two main parts presented in the form of tables in the lowest left part of the scorecard (see Appendix A). The first table has the security budget as a percentage of the IT budget. The second table provides information about how the security budget is allocated between the three sections: training, service and products.

Some participants were happy with the design as is. They expressed that as illustrated in the quote below:

“That’s sort of nice to see where the security addressed and the financial part of IT budget.” (Participant 2)

Other participants were interested in the effects on patient care directly, although they were not interested in the budget part of the scorecard as indicated in the quote below:

“we have no control over cost because as a protector on health information its more around what does that actually mean in terms of impact of that information so the financial piece is totally irrelevant.” (Participant 1)

“for the financial part I wouldn’t have any input as a clinician.” (Participant 4)

The participants thought the budget section was important, but that it needed modifications to the way the information was represented. Participants showed more interest in the incidents’ cost as illustrated by the below quote:

“The financial, in that format is probably not the right format ,as an organization we will definitely want to see costs with an incident so the table is irrelevant for our organization and would not be used, but definitely the costs of an incident” (Participant 3)

“% of IT budget is only part of the puzzle; you may have thought about how estimating the cost just based on IT budget is not going to be reading the whole”  
(Participant 7)

“you know what the budget is, it looks like a pre-set budget and I don’t know if that’s of any value that information unless the person was hoping to change it and you were finding in changing our own target but if not it is kind of redundant”  
(Participant 8)

The financial metrics were seen by different participants in different ways, some of them liked how the financial metrics were presented, others were not interested in financial metrics altogether. Another group suggested adding Incidents’ cost as a part of financial section.

## **5.7 General Recommendations for Improvements**

The main purpose of interviews was to obtain feedback from experts about the proposed scorecard in order to extract their views and interests where the tool is concerned. In this section of the findings chapter, the researcher outlines the feedback under the three sub sections to present what metrics the experts agreed on, what metrics are not important or can be removed and what important metrics were missed in the design. In addition to this, participant feedback about the design and visualization of the scorecard will be presented.

### **5.7.1 What Metrics are Good?**

The scorecard was discussed with participants. Participants were asked about what parts of the scorecard they thought could be used in their organizations by the researcher. The participants answered the question, identifying the most favorable or the most needed metrics in their workplaces. The top favorite among the incidents metrics with 73 % (n = 8) of participants noting this to be an important metric was to show the number of

incidents. Participants identified the number of incidents as the most important metric in the scorecard for people with clinical and non-clinical interests. In addition to this, some participants asked for the number of incidents to be classified to show the different categories of incidents according to severity. After the number of incidents metric, the cost of incidents and (56 % n = 6) mean time to incident recovery (46 % n = 5) were considered to the most important metrics to report in such as scorecard..

From an operational perspective the top security metric was the cost of mitigation (36 % n = 4). Here, participants wanted mitigation to metric reporting to be restricted to incidents rather than vulnerabilities. Participants also wanted a definition for vulnerability definition to be used in conjunction with the metrics that report on incidents as illustrated in the below quote:

“Cost of mitigation a great chart definitely a good metrics, as it hi light the financial impact to mitigate the incidents been identified” (Participant 5)

Participants’ interest in incidents details appeared clearly in their selection of the favourable metrics in the scorecard, as they agreed on selecting incidents related metrics.

### **5.7.2 What Metrics are Irrelevant**

Most participants believed metrics from the Operations section to be irrelevant to their work. Participants identified that these metrics are technical metrics with details that may not be important to managers. The top unwanted metric was the vulnerability scanning coverage (55 % n = 6) as shown in the participant quotes below:

“It doesn’t stand out, for managers.” (Participant 5)

“Vulnerability scanning coverage, not of reality in healthcare, we don’t have that today, and probably we wouldn’t in any case. Other organizations might be different but definitely in health care no.” (Participant 3)

Some participants linked including this metric by the need to track it, for example if its' value changes a lot and managers need to know about that" then the metric should be included as outlined by one participant in the following quote:.

"I'm not so sure about vulnerability Scanning coverage, unless this kind of moves a lot. I mean if for instance I was just started to do this and I wanted to track I was making sure getting more and more that would be good, but by the time you can probably reach 90-100 % which is almost flat line at some point so that will not be as relevant." (Participant 9)

Other participants believed that some metrics could be removed such as the number of known vulnerabilities (36 % n = 4). This is illustrated in the quote below:

"We don't record or track this kind of statistics, number of known vulnerabilities." (Participant 3)

This was the same for participants when the number of known vulnerabilities in the graph with unmitigated vulnerabilities was discussed. Participant 9 thought there is no need to know about the number of vulnerabilities present as described in the quote below:

"Not necessarily in a chart form , I'm not sure but I think the chart with unmitigated and the known, it's better to know only the unmitigated and just watching that going up and down, I don't care about it if the door is locked what I want to know is the door is open. In other words, I need to know what to worry about." (Participant 9)

In terms of the impact metrics some participants chose the mean time between incidents (36% n = 4) to exclude from the report care as this metric would be difficult to calculate it accurately as outlined in some of the following participant quotes:

"mean time to incident recovery, you've been told that it's all taken care of , and then you find out they fixed three of the four machines but they didn't fix the fourth one, so the incident isn't really over, so what to do, how to go back and

reset the data ? You just have to be so careful that people are not misled by the numbers” (Participant 7)

A participant suggested that if this metric were to be included there must be a comment to indicate if the numbers have changed in response to their being an update to the data or new data being added. Participants with clinical backgrounds identified several financial and cost metrics that could be removed from the scorecard. 18% (n = 2) of participants with clinical backgrounds suggested they wanted to see information related to patients’ safety and confidentiality (regardless of the money spent to address security issues). Two participants refused to remove any metrics from the scorecard. Instead, they believed all metrics should appear in the scorecard. Lastly, one participant chose to remove budget percentage (9% n = 1) spent on incidents from the scorecard as shown in the quote below:

“Budget % is irrelevant because the numbers might be differs from year to year and month to month depending on how plan on, instead of having the percentage for the year I would tie to percentage of everything, that I think would be more useful.” (Participant 6)

This section presented the participants selections for the least favourable metrics, or the metrics that should be removed from the scorecard, most of these metrics were related to vulnerabilities as the participants thought these metrics are out of managers’ interest.

### **5.7.3 Additional Metrics Suggested**

As all participants agreed that, the metrics related to incidents are the most important in the scorecard. Participants asked for more related metrics to be added to the scorecard. The top suggestion was having a classification for the incidents (63 % n = 7) included in the scorecard. Incidents varied in severity and effect for an organization so participants

believed it does not make sense to represent all incidents summed equally in the number of incidents metric.

Participants suggested classifications could be done according to the source of an incident such as in the case of incidents being classified according to human, related architectural or technological incidents. Participants also suggested classifying incidents according to their severity as outlined in the below participant quotes:

“if we have for instance [province] [health], [name of ] health authority an incident a critical incident classification metrics so from a p1 incident to a p4 incident so p4 p3 typically can be low priority and not that important for us to address right away. Definitely p1 or p2 incidents which is perhaps impact on a whole facility or risk a patient care requires immediate attention.” (Participant 3)

“Knowing the number of security incidents is helpful but you need to know what the types of incidents.” (Participant 7)

“If they could see a breakdown of the types of incidents so whether you are talking about someone accessing a system inappropriately or whether they lost their laptops or, I don’t know how all these types of incidents are defined but I think it will be of great value if you can breakdown the type of incidents.” (Participant 8)

“I think it would help but I think needs more, explanation of incidents, what the scale it be like severity of the incidents as we do electronic medical record in that case any breach or any incident depend on what it is. The scale of severity of incident, you can’t cost out something based on just a number like that you need to know what the severity is.” (Participant 10)

Participants suggested other details about incidents needed to be included (27 % n = 3) as the effect on patients due to incidents could be significant as one of the participants outlines below:

“If you could combine the number of incidents with reported patient effect that will make a very strong scorecard” (Participant 1)



Some participants wanted to see more details about the incident as the location of the incident as illustrated below:

“if I am managing an area I would like to know the type of incidents happening who’s involved physician nurse a clerk that to me is the thing of importance you going to have to investigate probably to find out because what you are looking for is some pattern of behavior maybe that type of incident and the location of the incident would be of more values” (Participant 8)

“this is very quantitative data, I’m not sure if there is any way that qualitative data can be captured like different themes of what the incidents might have been cause I think that would be really helpful specially in organization where I’m working that way there will be some strategies developed in how to mitigate those kind of things”(Participant 4)

Participants also suggested adding the top recent incidents as examples of incidents that have happened during the month to help managers to understand the weaknesses of the system quickly (18 % n = 2) as the excerpts from the interviews suggest:

“maybe another section would be last 7 days or last 5 days, this will be really good if we are having a monthly meeting , but what if an incident that happened couple days ago then we would be able to have last week and what that incident that happened couple days ago how did that impact if you know the numbers” (Participant 6)

“I’ll put a little very short summary of the top most recent incidents ,because they said oh we still have problem with that I didn’t know that was still a problem ok, so the people know exact the size of issues going on not just the definitions” (Participant 7)

For operation metrics, some participants suggested using a classification for vulnerabilities according to their severity (27 % n = 3) as outlined by two participants below:

“Total number of vulnerabilities, that would be good too like a breakdown if its workstation vulnerabilities or intrusion like if the users themselves are doing something or its attacks coming in” (Participant 5)

“if you have a scale of security you also have a scale of vulnerability you just putting how many different incidents , you have different levels of security that have been breached , by different levels of vulnerabilities” (Participant 10)

Participants also suggested new metrics about down time details (9 % n = 1) as

illustrated by the quote:

“ if its costing you money to take my system down for 5 hours to prove that I can take it down and bring it back up did I lose time ?did I lose business did I have everybody understanding each others with no computers, that actually not I just said that from a business standard when specially health care standpoint how often did my system go down and how much did it cost me ?” (Participant 9)

Some participants pointed out the importance of training for the organization and two participants expressed their interest in add training related metrics to the scorecard (18 % n = 2) as outlined in the quote below:

“if I want to track make sure we staying on top of our training I might want something similar to your unmitigated vulnerability. Known vulnerability which is for each month maybe one said new employees on and any untrained and I wouldn't want see any red if I saw any red I want to know why. You can just do this in a number up here under operations or something” (Participant 9)

For the financial section of the scorecard, participant 6 suggested adding a comparison of spending from year to year and adding a point in time historical cost (9 % n = 1) to the scorecard. Here, the participant states:

“Comparing spending (money) from year to year, like showing historical cost with time change, and % of cost change, Point-in-time historical costs is missing. i.e. 2 years ago, spent \$48k on toner for printers. This year, did we spend more or less? Percent change. Percent and \$ change over evergreen cycle.” (Participant 6)

The additional suggested metrics were mostly about incidents, participants asked for viewing of metrics classification according to severity and type also showing the top recent incidents with details. They also asked for vulnerabilities classification, details about downtime if this is a critical issue in the organization, metrics related to training, and metrics related to budget and spending.

#### 5.7.4 Visualization and Structure

All participants 100 % (n = 11) recommended having clear definitions for the terms used in the scorecard to avoid any misunderstandings. Participated suggested writing definitions on the back of a one-page scorecard sheet or showing the definitions for the metrics as a popup if the scorecard were in the form of webpage as described below:

“still the definitions is important, again if you put this on a webpage if you hover over you can get pop up window definitions or you can put it on the back of the paper if you like.” (Participant 7)

Another suggestion that was made by participants was to improve the visualization and usability of the scorecard and to put the scorecard online as a webpage and control access to this page as part of sensitive information in the organization (27 % n = 3). This participant suggestion expands the possibilities for users as in addition to providing a brief status report, users can click on to see a specific graph or number to get more information (and the scorecard can be printed out if needed). Participants describe this below:

“I think I would put it online and I would put little pop ups to show you what everything means.” (Participant 7)

“I think I would put it online and I would put little pop ups to show you what everything means.” (Participant 9)

Another suggestion for a scorecard is to include multiple projects in graphs in case the organization is managing different sites so each site needs to have a different curve in the graph with a curve showing the average number of projects (18% n = 2) as described in the following quotes:

“Show multiple lines for different projects that exist on different timelines. Existing lines show existing average for all projects.” (Participant 6)

“We usually are given every month a report each site and we are managing 9 sites, it’s not actually comparing all the sites together, it will be useful if we did having all of them in one.” (Participant 10)

## 5.8 Conclusion

In this chapter, the researcher reviewed the study findings showing the demographic characteristics of the participants and the results from the semi-structured interviews. The interview results were coded into categories and explained the main points of the study. These categories are found in Table 4. Each section of the table with its categories is discussed using quotes from the interviews to show how the participants responded to the questions and participants reactions during the part of the interview they were asked to think-aloud about in order to test the usability of the scorecard and get their feedback about the design and their visualization of the scorecard. Participants expressed notable interest in the scorecard as a security-reporting tool, especially to report incidents. Therefore, the incident metrics were the most favorable metrics presented to participants. The participant’s ideas about managing security were about knowing what incidents happened and how they happened in detail, as well what the effects of the incidents are on the organization in order to avoid those incidents from happening again. The participants suggested removing some metrics especially from the operations section of the scorecard. Participant thought that these metrics were more technical and managers would not be interested in following up on these metrics with them unless there was a reason to do so. Participants also suggested modifications to the metrics such as the classification of the incidents that have happened according to incident severity.

The visual appearance of the scorecard was acceptable to most participants. Participants made some recommendations that could be used to improve the scorecard.

The recommendations include providing definitions for the terms used in the scorecard to avoid confusion or misunderstanding of information by users. In general, the participants' views of the scorecard were consistent and their suggestions were valuable. Table 5 illustrates a summary of participants suggestions regarding the scorecard prototype reviewed. Table 5 summarizes all the recommendations and improvements discussed above. It shows the good metrics, which are the metrics in the suggested prototype that are interesting and can be used in the participants' workplaces as well as the irrelevant metrics (as identified by participants) that need to be omitted from the scorecard. In addition to this, the metrics that need to be added to the scorecard and the suggestions related to the visualization of the scorecard are provided in the table below.

	Metrics	Frequency % (n = 11)
Good metrics	Incidents metrics (in general)	73% n = 8
	Cost of incidents	56 % n = 6
	Mean time to incident recovery	46 % n = 5
	Cost of mitigation (for incidents)	36 % n = 4
Irrelevant metrics	Vulnerability scanning coverage	55 % n = 6
	Number of known vulnerabilities	36 % n = 4
	Mean time between incidents	36 % n = 4
	Cost (clinical)	18 % n = 2
	Budget percentage	9 % n = 1
Additional suggested metrics	Incident classification (severity, type)	63 % n = 7
	Incident details (location, frequency, effect)	27 % n = 3
	Top recent incidents	18 % n = 2
	Vulnerability classification	27 % n = 3
	Down time details	9% n = 1
	Training status	18 % n = 2
Visualization	Historical cost and budget comparison	9 % n = 1
	Clear definitions	100 % n = 11
	View online	27 % n = 3
	Multiple projects on graphs	18 % n = 2

**Table 5 Summary of participants' feedback about the scorecard**

## **Chapter 6 Discussion**

### **6.1 Introduction**

In this study, the researcher investigated the process of information security management in health care organizations. The study discussed using metrics to measure security in order to manage it. It introduced a scorecard for displaying the metrics so managers can understand the security status of their organization. The literature review in addition to the data collection and analysis of the study enabled the researcher to understand the process of managing security in health care organizations. Studying the possibility of using a security metrics scorecard in the management process clarified the security metrics concept. The research study determined what types of metrics are more popular among security experts, and the best way to visualise them in the form of the scorecard. This chapter outlines the results of the research study by introducing the updated version of the scorecard prototype according to the feedback collected. In this chapter, there will be direct answers for the four research questions mentioned in chapter 1 (i.e. How do health care organizations currently manage information security? What security metrics can be used in health care organizations? What do security managers think about using a security metrics scorecard in health care organizations? What are the specifications for a usable and effective security metrics scorecard?).

### **6.2 Security Management in Healthcare**

Information security managers in health care organizations use the same techniques and methods as other kinds of organizations, but they need to be more careful and more specific because of the sensitivity of the information they are working on to protect. The

first research question in this thesis was “How do health care organizations currently manage information security?” In this section, the researcher will answer this question based on the study findings and will show how these results compared with the literature review.

According to the participants in this study, health care information systems are complex and the communications between modules make it more difficult to control the security of the system. The main purpose is to avoid incidents and to minimize the effects of such incidents in case they occur. Incidents in health care can affect a patient’s health, privacy and finances. In case of incidents, managers need to know all the available details about the incident (like place, time, and effect on patients), who was involved, why it happened, and the controls needed to avoid this kind of incident from reoccurring. To maintain the security of the information system the participants in this study stated that they have technical security in their workplaces such as firewalls and antivirus and malware software. The security team members continuously monitor these tools to prevent these types of incidents. They also monitor the way the employees use the system and their activity log besides the network traffic in general to detect any suspicious behavior that might lead to an attack. They might also disable the USB drives and the CDs in computers to prevent any unauthorized copying of information.

All monitoring and auditing are part of policy compliance process. Organizations use policies to clarify the security rules and principles. There are also public policies imposed by government related to human safety and privacy. Security team members verify compliance with the security policy through auditing and monitoring the activities in the organization. All participants mentioned having policies and monitoring the

importance of compliance with these policies in their workplaces. To verify the accountability of workers participants mentioned that they use role based access controls that determine the parts of the system that users can access according to their roles in the organization. One of the participants referred to access control in health care as more granular so the access control applies on parts of the document not whole files. Another issue the participants considered important is employees' security training to confirm that they know exactly the rules and principles in the organization before even starting their work and update their knowledge regularly after that.

The literature mentioned security policies and principles in health care organizations (e.g. Buckovich et al., 1999). Buckovich and colleagues (1999) collected and compared privacy and security principles from ten different health care organizations and pointed out the importance of having policies and access control in place to maintain the privacy and confidentiality rights of patients. In addition, Bakker (1998) illustrated the basics of security in organizations showing the importance of security policy and people education. Many researchers have pointed out policies as a basic part of security programs while studying specific case studies as in Jafari et al. (2009), or while studying security as a process (Huang et al., 2008).

The security programs in health care organizations depend on standards and regulations developed by governments like PIPEDA, ISO 17799:2005; ISO 27001, ITIL in Canada and HIPPA, FISMA and NIST in the United States of America. The participants mentioned applying these standards in their workplaces and using the guidelines published by organizations like COACH, CIHI and Canada Health Infoway. In literature discussing security management in health care sometimes leads experts to mention the



standards that are currently being used. The study by Cavalli et al., (2004) showed how ISO 17799, the standard for information security management, combined with CEN/ENV12924 (a standard for security categorization and protection for health care information systems) when applied to health care information systems covers differing security requirements in the health care sector.

In this section, the researcher discussed how information security is managed in health care organizations according to security experts who participated in the study. The main areas for management discussed are technical security, information security, in addition to standards and guidelines. The study results compared with the security management literature in these areas.

### **6.3 Using Security Metrics in Health Care**

In order to manage security, there must be a method to measure the performance of the security system to track and compare the progress of any change. Information security management includes complex operations and too many numbers and data. The primary goal of metrics is to translate the data of the organization into a few meaningful numbers to help managers evaluate organizational performance (Jaquith, 2007). Using metrics that have been discussed in literature in many ways is key. For example, Jaquith (2007) gave a detailed analysis of using metrics in security management; the author described the good metric as it should be consistently measured, cheap to gather, expressed as a cardinal number or percentage and expressed using at least one unit of measure such as defects, hours, or dollars. Another description for the good metric can be found in many sources such as Nichols and Sudbury (2006) who described good metrics as SMART (specific, measurable, attainable, repeatable, and time dependent). If the metrics are

SMART, Security managers can depend on these metrics so they can make management decisions. Security metrics are used in different industries like in manufacturing (Qu & Zhang, 2007) information technology (Savola, 2007), and banking (Breu & Innerhofer–Oberperfler’s, 2008). In this thesis, the researcher discussed how to use security metrics in health care organizations to provide managers with the needed information to support their decision-making process. A monthly scorecard containing a set of selected metrics presented to security specialists who work in health care organizations and their comments and recommendations were collected. Their reaction towards using such technique as a tool in their workplaces was encouraging.

The second research question was “What security metrics can be used in health care organizations?”. Through analyzing the interviews that are done with security experts in health care organizations, the researcher extracted the answer to this question. The interviewer asked the participants some questions about security management and then showed them a scorecard prototype that shows security metrics, to check the acceptability and usability of the scorecard. The security metrics scorecard prototype used in this research, was built based on general security metrics listed in CIS (2010). Those metrics resulted from a general research study conducted by one hundred experts with different backgrounds who worked for CIS. The study aimed to introduce a set of basic security metrics that could be used in a wide range of organizations (see table 1). The security metrics included in the proposed prototype were made according to the assumptions made by the researcher about the general security objectives in health care organizations and what metrics matter for the managers.

From the interview data, the results showed that in health care, security managers are highly interested in incidents related metrics. The most important metrics according to the study participants are (incident classification, incident details, cost of incident, cost of mitigation, time to recover, top recent incidents). When something went wrong, they need to know exactly all the details to know the reason behind it and to prevent future breaches. According to the study, managers are not interested in technical metrics (like vulnerability scanning coverage or mitigated vulnerabilities) unless there is an issue related to something technical needs their follow up.

In the security metrics literature, in health care there appeared in the research trials to define security metrics based on existing standards. This work appeared in Huang et al., (2008) where the authors studied the application of security metrics in health care by using the SSE-CMM “The Systems Security Engineering Capability Maturity Model” taking into consideration the special nature of health care information by using HIPAA regulations standards for mapping. another example is the one appeared in Jafari et. al. (2009) who proposed a security metrics system that can be used to compare security between different organizations in order to start data sharing between them. Savola and Abie (2013) proposed a security metrics system based on risk impact assessment used in an E-health system.

#### **6.4 Security Metrics Scorecard**

In this section, the researcher will review how security metrics are being used in health care organizations, according to the study participants’, and how this topic appeared in the literature. The idea of using security metrics in health care organizations in general, received positive feedback from the study participants. They all praised the concept of

using security metrics in the form of a one page scorecard. This answers the research question (What do security managers think about using a security metrics scorecard in health care organizations?) All suggestions were related to metrics selection and presentation. The participants admitted that they use metrics even though they do not call them metrics or arrange them in reports like scorecards for managers, but a technical security team usually uses dashboards to review metrics.

The last research question ( i.e. What are the specifications for a usable and effective security metrics scorecard?) will be discussed by the researcher. In order to present security metrics in a usable form for managers, the researcher chose the balanced scorecard, which is a performance measurement system (Kaplan, 2008). The basic balanced scorecard has four perspectives (financial, customer, internal and learning and growth). These perspectives present the status of the organization as a whole so that managers can evaluate the strengths and weaknesses of the system and plan for improvement. The concept of a balanced scorecard used in the designed prototype of the security metrics scorecard, the perspectives in the scorecard selected to have three areas (Impact, Operations and financial). These terms are used to suit the information security terminology. The scorecard in this study was designed to show the security status of the organization on a monthly basis. The impact section presented the incidents' effect on the organization while the operations section presented how well the security functions work to prevent any breach. The financial section is about the money spending on security.

Balanced scorecards appear in literature as a general management system that can be used in hospitals to report on performance as in McCarthy (2012). Security scorecards

exist as a tool for management of security in organizations as in DeLooze (2006) who discusses using balanced scorecards for computer security in organizations.

Security metrics in the form of scorecards can be found in organizations' guidelines and regulations from specialized institutes like the SANS institute (Hoehl, 2010).

According to a participant in this research study, security vendors usually have security metrics reporting tools but they require an enterprise wide implementation for security and incident management system in order to be able to collect those metrics. Using a balanced scorecard system with a set of metrics selected from CIS (2010) resulted in the prototype in Appendix A that was tested in this study and discussed in the study interviews.

## **6.5 Human Computer Interaction and Usability Testing**

In this section, the researcher discusses the rationale for using the scorecard form based on balanced scorecard system for the study prototype, combining this with scorecard applications as mentioned in literature. To get feedback about the designed prototype of a security metrics scorecard, the researcher designed the study as a usability testing study.

Usability testing is a type of human computer interaction study. These kind of studies are concerned with the interaction between humans and machines from different aspects.

The study of human computer interaction on computer systems can be performed on a whole working systems or partially during the system development life cycle (Kushniruk & Borycki, 2008). Studying human computer interaction during the development stage enables the designer to gain more of an understanding of the requirements of systems.

Communicating with system users and getting feedback repeatedly through many iterations using the methods of usability engineering should result in more usable

systems. One of the methods of evaluation in usability engineering is usability testing. Usability testing refers to the evaluation of information systems by participants who represent system users. During the evaluation, users apply the “think aloud” technique by verbalizing their thoughts. Users’ interactions were recorded and analyzed to extract the feedback needed for improvement (Kushniruk & Patel, 2004). In this research, usability testing is used as a part of systems development lifecycle using prototyping to enable the participant to understand and visualize their needs and requirements more clearly (Jaquith, 2007). The researcher developed a prototype for the security metrics scorecard based on the basic recommended security metrics in CIS (2010) and applying the visualization recommendations suggested by Jaquith (2007) and Stabina (2005) to develop the prototype in a clear and informative form.

The security metrics scorecard prototype was used in the interviews and in the usability testing session. The participants that viewed the prototype were asked to think aloud. They expressed their thoughts about the scorecard: how they liked it, and how it can be improved. The sessions were recorded, the information analyzed, and the results translated into recommendations to reach a better usable and more effective security metrics scorecard. These recommendations formed the answer to the last research question as will be discussed in the next section.

## **6.6 Suggested Recommendations for Security Metrics Scorecard**

From the interviews with the participants and their feedback from the usability testing of the scorecard prototype, the researcher analyzed and put their requirements in specific points to answer the last research question (i, e. What are the specifications for usable and effective security metrics scorecard?), these points are:

**1- Definitions**

Include definitions for all terms used in the scorecard to avoid misunderstandings.

Definitions should be available so that they can be found easily (either on the back of the paper or as popup in case of electronic view). Not all people working in the field of security management use the same terms so having these definitions will ensure the accuracy of the information interpretation.

**2- Incidents Metrics**

Add incident metrics to the main section of the scorecard, and add metrics related to incidents classification according to their severity and type. Ensure you list the top five incidents with details.

**3- Financial Metrics**

In a monthly report, provide information about spending on incident mitigation, training and incident costs.

**4- Training Metrics**

Training is an important factor in security management so there must be a separate section (in the basic balanced scorecard design) to follow up the training coverage in the organization.

**5- Follow-up Metrics**

According to the organizations' status there might be different topics to follow up on each month so there is a need for having a specific section that includes variable statistics according to the organizations' security status or the managers' interests.

## **6- Warnings and Clarifications**

State clearly that the data appears in the scorecard, and that data is best viewed at the time that the scorecard is being preparing. Note that some fields might be prone to change in the future due to new inputs or unresolved issues.

## **7- Multi-projects**

If the organization has multiple projects or divisions, the metrics should present this fact and include multi-projects in the graphs to enable comparisons.

The above points are the main recommendations arising from the analysis of the data collected during the study.

## **6.7 Modified Scorecard Prototype**

After reviewing participant interviews, the researcher modified the original prototype based on participant comments. This led to the development of a modified version of the scorecard (Figure 7). In this version, the scorecard is divided into four main sections:

### **6.7.1 Incident Metrics**

Incident metrics are now at the top section of the scorecard as the managers mostly care about incidents that happened recently (according to the recommendations above). In the top part of the scorecard, there is a table for the recent incidents that happened, with some details related to them. The **description** briefly describes the incident. **Severity** shows the severity of the incident which represents the size of the impact of the incident on the organization, there are different classifications according to the standard used in the organization. There is a classification from the chief information officer branch of the



Canadian government classifying the incidents by severity to three levels (low, medium and high) (TBS-sct, 2012), where low is reflective of the least impact and high is the most severe of incidents. Also in CIHI security and privacy management protocol (CIHI, 2013), there is classification for the incidents' severity too (i.e. minor and major). The **type** of incident can be classified according to chief information officer branch of the Canadian government (TBS-sct, 2012). Classification include: Malicious code, known vulnerability exploit, system compromise, data compromise, denial of service, Access violation, accident or error, other or unknown. **Patients affected** on the scorecard shows the number of patients affected by the incidents. **Duration** displays the duration (time) the incident lasted, which is the time, needed for the system to overcome the effect of the incident and work normally. After this table there are two pie charts displaying the distribution of the incidents by type and severity. The pie chart graphs selected are based on recommendations made by participants, although they take a relatively large space on the scorecard, but they clearly represent the data and make the scorecard attractive.

Besides the charts, there are some metrics displayed as single numbers such as: **total number of incidents** or the number of incidents recorded during the month, this number displayed in the pie charts divided and clarified), **number of high-risk incidents** or the number of incidents with the severity (i.e. as high or major), the **mean time to recover** which displays the average time needed for the organizations' systems to recover from the incidents that happened during the month, and the **number of severe vulnerabilities** which shows the number of vulnerabilities in the system that are classified as severe and have not yet been mitigated. The next section will discuss the financial metrics.

### 6.7.2 Financial Metrics

The financial metrics that are interesting for the managers according to the participants are those related to incidents like:

**Cost of Incidents:** presents the total cost to the organization from security incidents occurring during the month.

**Cost of Mitigation:** the cost needed to recover the effect of the incident and bring the system back to normal status, this cost does not include the recovery cost for people who might have been affected by the incidents or the legal processes: it is only the system part of the cost.

**Total Security Spending by the End of the Month** as a percent of the total allocated budget in the specific fiscal period. This shows the percentage of the budget used and the percentage of the rest.

### 6.7.3 Training Metrics

This section of the scorecard presents the training status in the organization by the end of the month and includes a description of a number of aspects of training such as:

**unfinished regular training** or the number of employees who did not finish training / the number of the employees planned to finish the training by that time, **unfinished initial training** or the number of new employees who did not finish the initial training / the total number of new employees by the end of the month, and **unfinished special training** or the number of employees who did not finish special training/the number of employees planned to take the training. Special training can be for any special events happening in the organization to increase the employees' knowledge or as a result of a breach

happening. Lastly, **training budget** refers to the percentage of the spending on the training as a percentage of the total budget allocated for training by the end of the month.

#### **6.7.4 Selective Follow-up Metrics**

This section is a variable section as it includes data related to the organizations' status providing the manager with detailed information about specific topics that might need to be followed up on due to specific conditions. Some examples appear in the scorecard Figure 6. In the first example, the manager might be interested in watching for changes in the cost of incidents or cost of mitigation during the last twelve months in the organization to see the effect of new training or change in the system. In the second example if the training is not meeting the required level the manager might need to check the graph showing the number of untrained employees each month. In a third example, in case of the organization has more than one unit or project, the manager might need to check the distribution of the incidents in each project and compare them. In a fourth example, there is the case of incidents increasing notably at a specific time of the year so the manager needs to compare the number of incidents in the last two years.

All the above examples of different data analyses appear in the sample scorecard in Figure 6. They are just examples and the combinations are indefinite as long the data are available the manager can ask for extra analysis in the scorecard which makes the resulting scorecard a helpful resource in decision making process. In the last section of the scorecard, there is the comment space that can contain any related comment or note, and definitions are on the other side of the scorecard and include definitions for all terms used and notes or warnings to clarify any points that can lead to ambiguity see Table 6.

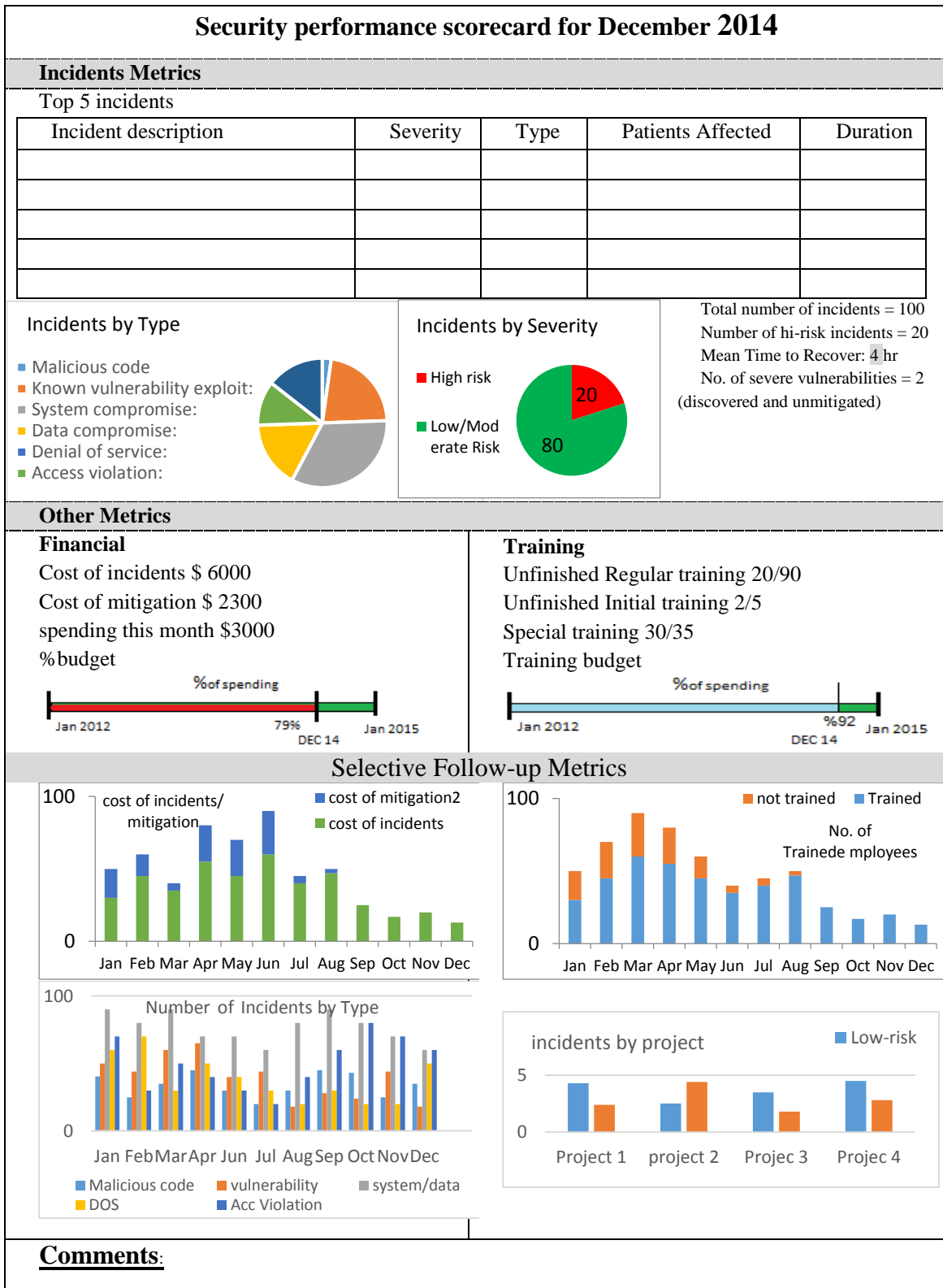


Figure 7 Security Metrics scorecard (modified) page 1

<b>Definitions and Notes</b>	
<b>Term</b>	<b>Definition</b>
<b>Incident</b>	The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
<b>Description</b>	describes briefly the incident
<b>Severity</b>	The size of the impact on the organization
<b>Type</b>	Malicious code, Known vulnerability exploit, System compromise, Data compromise, Denial of service, Access violation, Accident or error, or Other
<b>Patients affected</b>	shows the number of patients affected by the incidents
<b>Duration</b>	The time needed by the system to overcome the effect of the incident and work normally.
<b>Total No. of incidents</b>	presents the number of incidents recorded during the month,
<b>Number of High-risk incidents</b>	the number of incidents with the severity (High or major)
<b>Mean time to recover</b>	The average time needed for the organizations systems to recover from the incidents happened during the month.
<b>Severe vulnerabilities</b>	number of vulnerabilities in the system that are classified as severe
<b>Cost of incidents</b>	The total cost to the organization from security incidents during the month
<b>Cost of mitigation</b>	The cost needed to recover the effect of the incident and bring the system back to normal status, this cost does not include the recover cost to people who might been affected by the incidents or the legal processes it is only the system part of the cost.
<b>Total Security spending by the end of the month</b>	As a percent of the total allocated budget in the specific fiscal period. This shows the percentage of the budget used.
<b>Unfinished regular training:</b>	Number of employees who did not finish training / the number of the employees planned to finish the training by that time.
<b>Unfinished initial training:</b>	the number of new employees who did not finish the initial training / the total number of new employees by the end of the month
<b>Unfinished special training:</b>	Number of employees who did not finish the special training / the number of employees planned to take the training. Special training can be any special events happen in the organization to improve security awareness or because of a breach happened.
<b>Training budget</b>	Percentage of the spending on the training as a percentage of the total budget allocated for training by the end of the month.
<b>Selective follow-up metrics</b>	specific topics might need follow up due to specific condition
<b>Notes</b>	

**Table 6 Definitions appear in Security metrics scorecard (modified) page 2**

## **6.8 Research Limitations**

There are a number of limitations of this research. This research study was designed based on qualitative approaches; the interview part consisted of a demographic questionnaire, usability testing and semi-structured interview. The nature of the study related to information security left many experts hesitant about participation. The length of the session (30-40) minutes, which is a relatively long time to be extracted from busy schedules, and using communication technology also formed an obstacle. Security experts, are more cautious about information, that can be revealed about the organization they work for through them.

### **6.8.1 Limited Sample Size**

The recruitment process used in this study was snowball sampling (Polit & Hungler, 1991). Participants were invited to participate in the research by sending an invitation email to the University of Victoria Health Information Science graduate students listserve and Alumni listserv. Those who participated in the study were asked to send an invitation email to others who might be interested. Initially, the number of participants was very small (4 participants) so the recruitment process starting point was modified to include posting information about the study on the Canadian Health Informatics Association (COACH) website and sending emails to experts from the National Institute of Health Informatics (NIHI) website, in addition to the basic two email lists at university of Victoria. Many participants were worried about the nature of the study as they are working in the field of security; they needed to confirm that they would not reveal any information might threaten the security of their workplaces. The study questions were

designed to obtain general answers and no specific identifiers included in the analysis. These points were all clearly stated in the invitation email and consent form.

Another challenging point was the design of the study, as it required the use of SKYPE software for communication between the researcher and the participant. Some workplaces were blocking the use of SKYPE so participants had to do the interviews from different places.

During the data collection and analysis, the saturation point was reached after interviewing 11 participants. All participants were working as a part of information security teams in health care organizations, but not all of them were managers. The researcher preferred to do the study with more top management persons as they are the main users of the scorecard but it was not possible to reach more managers after many recruitment trials. The researcher assumed if some of the participants are not the direct user of the scorecard, they must be participating in delivering its information and report on the included data as part of their jobs. This assumption proved to be true through the interviews. Although the study was designed to discover the security management in health care organizations in general, the sample size might be limiting the generalization of the results.

#### **6.8.2 Inability to Apply Additional Iteration of the Study.**

After doing the interviews and analyzing the data from the usability study and participants' recommendations for improvement, the researcher collected all the feedback and modified the scorecard to the form in figure 6. Ideally, a researcher would do another round of usability studies of the new prototype. This would result in more accurate results. The second iteration might be useful in introducing the scorecard in an electronic

form as a website. However, due to time limitation and difficulty to reach the participants for another set of interviews. The researcher assumed the recommendations were enough to reach an acceptable and usable version of the final scorecard. Taking in consideration that the introduced scorecard is a starting point for security teams in health care organization to introduce the idea of using a simple scorecard that presents a quick accurate and reliable information about the security status in the organization monthly.

## **6.9 Future Research**

Studying the utilization of a security metrics scorecard in health care organizations opens many areas of research. This research can be extended to study the implementation of the scorecard in a specific health care organization as a case study. Another direction is using security metrics to compare security in two or more organizations for the purpose of integration and information sharing. In order to verify the efficiency of security metrics scorecard studies researchers can compare the security status of an organization before and after using the scorecard as a function of severe incidents happening in a specific period or a study about the effects of watching the frequency of specific types of incidents on management decisions. The study results presented here show how security training is important for improving the security level of the organizations. More research can be oriented in this direction in the future to enrich the training strategies undertaken health care environments. Financial metrics can be studied in detail and we can study the effect of security spending on the overall performance of the health care organization. The last suggestion for research is using the same concepts and techniques to design a security metrics scorecard for reporting on security status annually.



### **6.10 Security Metrics and Health Informatics Education**

From the research and the interviews with the participants, the conclusion reached about security management in health care organizations is the main important goals for security management is preventing security incidents and minimizing their effect on the organization. Besides the technical controls and following the rules and regulations, health care organizations depend on training. Security training should be extended from the health care organizations to be a part of health informatics education. Every student graduating from a health informatics program should be equipped with basic knowledge related to security and privacy in the health care sector. Security and privacy education should include the basic standards, regulations and laws ruling health care security and privacy. In addition to this, there is a need for basic initial training provided to health care organizations for new employees. This kind of information will define the person's limits, how to avoid incidents and how to report them.

### **6.11 Study Contribution to Health Information Practice**

This research study introduced a security metrics scorecard with basic metrics that are collected in every health care organization. This scorecard should help managers review the security status of the organization. It can also be used in discussions with people inside the organization for management meetings or outside the organization for integration and data sharing preparation meetings. Using this kind of reporting tool should help managers in making decisions related to security budget assignments, by explaining the security needs. To use this scorecard efficiently the metrics should be collected regularly and automatically so the results can be trusted.

## Chapter 7 Conclusion

Information security management in health care organizations is an essential part of health information systems management. Security breaches in health care organizations may lead to dangerous consequences for a patient's health and privacy. The main goals of security work are to control risks and lower the impact of security incidents. To achieve such goals, managers will need to have good visibility on the current security status of the organization. Security metrics help in achieving such visibility. In this work, the researcher studied information security management in health care organizations and introduced a new security metrics scorecard for managers. Most of the work in the literature related to security management in health care organizations is limited to special settings and case studies. In this work, the researcher studied security in health care organizations in general, and proposed the security metrics concept to be used in the form of scorecards to aid security status measurement. Using this scorecard improves understanding of security status in order to help decision-makers.

The security metrics scorecard summarizes the security data in the organization in the form of quantified metrics. The scorecard was designed to represent in one page a quick summary of the organizations' security status. The design was intended to be clear, easy to read and understand with no complex graphs or ambiguous numbers. To reach a usable form of the scorecard, the researcher designed a study based on qualitative research methods. The study consisted of a demographic questionnaire to collect information about study participants related to their experience and job descriptions,

while semi-structured interviews facilitated the discussion about security management in health care organizations as performed by the participants. The usability testing examined the usability of a scorecard prototype designed by the researcher based on basic security metrics arranged in a structure inspired by the balanced scorecard system that is used to assess organizational performance.

Metrics used in this study are similar to basic metrics that are normally collected in organizations as part of security management. These metrics were included in the prototype. The recruitment for the study resulted in 11 security experts participating. Data collection and analysis enabled the researcher to find the answers to the research questions. More specifically, security management areas of concern were identified. These included technical security like anti-virus and firewalls and information security like access control and audit trails. The policies, standards and guidelines like HIPAA and ISO 27001 in addition to training the employees to follow these regulations in the basic management areas in health care organizations. All participants' feedback related to security management were similar to research findings in the literature at this point.

The difference between health care and other industries was the participants' concerns about size of effect on patients' health and privacy. Around seventy percent of the participants stated clearly that incident related metrics are the ones that they want to check regularly. They wanted to see the details of the recent incidents, the classification of incidents according to type and severity, the cost of incidents and of mitigation. In addition to the incidents metrics the participants also pointed out the importance of the training related metrics, and the financial metrics. The proposed scorecard included a free area that can have metrics selected by managers according to the organization's

status and their plans. Based on the study findings a good security metrics scorecard needs to include metrics that are interesting for users and include illustrations of these metrics that are clear. Also, there should be a section with definitions for the terms in the metrics scorecard and allows for comments about any data that might be changing in the future according to new inputs or unresolved issues.

The security metrics scorecard provides managers with regular specific evaluation of security. It can help in comparing different business units in a health care organization. Scorecards can be part of comparing security among different health care organizations as a part of information sharing and integration preparation. Throughout the study, the researcher reviewed the management of information security as found in literature and in the work experience of security experts. The result translated into a scorecard that can help security managers in doing their jobs and keeping the information in health care organizations more secure.

## References

- Ashenden, D. (2008). Information Security management: A human challenge?. Information Security Technical Report, 13(4), 195-201.
- Azuwa, M., Ahmad, R., Sahib, S., & Shamsuddin, S. (2012). Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1(4), 280-288.
- Bakker, A. (1998). Security in perspective; luxury or must?. *International journal of medical informatics*, 49(1), 31-37.
- Behlen, F. M., & Johnson, S. B. (1999). Multicenter patient records research security policies and tools. *Journal of the American Medical Informatics Association*, 6(6), 435-443.
- Bønes, E., Hasvold, P., Henriksen, E., & Strandenaes, T. (2007). Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *International journal of medical informatics*, 76(9), 677-687.
- Breu, R., Innerhofer-Oberperfler, F., & Yautsiukhin, A. (2008, March). Quantitative assessment of enterprise security system. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on (pp. 921-928). IEEE.
- BCMA British Columbia medical Association. (2009). Privacy and security in the BC health care system today, Available from [https://www.bcma.org/files/Privacy\\_and\\_Security\\_in\\_BC\\_Healthcare\\_System\\_Today.pdf](https://www.bcma.org/files/Privacy_and_Security_in_BC_Healthcare_System_Today.pdf)
- Buckovich, S. A., Rippen, H. E., & Rozen, M. J. (1999). Driving Toward Guiding Principles A Goal for Privacy, Confidentiality, and Security of Health Information. *Journal of the American Medical Informatics Association*, 6(2), 122-133.
- Cavalli, E., Mattasoglio, A., Pincioli, F., & Spaggiari, P. (2004). Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics*, 73(3), 297-303.
- Cbc news. (JULY 11, 2014). B.C. PharmaNet hit by hacker, 1,600 accounts breached. Retrieved from <http://www.cbc.ca/news/canada/british-columbia/b-c-pharmanet-hit-by-hacker-1-600-accounts-breached-1.2704446>

CIHI Canadian Institute of Health Information. (2013). Privacy and Security Incident Management Protocol, Retrieved from [https://secure.cihi.ca/free\\_products/Incident%20Protocol%20\(CIHiway%20Version\)\\_EN\\_web.pdf](https://secure.cihi.ca/free_products/Incident%20Protocol%20(CIHiway%20Version)_EN_web.pdf)

CIS Community. (2010). The CIS security metrics, Retrieved December 12, 2010, from <http://benchmarks.cisecurity.org/downloads/metrics/>

Collmann, J., & Cooper, T. (2007). Breaching the security of the Kaiser Permanente Internet patient portal: the organizational foundations of information security. *Journal of the American Medical Informatics Association*, 14(2), 239-243.

eHealth Ontario . (2010). Guide to information security for the healthcaresector information and resources for complex organizations, Available from [http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide\\_Complex.pdf](http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_Complex.pdf)

Few, S. (2004). Show me the numbers: Designing Tables and Graphs to Enlighten. GVU's WWW User Survey Team, (1998). General Demographics Questionnaire. Retrieved from [http://www.cc.gatech.edu/gvu/user\\_surveys/survey-1998-10/questions/general.html](http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/questions/general.html).

FISMA. (2002). The Federal Information Security Management Act of 2002 Retrieved from <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

Health care Information and Management Systems Society HIMSS, (2005). What health care executives should know and do about information security. Retrieved from <http://www.himss.org/content/files/CEOWhitePaperFinal.pdf>

Herrmann, D. S. (2007). Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI. Auerbach Publications, (pp. 48:50)

Hsieh, H., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15 (9), 1277-1288.

Huang, L., Bai, X., & Nair, S. (2008, May). Developing a SSE-CMM-based security risk assessment process for patient-centered healthcare systems. In *Proceedings of the 6th international workshop on Software quality* (pp. 11-16). ACM.

Humer, C. & Finkle, J. (2014). Your medical record is worth more to hackers than your credit card, Reuters. Retrieved from <http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924>

- Ilioudis, C., & Pangalos, G. (2001). A framework for an institutional high level security policy for the processing of medical data and their transmission through the Internet. *J Med Internet Res*, 3(2):e14. doi: 10.2196/jmir.3.2.e14.
- Jackson, W., & Verberg, N. (2007). *Methods: Doing social research* 4th Ed. Toronto: Prentice Hall
- Jafari, S., Mtenzi, F., Fitzpatrick, R., & O'Shea, B. (2009). An approach for developing comparative security metrics for healthcare organizations. In *ICITST*(pp. 1-6).
- Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Professional.
- Kaplan, R. S. (2008). Conceptual foundations of the balanced scorecard. *Handbooks of Management Accounting Research*, 3, 1253-1269.
- Kirk, J. (2009). NHS Worm Infection Was 'Entirely Avoidable', says review. Retrieved from [http://www.csoonline.com/article/478726/NHS\\_Worm\\_Infection\\_Was\\_Entirely\\_Avoidable\\_Says\\_Review](http://www.csoonline.com/article/478726/NHS_Worm_Infection_Was_Entirely_Avoidable_Says_Review) , IDG News Service, February 02, 2009
- Kokolakis, S., Gritzalis, D., & Katsikas, S. (1998). Generic security policies for healthcare information systems. *Health informatics journal*, 4(3-4), 184-195.
- Kolkowska, E., Hedström, K., & Karlsson, F. (2008). Information Security Goals in a Swedish Hospital. In *The 31st Information Systems Research Seminar in Scandinavia*.
- Kushniruk, A. W., & Patel, V. L. (2004). Cognitive and usability engineering methods for the evaluation of clinical information systems. *Journal of biomedical informatics*, 37(1), 56.
- Kushniruk, A. W., & Borycki, E. M. (2006). Low-cost rapid usability engineering: designing and customizing usable healthcare information systems. *Healthc Q*, 9(4), 98-100.
- Kushniruk, A. W., & Borycki, E. (2008). Human, social, and organizational aspects of health information systems. *Medical Information Science Reference*.
- Kvale, S. (2008). *Doing interviews* (Vol. 2). Sage Publications Limited.
- Mello, J. P., 08/28/14, Hacker Attacks on Healthcare Providers Jump 600 Percent. Retrieved from <http://www.technewsworld.com/story/80959.html>
- Matthews, A. (2007). Trust Systems for Regional Health care, *Healthcare Quarterly*, 10(4), 146-148.

Nagle, L. M. (2007). Informatics: Emerging concepts and issues. *Nursing leadership-academy of Canadian executive nurses-*, 20(1), 30.

Nichols, E. A., & Sudbury, A. (2006). Implementing security metrics initiatives. *Information Systems Security*, 15(5), 30-38.

NIST National Institute of Standards and Technology. (2014). Special Publication 800 Series. Retrieved from <http://csrc.nist.gov/publications/PubsSPs.html>

Park, W. S., Seo, S. W., Son, S. S., Lee, M. J., Kim, S. H., Choi, E. M., ... & Kim, O. N. (2010). Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds. *Healthcare informatics research*, 16(2), 89-99.

Pascal, W., El Emam, K., McCarrey, M. (2009). Public Accountability and Transparency the Missing Piece of the Privacy Puzzle, 4th Quarter December 2009 HCIM&C. Retrieved from <http://www.canadiansecuritymag.com/IT-Security/News/Protecting-patient-data.html>

Polit, D. F., & Hungler, B. P. (1991). *Nursing Research: Instructor's manual*. Lippincott.

Ponemon Institute. (2014). *Fourth Annual Benchmark Study on Patient Privacy & Data Security*.

Preece, J., Rogers, Y., & Sharp, H. (2004). *Interaction design*. Apogeo Editore

Qu, W., & Zhang, D. Z. (2007, August). Security metrics models and application with SVM in information security management. In *Machine Learning and Cybernetics, 2007 International Conference on* (Vol. 6, pp. 3234-3238). IEEE.

Ravenel, J. P. (2006). Effective operational security metrics. *EDPACS*, 33(12), 10-19.

Ravera, L., Colombo, I., Tedeschi, M., & Ravera, A. (2004). Security and privacy at the private multispecialty hospital Istituto Clinico Humanitas: strategy and reality. *International journal of medical informatics*, 73(3), 321-324.

Salkind, N. J. (2006). *Encyclopedia of Measurement and Statistics*, (Vol. 3, pp. 808-812) Thousand Oaks, CA.

Sanders, W. H. (2014). Quantitative Security Metrics: Unattainable Holy Grail or a Vital Breakthrough within Our Reach?. *Security & Privacy, IEEE*, 12(2), 67-69.

Savola, R. (2007, August). Towards a security metrics taxonomy for the information and communication technology industry. In *Software Engineering Advances, 2007. ICSEA 2007. International Conference on* (pp. 60-60). IEEE.



Savola, R. M., & Abie, H. (2013, September). Metrics-driven security objective decomposition for an e-health application with adaptive security management. In *Proceedings of the International Workshop on Adaptive Security* (p. 6). ACM.

Shortliffe, E. H., & Cimino, J. J. (Eds.). (2006). *Biomedical informatics: computer applications in health care and biomedicine*. Springer.

Stabina, R. (2005). *Quantitative Data Graphics: Best Practices of Designing Tables and Graphs for Use in Not-for-Profit Evaluation Reports* (Doctoral dissertation, University of Oregon).

Sutton, N., (2008) Protecting patient data. Retrieved from <http://www.canadiansecuritymag.com/IT-Security/News/Protecting-patient-data.html>

The Economist, 2013, [daily chart Feb 4, 2013]. Stock market performance. Retrieved from <http://www.economist.com/blogs/graphicdetail/2013/02/daily-chart-0>

Van der Haak, M., Wolff, A. C., Brandner, R., Drings, P., Wannemacher, M., & Wetter, T. (2003). Data security and protection in cross-institutional electronic patient records. *International journal of medical informatics*, 70(2-3), 117-130.

Van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *International journal of medical informatics*, 78(3), 141-160.

Voelker, K. E., Rakich, J. S., & French, G. R. (2001). The balanced scorecard in healthcare organizations: a performance measurement and strategic planning methodology. *Hospital topics*, 79(3), 13-24.

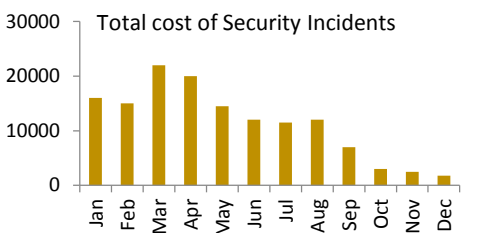
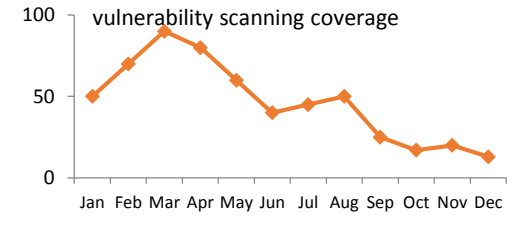
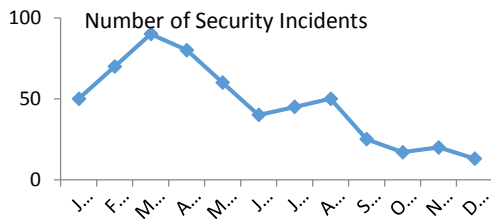
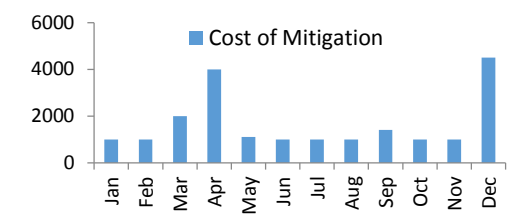
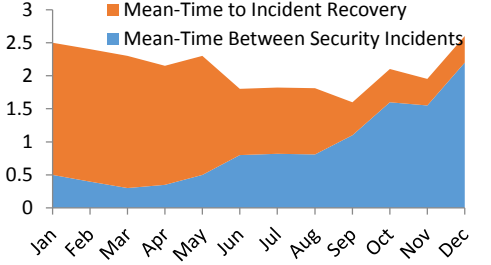
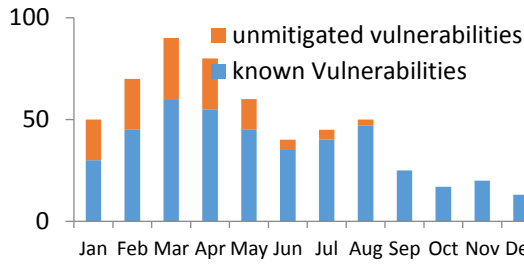
Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376.

Wang, A., J., (2005), Information security models and metrics. 43rd ACM Southeast Conference, 178-184.

Weiß, S., Weissmann, O., & Dressler, F. (2005, November). A comprehensive and comparative metric for information security. In *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2005)* (pp. 1-10).

Wimalasiri, J. S., Ray, P., & Wikon, C.S., (2005). Security of electronic health records based on web services. *IEEE Proceedings of 7th International Workshop*, 91- 95.

## Appendix A

<b>Security performance scorecard for December 2012 (Prototype)</b>				
<b>Impact</b>		<b>Operation</b>		
<b>This Month</b>				
Total Number of Incidents: <b>22</b> Tot Cost of Incidents: <b>\$6000</b> Mean Time Between Incidents: <b>2 days 2 hours</b> Mean Time to Recover: <b>4 hours</b>		Number of applications: <b>20</b> Number of Systems with No-Known Severe Vulnerabilities: <b>9</b> Vulnerability scanning Coverage = <b>90%</b> Number of Known Vulnerabilities: <b>67</b> Mean-Time to Mitigate Vulnerabilities: <b>5 days</b> Total Cost of Mitigation: <b>\$2300</b>		
<b>Past 12 Month</b>				
				
				
				
<b>Financial</b>				
	Q1	Q2	Q3	Q4
% of IT Budget	7	6	5	3
IT security budget allocation				
Products	30%	30%	20%	10%
Service	20%	20%	25%	40%
Training	15%	5%	5%	8%
<b>Comments:</b>				

## Appendix B: Demographic Questionnaire

What is your age?

- 25 or under
- 26-40
- 41-55
- 56 or older

How long have you been working in security?

- less than 5 years
- 5 to 10 years
- more than 10 years

How long have you been working in the health information and security area?

- less than 5 years
- 5 to 10 years
- more than 10 years

What is your job?

- Security engineer
- Telecommunication engineer
- privacy officer

124

- Quality assurance
- Legal
- Finance
- Marketing or Public relations
- CEO chief executive officer
- CSO chief security officer
- ISSM information systems security manager
- ISSO information systems security Officer
- other .....

Which of the following best describes your role in industry?

- Upper management
- Middle management
- Junior management
- Administrative staff
- Support staff
- Other

## **Appendix C Interview guide**

### Part 1

1. can you tell me about how information security is being managed in your workplace?
2. What security metrics are collected regularly?

### Why?

3. What are the specifications that make security metrics usable and effective in managing information security in your organization?

Now I'll show you a sample scorecard, and you are asked to review it and think aloud to give your feedback on the selected metrics and if they can be used in your organization, and also on the way they are presented (visualization),

### Part 2

After reviewing the suggested scorecard:

4. what parts of it do you think can be used in your organization?
5. what parts not important or can be omitted?
6. what metrics need to be added and what the best way to visualize them?
7. do you think metrics used in health care organizations vary from other type of organizations? If yes then how?

8. Do you have suggestions for improving the scorecard?

## Appendix D

**School of Health Information Science  
University of Victoria**

**Participant Consent Form**

---

Developing Security Metrics Scorecard for Health Care Organizations

You are invited to participate in a study entitled Developing Security Metrics Scorecard for Health Care Organizations that is being conducted by Heba Elrefaey.

Heba Elrefaey is a graduate student in the department of Health Information Science at the University of Victoria and you may contact her if you have further questions by email ([hebae@uvic.ca](mailto:hebae@uvic.ca))

As a graduate student, I am required to conduct research as part of the requirements for a master degree in Health Information Science. It is being conducted under the supervision of Dr. Elizabeth Borycki. You may contact my supervisor at (250- 472-5432).

Purpose and Objectives

The purpose of this research project is to develop a tool to measure security in health care organizations and help security managers in this field. This tool will be a scorecard for security metrics. Scorecards will need to be acceptable and usable to health care security managers. The research will be conducted by interviewing a group of security managers in health care organizations and collecting their feedback about a suggested scorecard prototype, then analyzing the results to reach an acceptable form.

#### Importance of this Research

Research of this type will contribute in facilitating the security management through health care organizations by providing a metrics scorecard prototype. This scorecard will help managing the security within the organization and improves the security level. Also, it will make the communication between health care organizations easier if they are using the same metrics technique. This study will encourage more research in the area of security management and related issues such as introducing new policies for different parts of the information systems in health care organizations.

#### Participants Selection

You are being asked to participate in this study because you have work experience in the field of information security in health care organization.

#### What is involved



If you consent to voluntarily participate in this research, your participation will be called by Skype and the call will include filling questionnaire and being interviewed, and then you will be asked to go through security metrics scorecard and give your feedback about its usability.

Audio-tapes will be taken. A transcription will be made. Video tapes will be taken of your computer screen while you are checking the scorecard, if you are using a webcam the video will include your picture but it will never be used in the dissemination of results or published in any other ways.

The data collection session will take approximately 30-40 minutes and can be held at any place as it will be online.

#### Inconvenience

Participation in this study may cause some inconvenience to you, including the time you will spend and the effort you will do in the experiment session.

#### Risks

There are no known or anticipated risks to you by participating in this research

#### Benefits

By participating in this research you are helping health informatics professionals to make information in health care organizations more secure, this will help people in the society to worry less about their privacy in these settings. For the state of knowledge, this research will encourage more research efforts in the field of security in health care organizations.

### Voluntary Participation

Your participation in this research must be completely voluntary. If you do decide to participate, you may withdraw at any time without any consequences or any explanation. If you do withdraw from the study your data will be permanently deleted from the system.

### Anonymity

In terms of protecting your anonymity all unique and identifying information will be removed during transcribing of the audio and video data.

### Confidentiality

Your confidentiality and the confidentiality of the data will be protected as all unique and identifying information will be removed during transcribing of the audio and video data.

### Dissemination of Results

It is anticipated that the results of this study will be shared with others in the form of published thesis.

### Disposal of Data

Data from this study will be disposed in the form of deletion of electronic files.

### Contacts

Individuals that may be contacted regarding this study include researcher and supervisor as stated in the beginning of the consent;

In addition, you may verify the ethical approval of this study, or raise any concerns you might have, by contacting the Human Research Ethics Office at the University of Victoria (250-472-4545 or ethics@uvic.ca).

Your signature below indicates that you understand the above conditions of participation in this study, that you have had the opportunity to have your questions answered by the researchers, and that you consent to participate in this research project.

---

Name of Participant

---

Signature

---

Date

A copy of this consent will be left with you, and a copy will be taken by the researcher.

## Appendix E

School of Health Information Science

Email Invitattion

**University of Victoria, British Columbia**

---

Email Invitation to Participate in a Study

Developing Security Metrics Scorecard for Health Care Organizations

You are invited to participate in a study entitled “**Developing Security Metrics Scorecard for Health Care Organizations**” that is being conducted by Heba Elrefaey who is a graduate student at the School of Health Information Science at the University of Victoria.

The purpose of this research project is to develop a tool to measure security in health care organizations. Research of this type will contribute in facilitating the security management through health care organizations by introducing a metrics scorecard prototype. This scorecard will help managing the security within the organization and improves the security level. Scorecards will need to be acceptable and usable by health care information security managers. The research will be conducted by interviewing a group of security managers in health care organizations and collecting their feedback

about a suggested scorecard prototype, then analyzing the results to reach an acceptable form.

You are being asked to participate in this study because you have work experience in the field of information security in health care organization.

#### What is involved

If you agree to voluntarily participate in this research, you will be asked to complete a demographic questionnaire and participate in a semi-structured interview and usability test for the proposed scorecard lasting approximately 45 minutes. You will be asked for demographic information and then interviewed about the security metrics and management in your workplace. That will be conducted by using Skype communication software. Audio and screens will be recorded.

If you are interested in this study or have further questions, you may contact Heba Elrefaey by email ([hebae@uvic.ca](mailto:hebae@uvic.ca)) to obtain additional information.

## Appendix F Website Post

Heba Elrefaey a graduate student at the School of Health Information Science at University of Victoria is conducting a research study titled "*Developing Security Metrics Scorecard for Health Care Organizations*". The purpose of this research is developing a scorecard to help managers measure information security in health care organizations, this will contribute in facilitating the security management and improves the security level in health care organizations.

We are looking for volunteers to participate in the evaluation of this new scorecard by providing their feedback in a short (about 30 min) one-time interview. It will include demographic questionnaire and interview about the security management and commenting on the scorecard prototype. The study will be conducted using Skype communication software.

Participants should have work experience in the field of information security in health care.

If you are interested to participate in this and contribute to the new research or if you have any questions, please email Heba [hebae@uvic.ca](mailto:hebae@uvic.ca).

## Appendix G

### THE ECONOMIST NEWSPAPER LIMITED LICENSE

#### TERMS AND CONDITIONS

Apr 13, 2013

---

---

This is a License Agreement between heba elrefaey ("You") and The Economist Newspaper Limited ("The Economist Newspaper Limited") provided by Copyright Clearance Center ("CCC"). The license consists of your order details, the terms and conditions provided by The Economist Newspaper Limited, and the payment terms and conditions.

All payments must be made in full to CCC. For payment instructions, please see information listed at the bottom of this form.

License Number

3127360128223

License date

Apr 13, 2013

Licensed content publisher

The Economist Newspaper Limited

Licensed content publication

The Economist

136

Licensed content title

What crisis?

Licensed content author

Licensed content date

Feb 4, 2013

Volume number

Issue number

Pages

1

Type of Use

Thesis/Dissertation

Requestor type

Student

Portion

Charts/Graphs

Circulation

1

Format

Print and electronic

Geographic Rights

Canada

Order Reference Number

Institution name



137

univrsity of victoria

Course name

HINF 599 thesis

Name of instructor

Elizabeth Borycki

Billing Type

Invoice

Billing address

20-11020 williams road

richmond, BC v7a1x8

Canada

Economist VAT number

GB 340 4368 76

Permissions price

0.00 USD / 0.00 GBP

VAT/Local Sales Tax

0.00 USD / 0.00 GBP

Total

0.00 USD / 0.00 GBP

Terms and Conditions

**TERMS AND CONDITIONS**

These are terms and conditions under which The Economist Newspaper Limited ("The Economist") is willing to license the content ("Content") identified in the order form above ("Order Form") to the user named in the Order Form ("You"). It (along with the Order Form) forms a legally binding licence agreement ("Licence") between you and The Economist.

The Economist authorises You to reproduce the Content, subject to payment of the non-refundable fee set out in the Order Form and to the terms of this Licence.

The Licence permits the one-time use by You of the content either in the English language, or in translation in the language specified in the Order Form, in the work ("Work") and format specified in the Order Form. This permission, for electronic rights, shall last for the duration specified in the Order Form, and for print rights, shall allow the circulation/distribution specified there.

Separate permission must be sought in advance for any other proposed use whatsoever, including without limitation, future distributions, editions, translations or reproduction in any other medium from what is expressly authorised in this Licence.

Where a translation is authorised in the Order Form, You must ensure that the translation of the Content will be carried out to the highest possible standards; that it will be accurate, unabridged and without additions; and that it will not change the content, meaning, spirit or tone of the original material nor any opinion or view expressed directly or indirectly in it. The text of any Content shall not be added to or amended without the prior consent of The Publisher. Articles cannot be abridged. You accept and agree that The Economist shall not bear any liability whatsoever arising in relation to any such translated, amended or abridged material and You agree to indemnify The Economist and

its affiliates against any liabilities, costs, losses or damages they may suffer in relation to any such material.

The permissions granted in this Licence are granted on a fully non-exclusive basis and The Economist may allow other users and/or publishers anywhere in the world to reproduce the same material. The Content is provided without any warranties in respect of its content or form, and to the fullest extent possible under the law, The Economist disclaims all implied warranties. The Economist shall not be liable for any costs, damages or losses arising directly or indirectly from the use of, or reliance on, the Content. The Economist's maximum aggregate liability shall in any event be limited to the amount of the fee paid by You.

The Content is the property of The Economist and is protected by copyright and other intellectual property rights. All orders that You make for any Content are subject to approval by The Economist, and The Economist has the right to deny any order.

Other than the rights specifically granted in this Licence, You may not modify, edit, copy, store, archive, distribute, transmit, create derivative works from or in any way commercially exploit the Content, or any content of The Economist, without its written permission. Except as specifically permitted in the Order Form, You may not use the Content (i) in connection with any online versions of newspapers, magazines or books; or (ii) in print or electronic (e.g., banner) advertisements.

You may not use the Content in any manner or context which would render it, or otherwise affiliate it with material that is likely to be considered (A) libellous, defamatory, inaccurate, abusive, inappropriate, profane, obscene, indecent, pornographic, sexually explicit or illegal, (B) unlawful or violating or encouraging the violation of any

local, state, national or international law; (C) infringing any patent, trademark, trade secret, copyright or other proprietary rights of any party; or (D) containing expressions of bigotry, racism or hate.

You further agree not to use the Content in any manner or context that would be derogatory to the author of the Content, any publications of The Economist Newspaper Limited, or any person depicted in the Content.

You agree to abide by all copyright notices and restrictions attached to the Content and not to alter or remove any trademark, copyright or any other notice from copies of the Content.

The permissions granted under this Licence do not include the right to use any logos or trade marks of The Economist and acknowledgement in the following form must be given in each place where the Content is reproduced:

"© The Economist Newspaper Limited, London (issue date)".

You acknowledge that that The Economist does not usually own the copyright in any photographs, cartoons or drawings. Permission to reproduce any of these is not given to You and would in any case probably also need to be obtained directly from the individual copyright holders. You agree fully to indemnify The Economist against any liabilities, costs, losses or damages The Economist may suffer arising out of or in relation to Your use of any photographs, cartoons or drawings.

This Licence is for Your benefit only (as the user named on the Order Form) and Your rights or obligations may not be assigned, transferred or sublicensed by You. The Economist is entitled to terminate and revoke this Licence with immediate effect if You breach any of its terms.

The Economist Newspaper Limited or CCC may, within ten (10) days from the date of license, deny the permissions described in this License at their sole discretion, for any reason or no reason, with a full refund payable to you (where permission is denied for reasons other than your misconduct or breach). Notice of such denial will be made using the contact information provided by you. Failure to receive such notice will not alter or invalidate the denial. In no event will CCC be responsible or liable for any costs, expenses or damage incurred by you as a result of a denial of your permission request, other than a refund of the amount(s) paid by you to CCC for denied permissions.

**License Contingent on Payment.** While you may exercise the rights licensed immediately upon issuance of the license at the end of the licensing process for the transaction, provided that you have disclosed complete and accurate details of your proposed use, no license is finally effective unless and until full payment is received from you (either by publisher or by CCC) as provided in CCC's Billing and Payment terms and conditions. If full payment is not received on a timely basis, then any license preliminarily granted shall be deemed automatically revoked and shall be void as if never granted. Further, in the event that you breach any of these terms and conditions or any of CCC's Billing and Payment terms and conditions, the license is automatically revoked and shall be void as if never granted. Use of materials as described in a revoked license, as well as any use of the materials beyond the scope of an unrevoked license, may constitute copyright infringement and publisher reserves the right to make any and all action to protect its copyright in the materials

This Licence shall be governed by English law and You submit to the exclusive jurisdiction of the English courts.

142

Special Terms: None

v1.2

If you would like to pay for this license now, please remit this license along with your payment made payable to "COPYRIGHT CLEARANCE CENTER" otherwise you will be invoiced within 48 hours of the license date. Payment should be in the form of a check or money order referencing your account number and this invoice number

RLNK500999161.

Once you receive your invoice for this order, you may pay your invoice by credit card.

Please follow instructions provided at that time.

Make Payment To:

Copyright Clearance Center

Dept 001

P.O. Box 843006

Boston, MA 02284-3006

For suggestions or comments regarding this order, contact RightsLink Customer

Support: [customercare@copyright.com](mailto:customercare@copyright.com) or +1-877-622-5543 (toll free in the US) or +1-978-646-2777.

Gratis licenses (referencing \$0 in the Total field) are free. Please retain this printable license for your reference. No payment is required.