

University of Groningen

## The threat nets approach to information system security risk analysis

Mirembe, Drake

**IMPORTANT NOTE:** You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

*Document Version*

Publisher's PDF, also known as Version of record

*Publication date:*

2015

[Link to publication in University of Groningen/UMCG research database](#)

*Citation for published version (APA):*

Mirembe, D. (2015). *The threat nets approach to information system security risk analysis*. University of Groningen, SOM research school.

### Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

### Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

# **The Threat Nets Approach to Information System Security Risk Analysis**

Drake Patrick Mirembe

Publisher: University of Groningen,  
Groningen, the Netherlands

Printed by: Ipskamp Drukkers B.V  
Enschede, the Netherlands

ISBN: 978-90-367-8140-4 (Book)  
978-90-367-8139-8 (Electronic version)

Drake Patrick Mirembe  
The Threat Nets Approach to Information System Security Risk Analysis  
Doctoral Dissertation, University of Groningen, the Netherlands

**Keywords:** outpatient case management, healthcare information management system, security management, threat analysis, Threat Nets Approach, information system security, design science research, service science, risk analysis, decision enhancement, threat business impact

Copy right: Drake Patrick Mirembe © 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system of any nature, or transmitted in any form or by any means. Electronic, mechanical, now known or hereafter invented, including photocopying or recording, without prior written permission of the author.



**rijksuniversiteit  
 groningen**

# **The Threat Nets Approach to Information System Security Risk Analysis**

## **Proefschrift**

ter verkrijging van de graad van doctor aan de  
Rijksuniversiteit Groningen  
op gezag van de  
rector magnificus prof. dr. E. Sterken  
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op

donderdag 1 oktober 2015 om 12:45 uur

door

**Drake Patrick Mirembe**

geboren op 28 juni 1978  
te Kyabasaigi, Oeganda

**Promotores**

Prof. dr. H.G. Sol

Prof. dr. J.T. Lubega

**Beoordelingscommissie**

Prof. dr. ir. M. Aiello

Prof. dr. E.O. de Brock

Prof. dr. ir. Th.P. van der Weide

*To my family Andrea Drake Kirabo, Alvin Drake Tendo and Martha Hope Nakitto*

## **Preface and Acknowledgement**

Healthcare information management systems like Remote Patient Monitoring Systems (RPMS) are becoming a backbone of service delivery in the healthcare industry. Given the critical role information systems are playing in healthcare service delivery, identifying and quantifying threats to information systems is a major task for information system managers. On a daily basis news outlets are awash with reports of information system security breaches, due to the lack of appropriate threat mitigation controls. Therefore, for security analysts to define and implement appropriate threat mitigation controls, they must understand the nature, likelihood and potential business impact of threats to information systems and hospitals at large.

The journey of writing this PhD thesis has not been an easy one. The road has been muddy and at times rocky with many humps. On a number of occasions I felt this project could not be completed. When the spark idea seemed not to work and normal life hassles took center stage. In those very difficult moments, there were people who believed in me and encouraged me to soldier on. I will be indebted to them. All I can state at this moment is a big thank you for being there for me, when I needed a shoulder to lean on.

Special thanks go to my promoters Prof. dr. Henk G. Sol and Prof. dr. Jude T. Lubega who picked me from pieces and gave me a chance to complete my childhood dream of pursuing a doctorate. I have learned a lot during this project; I cherish and treasure the knowledge and life skills I have acquired through their dedicated guidance and mentorship. Indeed they are a special pair of hands and I am honored to have worked with them on this project. Prof. Jude, I thank you for accepting my inconveniences, when I needed help. Prof. Henk, I acknowledge you in a special way for working out a fellowship for me at the University of Groningen and for being patient with me when personal challenges took center stage. I will forever be grateful to you.

A word of thanks also goes to colleagues who helped me in many ways; Steven Mutinyu, John Ngubiri, Pearl Rebecca Tumwebaze, Prossy Katumba, Edna Kyobutungi, Ronald Azairwe, Kutegeka Wilson, Robert Tumusiime, John Kizito, and Jacob Janja among others.

I register my gratitude in a special way to the management of Uganda Technology and Management University (UTAMU) and Makerere University in particular Prof. Baryamureeba for their unending encouragement and support. I would also like to thank the management of Case Hospital Kampala (CHK), Mengo Hospital (MH) and colleagues from ClinicMaster International Ltd (CIL) who offered all the necessary support to enable the evaluation of the approach. A word of appreciation also goes to members of Uganda Infosec Community (UIC) who provided initial feedback on the approach and participated in the evaluation exercises. I cannot forget Barbara Lillian Kizito who provided insights on risk quantification from the insurance perspective.

Special thanks goes to my dear wife, Martha Hope Nakitto for being there for me whenever I needed a word of encouragement. You're a special blessing to me and this PhD also belongs to you for your unwavering support, care and understanding. Your contribution to this PhD is a true manifestation of your name "Martha" a woman of noble character and I am privileged to be that special friend in your life. My gratitude also goes to my parents (Dr. George Bagonza and Ms. Scovia Jjagwe) and siblings especially Mrs. Immaculate Muyomba and Dr. Wilson Amanyire who have continuously supported me.

Lastly, I thank God for his favor, guidance and providence. Without the hand of the most high this thesis would not be possible. There were many valleys and mountains but his grace sustained me there. I will forever be a living testimony of his works.

Drake Patrick Mirembe, 2015



## CONTENTS

---

<b>1. Research Background and Approach.....</b>	<b>1</b>
1.1 Healthcare Delivery Challenges.....	1
1.2 Trends in Healthcare Service Provisioning.....	2
1.3 Remote Patient Monitoring Systems Opportunities.....	3
1.4 RPMS Issues .....	6
1.5 Motivation and Research Problem.....	7
1.6 Research Objective and Questions.....	8
1.7 Research Approach .....	9
1.8 Thesis Organization .....	13
<b>2. Understanding Threat Analysis .....</b>	<b>15</b>
2.1 Approaches to Understanding Threat Analysis.....	15
2.2 A Threat Analysis Process .....	16
2.3 Threat Analysis Approaches .....	19
2.4 Threat Analysis Decisions that Matter .....	23
<b>3. Threat Analysis Issues: Practitioners Perspective.....</b>	<b>25</b>
3.1 Study Objectives .....	25
3.2 Study Approach.....	25
3.3 Presentation and Discussion of Results.....	30
3.4 Requirements for an Ideal Threat Analysis Approach.....	36
<b>4. The Threat Nets Approach .....</b>	<b>39</b>
4.1 General Overview of the Threat Nets Approach.....	39
4.2 Threat Analysis Scenario .....	40
4.3 The “Ways of” Framework .....	41
4.4 Way of Thinking .....	42
4.5 Way of Governance.....	45
4.6 Way of Modelling .....	47
4.7 Way of Working.....	50
<b>5. Threat Nets Approach Evaluation .....</b>	<b>67</b>
5.1 Evaluation Objectives .....	67
5.2 Evaluation Parameters and Procedures .....	67
5.3 Evaluation Results.....	85

5.4 Interpretation and Discussion of Results.....	90
<b>6. Epilogue.....</b>	<b>93</b>
6.1 Thesis Overview .....	93
6.2 Contributions to Society and Knowledge.....	97
6.3 Research Limitations.....	99
6.4 Conclusions and Future Works .....	99
<b>References .....</b>	<b>101</b>
<b>Appendices .....</b>	<b>111</b>
<b>Appendix 1: Exploratory Study Unstructured Interview Guide .....</b>	<b>111</b>
<b>Appendix 2: Exploratory Study Questionnaire .....</b>	<b>112</b>
<b>Appendix 3: ThreNet Tool Description .....</b>	<b>115</b>
<b>Appendix 4: Threat Nets Approach Evaluation Questionnaire for Security Experts</b>	<b>124</b>
<b>Appendix 5: Threat Nets Approach Evaluation Questionnaire for Business Analysts</b> .....	<b>127</b>
<b>List of Acronyms.....</b>	<b>129</b>
<b>Summary .....</b>	<b>131</b>
<b>Samenvatting .....</b>	<b>135</b>
<b>Curriculum Vitae.....</b>	<b>139</b>

## List of Figures

Figure 1-1: Structure of a Generic Sensor .....	3
Figure 1-2: A Generic Architecture of a Remote Patient Monitoring System .....	4
Figure 1-3: The Inductive Hypothetic Research Strategy (Sol, 1982) .....	12
Figure 2-1: A Fault Tree Analysis for an E-mail Service.....	20
Figure 2-2: Attack Tree Example (Schneier, 1999) .....	21
Figure 3-1: Online Questionnaire .....	29
Figure 3-2: Expert Responses.....	29
Figure 4-1: General Overview of the Threat Nets Approach .....	40
Figure 4-2: Sol's "Ways of" Framework (Sol, 1988) .....	42
Figure 4-3: Relationship between System Characteristics and Vulnerabilities.....	43
Figure 4-4: Threat Nets Approach Use-Case Diagram.....	48
Figure 4-5: Threat Nets Approach Sequence Diagram.....	49
Figure 4-6: Threat Nets Approach Activities .....	50
Figure 4-7: Threat Likelihood Assessment Service Activity Diagram .....	54
Figure 4-8: A Threat Tree Illustrating a Threat Progression .....	59
Figure 4-9: Threat Impact and ROI Evaluation Activity Diagram.....	60
Figure 5-1: E-mail Sharing the Threat Nets Approach with Evaluators.....	70
Figure 5-2: Case Study Threat Analysis Projects Created in the ThreNet Tool.....	73
Figure 5-3: Assignment of Roles to Threat Analysts' .....	73
Figure 5-4: Assessment of Completeness of ClinicMaster Components at Case Hospital ...	74
Figure 5-5: Assessment of Completeness of Human Resources ClinicMaster Component at Mengo Hospital .....	75
Figure 5-6: Computation of Likelihood of Unauthorized Access of Patient Data at Case Hospital .....	76
Figure 5-7: Computation of Likelihood of Unauthorized Access of Patient Data at Mengo Hospital .....	77
Figure 5-8: A Security Expert Report on Likelihood of Unauthorized Access to Patient Data .....	78
Figure 5-9: Assessment of Threat Business Impact Lost Network Connectivity at Case Hospital .....	79
Figure 5-10: Assessment of Threat Business Impact of Lost Connectivity Threat at Mengo Hospital .....	80
Figure 5-11: Service for Assessing Cost-Effectiveness of Threat Mitigation Controls at Case Hospital .....	81
Figure 5-12: Service for Assessing Cost-Effectiveness of Threat Mitigation Controls at Mengo Hospital .....	82
Figure 5-13: Online Questionnaire.....	83
Figure 5-14: Participants' Responses .....	83

## **List of Tables**

Table 3-1: Profile of the First Group of Experts .....	26
Table 3-2: Profile of Second Group of Experts .....	27
Table 3-3: Typical Threat Analysis Process .....	31
Table 3-4: Challenges Experts Face when Analyzing Threats .....	33
Table 3-5: Characteristics of an Ideal Threat Analysis Approach .....	34
Table 3-6: Parameters for Threat Analysis Approach Evaluation .....	35
Table 4-1: Guidelines to Facilitate Coordination during Threat Analysis .....	47
Table 4-2: Illustration of Vulnerability Assessment of the Governance Component .....	51
Table 4-3: Threat Likelihood Assessment Guidelines .....	56
Table 4-4: Guidelines for Conducting Threat Impact Evaluation .....	61
Table 4-5: Brand Value Evaluation Factors .....	62
Table 4-6: A Typical Threat Business Impact Evaluation .....	64
Table 4-7: A Typical ROI Computational Model .....	65
Table: 5-1: Profile of the Participants at Case and Mengo Hospitals .....	69
Table 5-2: Results of Expert Assessment of Likelihood of Unauthorized Access to Patient Data at Case Hospital Kampala .....	85
Table 5-3: Likelihood of Unauthorized Access to Patient Data at Mengo Hospital .....	86
Table 5-4: Business Analysts Conclusions on the Impact of Unauthorized Access to Patient Data at Case Hospital Kampala .....	86
Table 5-5: Business Analysts' Conclusions on Impact of Unauthorized Access to Patient Data at Mengo Hospital .....	86
Table 5-6: Quantitative Security Experts' Results from Two Case Studies .....	88
Table 5-7: Results of Evaluation by Business Analysts .....	89



## **1. Research Background and Approach**

---

*In order to design services that enhance healthcare information management system risk analysis, there is need to understand the threat analysis problem landscape. Therefore, this chapter introduces the threat analysis problem domain and presents the approach that was used to undertake the research. Section 1.1 presents the healthcare delivery challenges and section 1.2 discusses trends in healthcare service delivery, which include the application of ICTs to deliver services to remote patients. Section 1.3 presents remote patient monitoring system (RPMS) opportunities and section 1.4 discuss the RPMS concerns that must be addressed before the RPMS can be integrated in mainstream healthcare service delivery systems. Section 1.5 presents the research motivation and states the associated research problem. The research objective and questions are discussed in section 1.6 and in section 1.7 a research approach that was used to conduct the research is presented. The chapter ends with a presentation of the thesis organization in section 1.8.*

### **1.1 Healthcare Delivery Challenges**

According to the world health statistics report (WHO, 2013), Non-Communicable Diseases (NCDs), also known as chronic diseases, are the leading cause of death globally with 36 million deaths annually. The report (WHO, 2013), further indicates that about 9 million of all NCD deaths occur before the age of 60. The report also notes that about 80% of all NCD deaths occur in developing countries like Uganda. The high NCD deaths in developing countries are a result of growing economies, resulting into affluent lifestyle mainly by the middle class (Dalal et al., 2011). It is the affluent lifestyle that increases the NCD risk factors like tobacco use, physical inactivity, the harmful use of alcohol and unhealthy diets (WHO, 2013; Maher et al., 2010; Boutayeb, 2006).

Besides the increasing burden of NCDs, the global healthcare system is facing pressure from the rapidly expanding and aging global population (Jong-wook, 2013; Totten et al., 2013; WHO, 2012). According to the United Nations (UN, 2004), the global human population is projected at slightly over 7 Billion as of December 2012 and expected to reach 9.22 Billion by 2070. But research (UN, 2004; WHO, 2012; Totten et al., 2013) indicates that the rate at which healthcare professionals are being channeled into the industry is not proportional to the growing demand. For example in Uganda, the population is growing at a rate of 3.2%, an average of one million people per year (WHO, 2012; UN, 2004, p 206), yet the number of medical doctors graduating per year in Uganda is about 220 (Konde-Lule et al., 2007; Kinfu et al., 2009; Maseruka, 2010). According to the World Health Organization Report 2013 (WHO, 2013), the Ugandan case is not isolated. It is worth to note that, even

developed countries are facing shortage of healthcare professionals. According to Association of American Medical Colleges (AAMC) research (Kirch et al., 2012) the United States (US) is projected to have 62,900 fewer doctors than needed by 2015 and by 2025, that shortage is projected to likely double to about 130,600.

Besides the limited numbers of healthcare professionals, the healthcare industry is facing challenges of low investment in core infrastructure particularly in developing countries (WHO, 2013). Therefore, low investment coupled with the growing demand for healthcare services are stimulating healthcare service providers to find innovative solutions that can enable effective service delivery at 'optimal' costs.

### **1.2 Trends in Healthcare Service Provisioning**

In order to meet the growing demand of healthcare services, providers like hospitals are strengthening the Outpatient Case Management Scheme (OCMS) among other approaches (Totten et al., 2013). The OCMS aims at minimizing the duration of hospitalization of patients, that is hospitalize only when and as short as it is absolutely necessary. Reducing the hospitalization period has a wide range of benefits to both the patient and the hospital. The outpatient practice enables the hospital to use minimal resources to deliver services to a wider community. For example one nursing assistant can attend to ten outpatients in a day, but only a handful inpatients at the same time (Brian, 2013). To the patient, recovering from home means low costs of treatment, but also faster healing as research in (Karen & Prokesch, 2013) indicates that outpatients have a higher recovery rate than inpatients. Research in (Totten et al., 2013) also indicates that the healing process is greatly influenced by the psychological state of mind, which in turn is affected by the environmental conditions.

While the outpatient case management scheme offers a number of benefits, the scheme has its inherent challenges (Hickam et al., 2013). These include: poor adherence to prescription, inability of healthcare service providers to respond to sudden changes in patient state, lack of timely updates on the patient's physiological status and lack of patient medical history particularly in developing countries.

The decision to admit a patient or offer outpatient service is influenced by the perceived risks discussed above (Totten et al., 2013). Thus, hospitals are seeking for innovative healthcare information management systems like remote patient monitoring systems which can provide real-time patient physiological data at minimal risks to patients and hospitals (Shnayder et al., 2005).

### 1.3 Remote Patient Monitoring Systems Opportunities

The demand for remote patient monitoring information systems coupled by advances in low power radio technologies like Zig-bee (Zigbee-Alliance, 2012), integrated circuit designs (ChipCon, 2012), and sensing technologies (Xbow, 2013) have led to the development of *Wireless Sensors (WS)*. A generic wireless sensor can be viewed as a block of three functional modules: data acquisition, preprocessing, and communication modules and a utility power module (ChipCon, 2012). The data acquisition module encompasses algorithms that perform the sampling of patient's vital signs like temperature and heart rate. The preprocessing module performs *data structuring and filtering* while the communication module is charged with *sending and receiving of data packets*, refer to Figure 1-1.

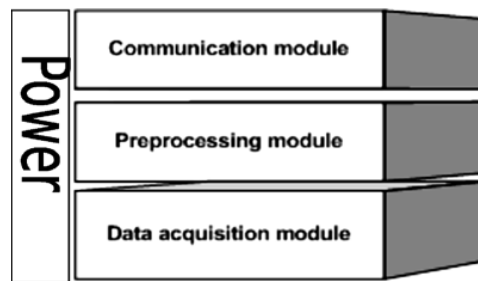


Figure 1-1: Structure of a Generic Sensor

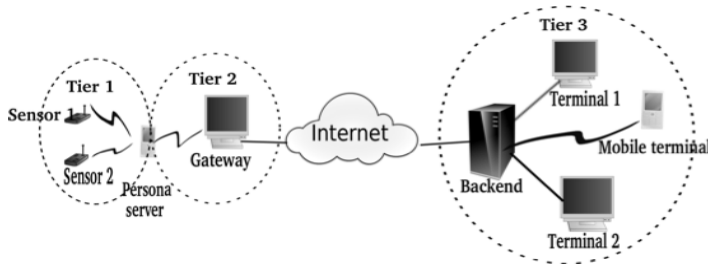
Motivated by capabilities of wireless sensors and opportunities to deploy them in mission critical applications, researchers have designed frameworks and models of their application across a wide spectrum of industries. Notable applications include: monitoring the physiological status of soldiers on the battlefield (Borsotto et al., 2004), monitoring of patients (MobiHealth, 2011; Shnayder et al., 2005; Tachakra et al., 2003), and tracking of animals in protected areas (Walters et al., 2006).

#### The Architecture of Remote Patient Monitoring System

A generic Remote Patient Monitoring System (RPMS) can be viewed as an integrated Healthcare Information Management System (HIMS) consisting of a set of wireless sensors, personal server, and communication links and a patient record database. A healthcare information management system refers to an information system “that captures, stores, manages or transmits information related to the health of individuals or the activities of organizations that work within the health sector” (Pacific Health Information Network, 2011, par 1). Wireless sensors on a patient sample and relay data to a **personal server (PS)**, which in turn relays the patient data to a patient record management system at the hospital



(Kambourakis et al., 2007). The PS is a high performance device with greater computing capabilities than ordinary sensors. Some of the devices that perform PS roles include; smart phones and tablets. The personal server is normally the local network controlling entity (Pfleeger & Pfleeger, 2003) for the network. The personal server aggregates and coordinates the flow of data between sensors, itself, and the core remote data processing infrastructure (a patient record management information system). In addition, the personal server offers capabilities of long distance transmission of data to hospital data centers or cloud services. In most remote patient monitoring systems like ClinicMaster, the personal server establishes communication sessions, assign sensor IDs, distribute security keys, and manages channel access. ClinicMaster is an integrated new generation health information management system (HIMS) which automates patient transactions in a hospital (Kutegeka, 2014). The system aggregates and indexes patient records and provides access to patient records to services provides on a variety of platforms. Furthermore, the system alerts the healthcare services providers about the patient's physiological condition using remote patient monitoring application via smart application system integration like the Samsung smart watches (Kutegeka, 2014). Figure 1-2 present a generic architecture of a typical remote patient monitoring system.



*Figure 1-2: A Generic Architecture of a Remote Patient Monitoring System*

When monitoring patients, wireless sensors are deployed on the body of the patient as tiny accessories like rings, watches, and buttons to pick vital physiological data from the patient (Jin et al., 2010; Kartsakli, et al., 2013). The current capabilities of medical sensors include; measurement of temperature, oxygen saturation in the blood, heart rate, acceleration, blood pressure and location tracking (Kartsakli, et al., 2013).

In general, RPMS encompasses a network of wireless sensors worn on the body of the patient (Tier 1) that connect to the base station, which in turn connects to a patient record management server via communication technologies like fiber, 3G, and Wi-fi among others. Sensors that make up the network at Tier 1 include: motion sensors, heart rate monitor, blood pressure monitor, oxygen level monitor, and temperature sensor among others.

Tier 2 encompasses the base station, which aggregates sensor readings, provides a graphical user interface (GUI) to support human-device interaction and links Tier 1 devices to Tier 3 infrastructure. Tier 3 encompasses a patient record management system and end-user terminals which enable healthcare service providers to access patient's data from sensors, integrate with a patient medical record, consult, as well as deliver the healthcare service like prescription, see Figure 1-2. To enable our readers visualize the application, we describe a typical application scenario in the following section.

### **RPMS Application Scenario**

In a typical RPMS deployment, a patient wears on-body sensors, which collects and relays their data in real-time or near real-time to patient record management system at the hospital (Kambourakis et al., 2007). To put this scenario into perspective, we present a case study of a stroke patient under rehabilitation who we shall call David.

*David is recovering from a stroke and his physician has prescribed to him a routine behavior pattern involving moments of rest and exercises. In order to offer more specialized care, David is admitted in a stroke rehabilitation center (hospital) for the first month. In the rehabilitation center, David must wear tiny sensors on his wrist watch that monitor his vital physiological status, and relay the data to his physician in real-time via ClinicMaster system.*

*After making some improvements, David is given some medications, discharged from the rehabilitation center and put under remote patient monitoring (outpatient management scheme). To enable David's physician receive real time updates on his physiological status, David wears sensors monitoring his location, heart rate, motion and temperature linked to his smart-phone application via blue-tooth.*

*As part of his routine exercise, David normally takes an evening walk around his neighborhood. On weekends, David joins his family for weekend shopping and other family activities to accelerate his healing. At times, David uses public transport to visit his friends and siblings in a nearby town on his own. When data is received at the healthcare service provider's infrastructure (ClinicMaster), it's relayed in real-time to David's doctor via a Clinic Communicator mobile application on the doctor's phone.*

The aforementioned scenario exposes the patient to a number of threats including: breach of personal privacy of a patient, integrity of medical records, and denial of service among others. Therefore, there is need to determine the system vulnerabilities, assess the likelihood of threats, and evaluate the threat business impact on the hospital running the information

system. Furthermore there is need to ascertain the efficiency of possible threat mitigation controls.

### 1.4 RPMS Issues

In healthcare service delivery, the guarantee of integrity, confidentiality, and availability of data upon which doctors make key decisions on case management is critical (Moshaddique & Kyung-sup, 2011). Therefore, the remote collection, collation and dissemination of patient data over public infrastructure outside the control of hospitals raises privacy, security, ethical and legal concerns about patient data (Kambourakis et al., 2007; Kumar & Lee, 2011; Gao et al., 2008; Moshaddique & Kyung-sup, 2011). A very important question is who carries the legal liabilities associated with data sampled from a patient at remote location over RPMS infrastructure in event of data misuse or poor decision making due to inaccurate data or lack of it? (Meingast et al., 2006; Gillon, 1994). Other critical questions that are being asked are: how can patient safety and privacy be guaranteed in such an environment and how insecure are remote patient monitoring systems (likelihood of threats and what would be their impact on hospitals).

Due to the fore mentioned concerns, hospitals are reluctant to integrate remote patient monitoring systems into mainstream hospital management information system despite their apparent potential to address outpatient care challenges (Hernandez, 2014; Rahman, 2005; Alasdair et al., 2008; Herrick et al., 2010; Sharon et al., 2012). The inertia to adopt remote patient monitoring systems has attracted attention of security management researchers as shown by the amount of literature published (Gillon, 1994; Kambourakis et al., 2007; Kumar & Lee, 2011; Gao et al., 2008; Moshaddique & Kyung-sup, 2011). Thus, approaches are advancing from two schools of thought: (1) Adaption of existing security management controls to remote patient monitoring systems (Undercoffer et al., 2002; Chan et al., 2003) and (2) definition of a new set of security management approaches (Anderson et al., 2004; ).

Broadly, *security management* is a field of management that focuses on asset management, physical security and human resource safety functions within an organization (Walsh, 2002). It entails the classification of organization's information assets, *analysis of threats*, development, documentation and implementation of policies, standards, procedures and guidelines to ensure secure consumption of services. On a technical level, the field deals with design and deployment of *security protocols* to offer services of authentication, confidentiality, integrity, privacy and none-repudiation (Walsh, 2002).

## Threat Analysis Overview

The effectiveness of a security management approach depends not only on the soundness of cryptographic primitives and security protocols but also on a pragmatic threat analysis approach (Saunders, 2007; Dolev & Yoa, 1981). Therefore, to design sound security controls (*threat mitigation controls*), one has to identify vulnerabilities in the information system, establish the nature of a threat, assess the likelihood of a threat and evaluate the threat business impact. It is common to find vulnerabilities in information systems because of oversights in the threat analysis process. Furthermore without empirical quantification of threat impact, information system managers find it difficult to convince top management in organizations to invest in threat mitigation controls (Keen, 2011).

Therefore, a number of threat analysis approaches have been proposed including; attack net (McDermott, 2001), security patterns (Steffan & Schumacher, 2002; OWASP, 2013), STRIDE (Shawn et al., 2006), Dolve-Yoa Mode (Dolev & Yoa, 1981), and attack trees (Schneier, 1999; Sjouke & Oostdijk, 2006). However, most of the existing techniques lack adequate expressiveness and semantics to enable reasoning about threats likelihood and impact, hence making the development of appropriate security controls difficult (Sjouke & Oostdijk, 2006). It is also fair to say, that most of the current approaches focus on threat visualization at the expense of systematic guidelines to facilitate threat identification, quantification and impact assessment.

In general, the quality of threat models largely depends on the knowledge and expertise (*tacit knowledge*) of the security analyst and his ability to incorporate this knowledge in the assessment of threat likelihood and impact (Kordy et al., 2011). Most of the current threat analysis approaches lack capabilities of incorporating *background knowledge* in the assessment of threats. Even techniques that have semantics are complex, making their use in regular practice difficult (Mirembe & Muyebe, 2008). Therefore, there is need to develop threat analysis approaches that allow incorporation of background knowledge into the analysis of threats, quantify their impact on the business but at the same time be simple to use. Questions like; where is the source of the threat? How big is the threat? How likely is the threat? Who will be affected? What can be done to mitigate the threat and at what cost?. Need to be addressed by a useful threat analysis approach.

## 1.5 Motivation and Research Problem

Based on the discussion so far, we can state that we were inspired to carry out the research discussed in this thesis because of the following:

We observe that there is a growing demand for healthcare services mainly fueled by the expanding and aging population (Jong-wook, 2013; Totten et al., 2013; WHO, 2012). To meet the demand, most hospitals are strengthening outpatient case management, using technologies like RPMS so as to address challenges of: poor adherence to prescription, inability to respond to sudden changes in patient state, and lack of timely updates on the patient's physiological status (Hickam et al., 2013).

However, the adoption of RPMS largely depends on the appropriate assessment of inherent risks and implementation of mitigation controls (Moshaddique & Kyung-sup, 2011). While the design of RPMS security protocols has gained a lot of attention in recent years as per the amount of literature published on the subject, little attention has been given to the design of approaches to guide the determination and quantification of threats. Thus, the inspiration to enhance threat analysis was induced by the limitations in the current threat analysis approaches that often result into definition of inadequate security controls (Pfleege & Pfleege, 2003; Dermott, 2001). Accordingly, this thesis seeks to contribute to a better understanding of risks to information systems in general. Therefore, we reason that, the slow adoption of RPMS by hospitals is in part due to perceived risks owed to the lack of a threat analysis approach.

It is important to note that most of RPMS security management approaches in literature have largely focused on development of security protocols at the expense of threat analysis approaches that would facilitate decision making on threat likelihood, impact and optimal investment on mitigation controls.

### **1.6 Research Objective and Questions**

Despite concerns about RPMS security management, little attention has been paid to the development of threat analysis approaches to facilitate collaborative threat identification and impact assessment. Accordingly, the research objective of this thesis is to develop a threat analysis approach to facilitate collaborative threat analysis among security experts and business analysts. Consequently, the key research question this thesis seeks to address is:

*“How can healthcare information systems threat analysis be enhanced?”*

In order to provide specific directions to guide the execution of the tasks, we derive four specific research questions from the main research question, which are:

1. What challenges do threat analysts' face?

2. What are the key steps in analyzing threats to an information system?
3. What would be the key characteristics of a threat analysis approach?
4. What are the ideal parameters for evaluating a threat analysis approach?

## 1.7 Research Approach

A research approach refers to methods that have been adopted to conduct the research. Venable (2006) describes a research approach as a family of research techniques and tools that drive actions and interpretation during the research. The nature of the problem and the anticipated solution are some of the determinants in the selection of an appropriate research approach (Guba & Lincoln, 1994). Generally, the research approach outlines a research philosophy (the underlying line of thinking) and the research strategy (plan of action) (Aregu, 2014). In this section we describe the research philosophy and strategy used in exploring and understanding the threat analysis problem and developing the Threat Nets Approach.

### Research Philosophy

The selection of a research philosophy has to be guided by the research questions, objectives, and the underlying philosophical foundations that uphold the research field (Burrell & Morgan, 1979). According to Flowers (2009), a research philosophy is a school of thought that guides the execution of the research. Each philosophical position has a distinct view of explaining reality (*ontology*), knowledge (*epistemology*) and values (*axiology*) (Guba & Lincoln, 1994). According to Burrell and Morgan (1979), developing a philosophical position requires a researcher to make some logical assumptions concerning *the nature of society and science* as different philosophical positions yield different results. Saunders et al. (2007), observe that it is imperative that researchers discuss their understanding of the philosophical positions in order to logically justify the philosophical stand of their inquiry.

This research uses design science research philosophy advanced by Hevner and Chatterjee (2010). Design science is an information system research philosophy in which questions relevant to human problems are addressed through the creation of innovative artefacts (Hevner & Chatterjee, 2010; Hevner, 2007). According to Knol (2013), “the science in design science lies in the notion that knowledge and understanding of the design problem and its solution are acquired in the building and application of an artifact” (p11). Design science research seeks to invent new innovative artefacts (*i.e., constructs, models,*

*methodologies and instantiations*) for solving wicked problems (Hevner et al., 2004; Venable, 2006). Hevner et al., (2004) describes wicked problems as those that are characterized by: unstable requirements, complex interactions among elements of the problem and solution set, critical dependence on human tacit knowledge to produce effective solutions, and reliance on human social abilities to create useful solutions. Thus, design science research involves the analysis of the environment to synthesize requirements, design of artefacts based on the requirements and the eventual evaluation of artefacts (Hevner et al., 2004; Knol, 2013).

According to Gonzalez and Sol (2012), it is essential that a researcher using design science philosophy takes an epistemological and ontological stance that affects “the way the validation strategy is conceived, and later on, accepted or rejected” (p403). Burrell and Morgan (1979) observed that various philosophical positions can broadly be categorized as either objectivism or subjectivism depending on the underlying assumptions the investigator makes about the nature of reality. Objectivism based research normally focuses on the identification and definition of elements and expression of relationships among them (Burrell & Morgan, 1979). While subjectivism promotes the notion that reality is restricted to an individual’s consciousness (i.e., simply put, reality does not exist beyond oneself). The two ontological positions led to three major epistemological paradigms of research philosophies in information systems; *positivism*, *interpretivism*, and *pragmatism* (Knol, 2013; Gonzalez & Sol, 2012).

*Positivism* is rooted in behavioral science and seeks to develop theories that explain or predict causal relationship in the social world. Positivists generally assume that reality is objectively given and can be described by measurable properties which are independent of the observer (researcher) and his or her instruments (Gonzalez & Sol, 2012; Aregu, 2014). Positivist studies generally attempt to test theory, in an attempt to increase the predictive understanding of phenomena (Smith, 1998). Orlikowski and Baroudi (1991, p.5) classified information system research as positivist if there was evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population. The critiques of positivism argue that it restricts the study of reality to formularized constructs of science governed by universal laws, while disregarding introspective and intuitive knowledge (Hirschheim, 1992; Cohen et al., 2007; Knol, 2013).

On the other hand, *interpretivism* seeks to explain contextual knowledge and the interpretation of reality by an individual based on experiences (one's view of reality) (Guba & Lincoln, 1994). According to Aregu (2014), interpretivism focuses on gaining an in-depth

understanding of the phenomena in context of people's values and beliefs instead of generalization of the natural world as advanced by positivism. Interpretivism relates to the ontology position of relativism which "holds that reality is a subjective construction of the mind" (Knol, 2013). This epistemology stand is relevant particularly when it comes to threat analysis, since the analysis of threats extensively depends on the *tacit knowledge* of the security analysts. Interpretivism is critiqued for being subjective and lacking any form of scientific generalization (Cohen et al., 2007; Mack, 2010).

Rorty (1999) introduced a third dimension of epistemology called *pragmatism*. Pragmatists argue that the purpose of science is not just to understand reality but rather to create useful knowledge. Proponents of pragmatism shift focus from knowledge as reality of the natural world to knowledge as tool of action (Hookway, 2012; Cornish & Gillespie, 2009). Pragmatist observe that a piece of knowledge should not be judged on the yardstick of truth but on its usefulness to address a given need. Pragmatism epistemological position relates to the ontology position of critical realism which accept relativism of knowledge in the social world (Knol, 2013; Kilpinen, 2008). Because of the action nurture of pragmatism, the epistemology position forms an important part of action research which focuses on addressing specific human problems (Goldkuhl, 2012). Opponents of pragmatism argue that the epistemology position is not grounded in common philosophical stands as such the validity of knowledge created can be contested by mainstream researchers (Orlikowski & Baroudi, 1991; Knol, 2013).

In order to address the main research question of this study, which is "*How can healthcare information systems threat analysis be enhanced*", this design science research adopts interpretivism with a pragmatic epistemological stance. Given our research goal, interpretivism fits well with this study as it seeks to understand the contextual methods, theories and values threat analysts rely on when analyzing threats to healthcare information systems. Pragmatism is suitable because the study seeks to develop practical knowledge in form of an approach that will enhance a threat analysis process.

### **Research Strategy**

Given the ambiguity of the threat analysis problem, this research adopted a strategy that was aimed at formulating a theory that would best explain the threat analysis phenomenon. The research adapted Sol's four stage inductive hypothetic research strategy as depicted in Figure 1.3 (Sol, 1982) to implement our design science research philosophy.



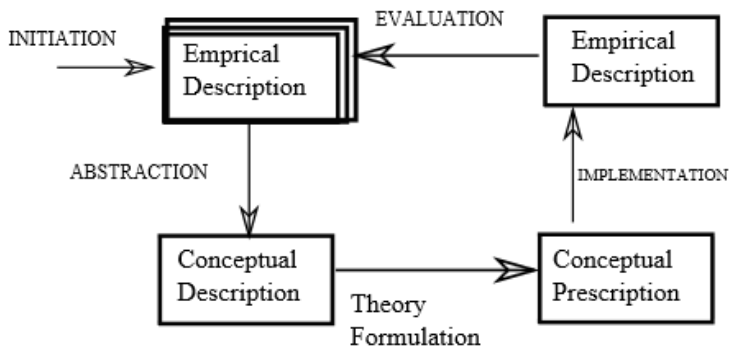


Figure 1-3: The Inductive Hypothetic Research Strategy (Sol, 1982)

### Initial Phase

The *empirical description* was aimed at gaining the understanding of the underlying healthcare information system threat analysis challenges, requirement for a threat analysis approach and the establishing variable for approach evaluation (*problem domain definition*). The empirical description was achieved through an extensive exploratory study, which involved literature review, semi-structured interviews and surveys among security experts in Uganda. The goal was to get an understanding of threat analysis process. We conducted an exploratory study to determine threat analysis process flow, challenges and areas of improvement (*threat analysis approach requirements*). The exploratory study involved the interaction with security experts who analyze threats and define security management controls. In order to confirm that the observed threat analysis gaps have not been addressed earlier, an extensive literature analysis on various threat analysis approaches was conducted. It is also important to note that the literature review helped us identify theories applicable in the solution domain (addressing research questions (2) and (3)).

### Abstraction Phase

Information from the initial phase was analyzed and resulted into the abstraction of essential aspects of the threat analysis process and the associated threat analysis approach requirements.

### Theory Formulation Phase

Aware of the fact that threat analysis is both a *process and human issue*, Sol's framework (Sol, 1982) was used to develop a prescriptive conceptual model that describes the elements of the solutions set in terms of the way of thinking, way of modelling, way of governance and way of working. Key theories like *attack trees* (Schneier, 1999), probability theory and

Keller's brand index approach (Keller, 2003) are applied in the quantification of threat likelihood and impact. Accordingly, the development of the Threat Nets Approach is introduced and grounded.

### **Implementation Phase**

In this phase, a web based Threat Nets based tool was implemented. The tool was designed to facilitate the use of the approach. The implementation phase also involved the application of the Threat Nets Approach to analyze threats to the ClinicMaster System at Case Hospital Kampala and Mengo Hospital as case studies.

### **Evaluation Phase**

During the *evaluation phase* different components of the approach were evaluated to ascertain their completeness, usability (ease of use and learnability) and usefulness. The approach was evaluated by a team of 14 security experts and business analysts.

## **1.8 Thesis Organization**

This thesis is organized into 6 chapters. Chapter 1, presents the background to the research domain and introduces various contextual issues in the areas of outpatient case management in general and healthcare information system security management in particular. The research problem is identified and its relevance stated. The research questions are identified and their associated research objective defined. The chapter presents a research approach that guided the processes of conducting the research.

In Chapter 2 a detailed review of the current state of art and practice in the field of threat analysis is discussed. The discussions are based on literature study. The chapter presents threat analysis processes, decisions that matter during threat analysis and approaches of enhancing the threat analysis process.

Chapter 3 presents the exploratory study among security experts in Kampala. The exploratory study was conducted to ascertain the correlation of observation in literature and actual practices by experts. The chapter presents the approach to the study and discusses the associated results. The chapter concludes with a discussion of requirements for an ideal threat analysis approach for healthcare information management systems.

Using the findings in Chapters 2 and 3, the Threat Nets Approach is formulated in Chapter 4. The approach is described using Sol's "Ways of "framework (Sol, 1982) in terms of; the

way of thinking (which presents the underlying theory), way of governance, way of modeling and way of working.

Chapter 5 specifically describes the evaluation schemes used to evaluate the completeness, usefulness and usability of the approach. The chapter concludes with the discussion of the evaluation results.

Chapter 6 summarizes the entire research in terms of: research approach, research contributions, limitations the researcher faced and lays out the future research direction in information system risk analysis in general.

## 2. Understanding Threat Analysis

---

*As a basis for grounding the research, this chapter discusses the current state of art and practice in analyzing threats to information systems. Section 2.1 presents methods used to understand the threat analysis phenomenon. Section 2.2 presents a discussion on the threat analysis process and the associated theories of process enhancement. Section 2.3 presents and discusses current threat analysis approaches and their associated limitations. The current threat analysis approaches fall into three categories; attack-centric, system-centric and asset-centric. These approaches do not provide logical techniques of assessing threat likelihood, impact and cost-effectiveness of threat mitigation controls. Thus, conclusions (decisions) on threat likelihood, threat impact and cost-effectiveness of threat mitigation controls are largely based on expert's intuition. We observe that such decisions suffer from natural bias of experts and poor synthesis of information on threat agents and system vulnerabilities. In section 2.5 requirements for an ideal threat analysis approach are established basing on literature study.*

### 2.1 Approaches to Understanding Threat Analysis

To understand how threats are identified and assessed, an extensive literature study was conducted. The literature study followed Levy and Ellis (2006) systematic scanning approach in which relevant journals, conference papers, and technical reports were examined. The goals of the literature study were to: gain understanding of the threat analysis process, establish decisions that matter, understand the challenges threat analysts face in making decisions and establish the desired characteristics of an ideal threat analysis approach for a healthcare information management system. The literature study was also meant to establish key theories upon which an ideal threat analysis approach can be developed. Simply put, the focus of literature study was to gain an in-depth understanding of the problem domain and characteristics of a possible solution. Emphasis was put on recent publications in high impact journals, conferences and books from key authorities in the area of information security and risk management. Special attention was given to studies focusing on risk analysis in healthcare information systems and challenges faced by threat analysts in general. Literature in the broader field of auditing was reviewed to gain an understanding of applicable theories of risk analysis decision enhancement services.

## 2.2 A Threat Analysis Process

According to Walsh (2002) and Fay (2007), threat analysis is a core process of information system management which focuses on *identification and quantification* of threats. Pfleeger et al. (2003) and Oladimeji et al. (2006) described threat analysis as a *goal oriented process* which deals with threat identification, quantification and mitigation of threats to assets. VMWARE (2013), describes threats analysis as a decision process through which security analysts have to decide on threat likelihood and its associated impact on the organization. Furthermore, threat analysis involves making decisions on cost-effective mitigation controls which makes it an integral part of IT investments decision-making process in organizations like hospitals (VMWARE, 2013). Shawn et al. (2006) states that the goals of analyzing threats are to identify and quantify all possible threat agents to an asset, in addition to the definition of cost effective threat mitigation controls. In healthcare information systems, an asset is any resource of value like software and patient data that can be compromised (Hernandez, 2014; Kumar & Lee, 2011; Pfleeger & Pfleeger, 2003). Pfleeger and Pfleeger (2003) defines a threat agent as any actor/event which has a potential to exploit information system vulnerabilities to cause harm to the system and its users. Vulnerabilities are weaknesses within the information system that threat agents can exploit (OWASP-RRM, 2014).

Walsh (2011) observed that threat analysis in healthcare information systems is a demanding task characterized by either limited information or information overload about threat agents and system characteristics. Consequently, Walsh proposed a nine step practical guide of conducting threat analysis based on the Risk Management Guide for Information Technology Systems 800-30 series (NIST, 2012). The 9 steps are; system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact determination, mitigation control definition, documentation and communication. The aim of the practical guide was to help hospitals comply with the complex Health Insurance Portability and Accountability Act (HIPAA) of 1996, which prescribes stringent patient data security and privacy requirements for healthcare information systems (Walsh, 2011). The practical guide also seeks to establish a framework of linking system characteristics to likelihood of threats (Walsh, 2011). Simply put, Walsh's (2011) practical guide is an attempt to enhanced security experts' decision making abilities on threats to healthcare information systems. While the practical guide provides sequential steps on how to analyze threats and identifies key information sources, the guide does not provide techniques for quantifying the likelihood of threats and their associated impact. Furthermore, the practical guide does not provide sound quantitative technique for assessing cost-effectiveness of threat mitigation controls.

The Information Systems Audit and Control Association (Canon, 2011) studied the relationship between system characteristics, vulnerabilities and threats and observed that threat likelihood depends on the likelihood of vulnerability exploitation. That is to say, the likelihood,  $P(T)$  of a threat  $T$ , is directly proportional to the likelihood of vulnerability exploitation,  $P(E)$ . We observe that the likelihood of vulnerability exploitation is dependent on the likelihood of flaws in the system characteristics of: governance, software properties, and human resource competencies. Thus, the assessment of threat likelihood should factor in the existence of flaws in the system characteristics in a logical manner.

According to OWASP-RRM (2014), threat impact can be measured based on technical and business factors. Technical factors focus on estimating the impact on confidentiality, integrity, authentication and availability of system services. While business factors aim at estimating the impact of threats in financial terms. VMWARE (2013) reasoned that visualizing threats to information systems in terms of financial costs improves decision making on IT investments in an organization. Walsh (2011) and Canon (2011) observed that the fundamental failures in information security management is due to unrealistic estimation of risks and their associated impact to the organization. The unrealistic evaluation of risks is in part due to heuristics decision making by threat analysts due to lack of logical information on threat agents profile and system characteristics. According to Westervelt (2011), "Many organizations are generally not assessing things from the likelihood of impact perspective, which is a purer form of risk measurement." Schneier (1999) and Westervelt (2011) reason that visualizing threats in empirical quantities improves decision makers' understanding of the magnitude of the risk resulting into better decisions on threat mitigation controls.

### **Threat Analysis Theoretical Insights**

Walsh (2011) reasons that to enhance the threat analysis process one has to understand how security experts analyze threats to healthcare information management systems. Theoretically, security experts are assumed to have sufficient information about the system characteristics and threat agents to make sound judgment about threat likelihood and impact (Canon, 2011). However, given the complexity of the threat analysis process that involves extensive scanning of both the internal and external environment of an information system, security experts have to rely on their tacit knowledge in the assessment of threat likelihood and impact (Walsh, 2011; Bayne, 2002). The lack of sufficient information and knowledge often results into poor understanding of threat likelihood and impact (Bayne, 2002; Canon, 2011; Kordy et al., 2011).

Aregu (2014) noted that information is a critical requirement in any decision making process and reasons that the provision of clear and concise information is one way of enhancing a decision making process. According to Aregu (2014) decision making is an execution of choice among alternatives based on available information. Walsh (2011) states that availability of information and knowledge about the system characteristics and threat agents is one of the most important success factors for analysis of threats in healthcare information systems. Therefore, providing information and knowledge on how to analyze threats in healthcare information systems in form of guidelines and techniques of computing threat likelihood, impact and return on investment is one way of enhancing the threat analysis process.

Accordingly, this study is grounded in two theories; decision enhancement theory (Keen & Sol, 2008) and risk management theory (Kwo-Shing et al., 2003). Keen and Sol (2008) state that decision enhancement aims at enhancing human decision making through decision process enhancement and the provision of studios to facilitate collaboration and change management. Decision enhancement is grounded in decision support system theory which focuses on supporting humans to make better decisions (Knol, 2013). The thrust of enhancing threat analysis process is to gain better understanding of threats to information system assets. Amiyo (2012) observed that in the field of risk management, decision support system theory is one of the anchor theories, since the main output of risk analysis processes are decisions on threat likelihood and impact. This study takes the process enhancement perspective of the decision enhancement theory because it seeks to enhance the threat analysis process by developing an approach that guides security experts on how to make better decisions on threat likelihood, threat impact and cost-effectiveness of threat mitigation controls.

The second theory that informs this study is the risk management theory which suggests “that through organization risk analysis and evaluation, the threats and vulnerabilities to information systems could be estimated and assessed” (Kwo-Shing et al., 2003 p.244). The results of risk analysis are important in facilitating decision making on threat mitigation control investments in a hospital (Vellani, 2006; Houlding et al, 2012). In the analysis of threats to a healthcare information management system, it is important to have a holistic organizational assessment of people, governance framework and the technology components of the information system (Vellani, 2006; Pardue & Patidar, 2011). It is worth noting that each component has a potential to introduce vulnerabilities that can increase the likelihood of threats (Samy et al., 2010; Houlding et al, 2012).

## 2.3 Threat Analysis Approaches

Contemporary threat analysis approaches fall under three categories; system-centric (Shostack, 2008; Lanzi et al., 2010), attacker-centric (Schneier, 1999) and asset-centric (Hyla et al., 2012; Ongtang et al., 2012). Generally all threat analysis approaches involve the identification of assets, system boundary mapping and decomposition, threat identification and vulnerability identification (Mockel & Abdallah, 2010; Shostack, 2008).

### System-Centric Approaches

System-centric approaches focus on identification of system vulnerabilities or faults. The security expert employing system-centric approach aims at capturing system design and deployment flaws which can be exploited by an unauthorized entity (Ongtang et al., 2012). In the system-centric approach, a security analyst steps through the system architecture looking for vulnerabilities against each component of the design, operational configurations and policies (Lanzi et al., 2010). The approach is the oldest technique of identifying vulnerabilities of a system and it has been extensively employed by mechanical engineers in the development of safety critical systems. The approach uses fault trees to visualize threats (Brooke & Paige, 2003; Ezell et al., 2000; Paté-Cornell, 1984).

Fault trees are a graphical representation of system failures (Paté-Cornell, 1984). The failures represent system vulnerabilities which are interpreted as threats to the secure operation of the system. Fault trees were first published in the 1960's and have since then been employed by mechanical engineers in the analysis of system faults in mission critical systems (Vesely et al., 1981). Figure 2-1 illustrates a typical example of a fault tree analysis of a failed access to e-mail services. Gate O indicate an OR gate (which indicate that the fault above the gate while occur if one of the pre-conditions below the gate are true) and gate A indicate an AND gate (which indicate that for the fault to progress all the pre-conditions below the gate must be true).

In Figure 2-1, failure to access an e-mail could be a result of a faulty network switch, cable or mail server. But for a mail server to fail, both the software and hardware must have faults.

According to Paté-Cornell (1984), a node in the fault tree represents an event and the edges represent a causal-effect relationship between events. Leaf nodes are linked to the higher nodes in the hierarchy via logic gates which represent transformations. In Figure 2-1, symbols marked with O (OR-gate) and A (And-gate) represent logic gates.



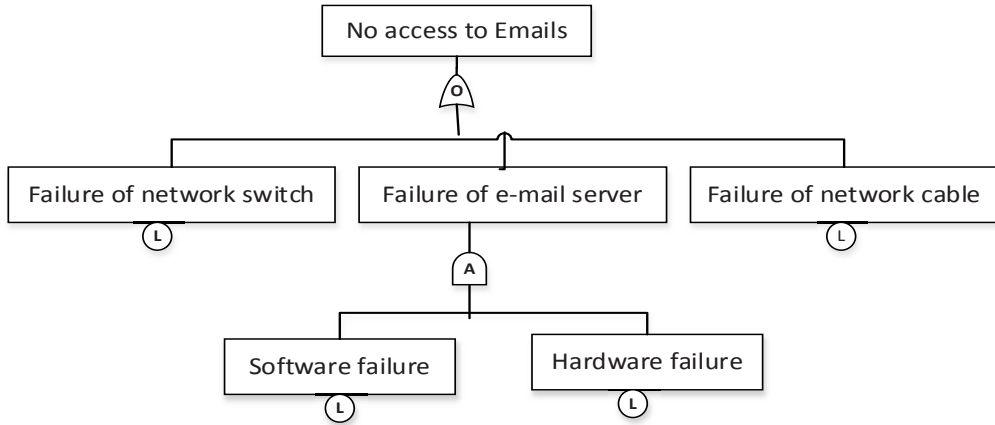


Figure 2-1: A Fault Tree Analysis for an E-mail Service

None-leaf nodes represent identified hazards for which predicted reliability of data is required, these are marked with L in Figure 2-1. Just like attack trees, intermediate nodes and leaf nodes represent refinements of a given fault or vulnerability (Schneier , 1999).

Approaches that use fault trees do neither provide mechanism of assessing fault likelihood and impact nor do they identify threats that can exploit the vulnerability. Furthermore, fault trees do not capture atomic details about the threat like attacker tools, knowledge, experience, motivation and goals, which is vital in the computation of threat likelihood and impact. The limitations of fault trees is what inspired the development of attacker centric approaches like attack trees and attacker nets (Schneier, 1999; McDermott, 2001).

### Attacker-Centric Approaches

Attacker-centric approaches are those that focus on profiling the invader motivation, goals and capabilities. Attacker-centric approaches use attack trees to visualize the various pathways by which invaders can compromise the security of the asset (Schneier, 1999; Sjouke & Oostdijk, 2006).

Schneier (1999) proposed attack trees, a directed graph based approach of how to profile progression of attacks on an asset (Figure 2-2). In an attack tree every node in the graph represents an adversary goal and the root node represents the overall goal that the invader must achieve. Intermediate nodes in the graph represent sub-goals called (refinement of its parent goal) the adversary has to accomplish in order to achieve the main objective. Leaf

nodes in the graph represent the atom of an attack i.e., sub-goals or goals that cannot be refined any further.

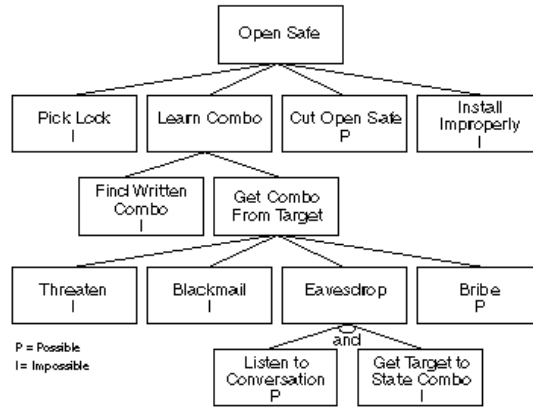


Figure 2-2: Attack Tree Example (Schneier, 1999)

Attack trees have simple semantics to allow the propagation of costs an invader must incur to achieve a given task which provides a framework of computing threat likelihood.

However, semantics for attack trees have limited internal structure and cannot facilitate logical reasoning about the threats (Sjouke & Oostdijk, 2006). For example which event can have more impact yet has low probability of occurrence? How is the existence of a vulnerability related to threat likelihood? How can the impact of the threat be measured? How to account for existence of defense measures (Kordy et al., 2011)? Thus, as much as attack trees are appealing to the security research community at conceptual level, there is need to enhance their structure in order to address the aforementioned concerns which are of practical importance to threat modelers. In addition, the attack tree approach does not provide an avenue of incorporating system specific details like existence of known vulnerabilities or history of exploitation in the computation of threat likelihood and impact (Kordy et al, 2011; Mirembe, 2008). A pronounced advantage of attack tree is the simplicity of representation. This is the reason they are very popular in the field of system security research but not in practice (Sjouke & Oostdijk, 2006). Like fault trees, attack trees do not address the fundamental challenges of threat analysis that include; lack of information, inability to measure the impact of threats, and lack of collaboration among stakeholders.

Another notable formal approach is attack nets proposed by McDermott (2001) that aims at improving the expressiveness of attack trees. Attack nets present a significant departure

from fault based analysis by separating *events* from *goals*. The separation of events from goals enhances the descriptive power of the representation, hence allowing the security analyst to investigate atomic components of attacks.

Despite the expressiveness of attack nets, the semantics of synthesizing information captured in the structure are not well defined (Mirembe & Muyeba, 2008). For example, when are two attack paths equal? How is the contribution to the overall goal computed? How is knowledge of known system vulnerabilities incorporated in the assessment of threats (Sjouke & Oostdijk, 2006; Kordy et al., 2011)? These unanswered questions are inspiring more research in the areas of threat analysis.

### Asset-Centric Approaches

According to Shostack (2008), asset-centric threat analysis often involves some level of risk assessment, approximation or ranking. Assets are classified according to their sensitivity and inherent value to a potential attacker, in order to prioritize risk levels (MyAppSecurity, 2012). Analysts using asset-centric approaches mainly use summative ranking of low, medium and high to estimate the level of risk.

Given the complexity of formal approaches, Shawn et al., (2006) proposed the STRIDE approach. The approach is derived from the understanding that the attacker goals can be one or more of the following; **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of services and **E**levation of privileges (STRIDE) (Scandariato et al., 2013). While STRIDE can be used to classify threats, it does not provide a scheme of identifying sources of threats, computing their likelihood or measuring their impact (Scandariato et al., 2013). In simple terms, STRIDE is a threat classification framework (Pendergrass et al., 2013).

Trike is another asset-centric approach proposed to construct threat models (Saitta et al., 2005; Mockel & Abdallah, 2010). Trike mainly focuses on definition of security requirements for each asset and the enumeration of threat. Once threats are identified, appropriate risk values are assigned to them by the expert and attack graphs created (Saitta et al., 2005). The analyst can then assign threat mitigation controls on the established threats. Once this process is completed, a risk model is created based on assets, roles, actions and threat exposure (Saitta et al., 2005). Trike has similarities to the STRIDE approach, but it differs in that it uses a risk-based tactic with distinct implementation, threat, and risk models. The Trike approach lacks documentation and use base. Therefore, its completeness and usefulness cannot easily be determined.

### Summary on Current Approaches

From the discussion so far, we observe that a typical threat analysis process involves identification of threats and vulnerabilities, quantification of threats and definition of threat mitigation controls. Current approaches neither provide sound techniques of assessing threat likelihood nor do they support collaboration among security experts and other stakeholders. Furthermore, they do not provide techniques of computing threat business impact on an organization. In addition, they lack a logical scheme of assessing the influence of system characteristics on the likelihood of threats.

## 2.4 Threat Analysis Decisions that Matter

From the works of the Center for Audit Quality (CAQ) (2014), the threat analysis process can be viewed as a judgment process that involves five basic actions which auditors (threat analysts) execute to arrive at a sound professional judgment. The actions are: identifying key issues (vulnerabilities and threats), gathering the facts, analyzing information, making decisions on threats, and documentation of conclusions (decisions). Below is a detailed discussion of the above listed actions.

- **Identifying key issues:** one of the very first actions a threat analyst undertakes is to identify and define vulnerabilities and threat agents. This action is complex since it depends on the threat analysts' ability to consider issues from multiple perspectives and making assumptions that might contradict normal assertions about threat agents (Mockel & Abdallah, 2010; Lanzi et al., 2010). The success of this action largely depends on the expert's intuition, experience and understanding of the information system under review. This action also involves the definition of security goals upon which the threat assessment is benchmarked.
- **Gathering the facts:** in order to make sound decisions on existence of vulnerabilities and threat agents, the threat analyst identifies relevant literature through critical assessment of internal and external information sources (Kordy et al., 2011). The information sources are purposively selected based on their accessibility and relevancy.
- **Analyzing information:** this involves appraising the likelihood of threats and their likely impact while considering facts established from the information gathering phase. This action involves the development of "what if" threat scenarios (Shawn et al., 2006).
- **Making decisions on threats:** this is the most visible and most important action for a threat analyst. From the "what if scenarios" the threat analyst decides on the most

probable threats (Saitta et al., 2005; Mockel & Abdallah, 2010). This involves the determination of threat likelihood and potential impact caused by the threats. Furthermore, the decision making action involves making judgments on the cost-effectiveness of threat mitigation controls (Walsh, 2011; Bayne, 2002).

- **Documenting the decision:** as alluded to earlier in section 2.2, the conclusions of the threat analysis process act as inputs in IT investments decision making in organizations like hospitals, particularly on threat mitigation controls. The decisions to acquire a given information system by an organization like a hospital is often based on the likely value the information system adds to the organization and on the perceived level of inherent risk it introduces (Vellani, 2006; Houlding et al, 2012). Also decisions on which threat mitigation controls to invest in, are informed by the perceived cost-effectiveness of the threat mitigation controls. Therefore, to facilitate decision making by organization management, results of the threat analysis process must be presented in a format that makes it easy for decision makers to objectively judge the benefits and risks of a given information system.

From the discussions so far we conclude that threat analysis in information systems involves making three decisions that matter. These are: *how likely is the threat to occur? what would be the impact to the organization should the threat occur? and how cost-effective are the proposed threat mitigation controls?* Therefore, an approach that attempts to enhance threat analysis should provide services of aiding threat analysts to make better decisions that matter. Accordingly, we observe from literature that an ideal threat analysis approach should provide services for guiding threat analysts on how to evaluate threats to an information system. The approach should provide recipes for evaluating threat likelihood, threat impact and estimating the cost-effectiveness of threat mitigation controls. In order to minimize experts' natural bias in decisions that matter and challenges associated with insufficient information, the approach should provide services for enabling collaboration among stakeholders as suggest by Scandariato et al. (2013) and Ruiz et al. (2012).

### **3. Threat Analysis Issues: Practitioners Perspective**

---

*In order to gain a deeper understanding of the threat analysis challenges and requirements for enhancing decisions on threat likelihood, threat impact and cost-effectiveness of threat mitigation controls, an exploratory study among IT security experts was conducted. Accordingly, this chapter discusses the exploratory exercises and its associated results. In section 3.1 the goals of the exploratory study are discussed. Section 3.2 describes how the exploratory study was conducted including selection of respondents and describing the step by step activities of the process. In section 3.3 the results of the study are presented in relation to the study objectives. The chapter concludes with the interpretation of results and definition of requirements for enhancing the threat analysis process through enhancing decisions on: threat likelihood, threat impact and the cost-effectiveness of threat mitigation controls in section 3.4.*

#### **3.1 Study Objectives**

To gain an in-depth understanding of the threat analysis phenomenon from the practitioners' perspective, a case study based inquiry was conducted. Yin (2003) describes a case study as an empirical inquiry that examines a contemporary phenomenon in a real life context. Given the fact that our research is based on abductive reasoning, the exploratory case study approach was chosen to deepen our understanding of: threat analysis processes, decisions that matters, and challenges threat analysts face in making decisions that matter. Furthermore the study aimed at relating observations from literature and practitioners perspectives with a sole purpose of generalizing issues of importance. More importantly, the study aimed at obtaining the practitioners' opinions on how threat analysis challenges can be addressed, resulting into the conceptualization of requirements for an ideal threat analysis approach.

#### **3.2 Study Approach**

##### **Selection of Respondents**

Information system risk analysis is a contextual activity, that is to say challenges of threat analysis in one information system may not necessary be the same for another information system. Consequently, respondents to this exploratory study were selected using a purposive sampling technique. A purposive sampling technique is a non-probability technique of mapping a sample space to a given survey (Weisberg et al., 1989). According to Tongco (2007), a purposive sampling technique, also known as judgment sampling, is the selection of respondents to a study based on their unique qualities that make them likely to provide

the desired opinions and experiences about a given phenomenon under investigation. The experts were purposively selected for the study because of: a) their formal training in information security b) experience in risk analysis c) experience in managing healthcare information management systems. Other factors the researcher considered to select respondents included: peer recommendation, research in information systems security, membership to information security bodies and willingness to participate in the research.

The case study was conducted in two stages. The first stage focused on gaining unbiased understanding of keys issues concerning threat analysis in healthcare information systems and desired characteristics of an ideal approach from the key informants. The second stage involved quantitatively corroborating the thematic issues that emerged from the first stage and generalizing emerging issues of interest. Table 3-1 presents the profile of the respondents who participated in the first stage.

N=5			
Profile	Category	Frequency	Percent (%)
Level of Education	Masters	2	40.0
	PhD	3	60.0
Years of experience	1-5 Years	1	20.0
	6-10 Years	2	40.0
	Above 10 Years	2	40.0
Place of work	Academia	2	40.0
	Industry	1	20.0
	Industry and Academia	2	40.0

*Table 3-1: Profile of the First Group of Experts*

In the first stage, 5 security experts were interviewed using an unstructured interview guide (Appendix 1) to generate thematic issues surrounding the threat analysis phenomenon. Then a survey was conducted among security experts. Out of the 14 experts who were targeted, 10 responded. Given the small number of information security experts in Uganda (Republic of Uganda, 2011), the sample of experts was considered sufficient. The security experts were drawn from the industry and academia with an average field experience of 5 years. The experts were sufficiently exposed to information system risk analysis as evidenced by the consultancy work profile and employment record.

Table 3-2 presents the profile of the respondents who participated on the second stage.

N=10			
Profile	Category	Frequency	Percent (%)
Level of Education	Bachelors	2	20.0
	Masters	6	60.0
	PhD	2	20.0
Years of experience	1-5 Years	5	50.0
	6-10 Years	4	40.0
	Above 10 Years	1	10.0
Place of work	Academia	3	30.0
	Industry	3	30.0
	Industry and Academia	4	40.0

*Table 3-2: Profile of Second Group of Experts*

### **Data Collection and Analysis**

The researcher employed both qualitative and quantitative methods of data collection and analysis. The researcher used the unstructured interview guide (Appendix 1), to collect data in stage one. In the second stage, survey questionnaires which comprised of 3 sections were used (see Appendix 2). The first section captured the respondent's background, the second section focused on getting opinions on thematic issues. Section two was composed of multiple response questions that were arranged randomly and the respondents were to select all statements they thought were relevant to the question. The third section contained an open-ended question intended to capture any information that the respondents thought was not captured in section 2. Questions for the first stage were formulated based on observations from literature, while questions for the second stage were formulated based on issues emerging from the literature and observations from the initial experts.

To ensure that valid and quality data were collected, the data collection tools were tested for content validity. According to Field (2005), validating the content of a research instrument increases the reliability of results and the response rate to the tool. The instrument validity focused on clarity of statements and relevancy to the research objectives. According to Mugenda and Mugenda (1999), validity refers to the extent to which a research tool measures what it is intended to measure. Each tool was reviewed by 3 experts who did not participate in the final exploratory study to assess the validity of the statements. Questions that were poorly phrased or found irrelevant for the study were corrected or deleted during this exercise, resulting into a valid tool.



### ***First Stage of Data Collection***

Semi-structured interviews were first used to gain an understanding of a threat analysis process from 5 key experts, as suggested by Sekaran (2003). The decision to use interviews as a data collection technique stemmed from their advantage of flexibility (Field, 2005). Face-to-face interviews are particularly ideal for exploratory studies as they allow the interviewer to clarify questions and to ensure the responses are understood (Sekaran 2003). It is important to note that face-to-face interviews have a better response rate than other forms of interviews as observed by Weisberg et al (1989). The interviews focused on understanding the threat analysis process in practice, the approaches used to analyze threats in healthcare information systems, challenges analysts face during threat analysis, decisions that matter during threat analysis and the desired requirements of an ideal threat analysis approach. The interviews were conducted between May 2011 and August 2013 and they lasted not more than thirty minutes. The interviews were conducted at the respondents' offices and were manually recorded in the researcher's journal. The face-to-face interviews were supplemented with telephone conversations as means of clarifying findings from the face-to-face interviews. Qualitative data were thematically analyzed using content analysis to identify the emerging issues surrounding the threat analysis phenomenon. The process of analyzing data followed a systematic iterative process involving the following steps: data familiarization, pattern construction, theme searching, themes review, collecting expert's responses along themes and documentation of themes as suggested by Braun and Clarke (2006).

### ***Second Stage of Data Collection***

The survey questionnaire method was used to collect data from 10 experts in order to establish how the thematic issues identified in the first stage could be generalized to a wider group of experts. The survey questionnaire consisting of the key issues that emerged from the open ended interviews and literature, was developed and sent to the experts via Google drive. Quantitative data from the survey questionnaire were analyzed using the Statistical Package for Social Scientists (SPSS) data analysis software. Figure 3-1 shows the online questionnaire that was used to collect the data.

Threat Modelling Approach Requirements ☆

Responses (8) Tools Add-ons Help All changes saved in Drive

View responses View live form

### Part two: Understanding threat analysis process

1. Select one option that best describes a typical threat modelling process?

- ☐ a. Security requirements > asset identification > threat identification > threat mitigation >
- ☐ b. System characterisation > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI
- ☐ c. Security objectives > application overview > application decomposition > threat identification > vulnerability identification
- ☐ Other:

2. For the option selected above in 1, would you like to provide more information to back up your selection

3. What challenges do threat modellers face? Select all that apply

- ☐ a. Lack of information
- ☐ b. Lack of knowledge to analyze threats
- ☐ c. Natural bias of the analyst
- ☐ d. Inability to quantify threat business impact
- ☐ e. Inability to logically estimate threat likelihood

Figure 3-1: Online Questionnaire

Figure 3-2: Shows a sample of expert responses in the Google drive spreadsheet application.

https://docs.google.com/spreadsheets/d/1uAltJ0ptsLVDB2RMQLyKJhCACn65Bv0QE-kY\_gbx2kQ/edit?usp=drive\_web

Getting Started Imported From Fire...

### Threat Modelling Approach Requirements (Responses)

File Edit View Insert Format Data Tools Add-ons Help

A	B	C	D	E	F
Timestamp	1. Highest level of education	2. Professional qualification	3. Years of experience in	4. Place of work:	1. Select one option that best describes a typical threat modelling process? 2. For the option selected above
8/13/2014 17:04:13	master	CCNA		4 Academia	b. System characterisation > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI
8/14/2014 12:42:51	Master	CCNA		3 Industry and Academia	Security objectives > application overview > application decomposition > threat identification > vulnerability identification
8/14/2014 13:05:17	Masters	CCNA, Cyberoam, Micro		5 Industry and Academia	b. System characterisation > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI
8/14/2014 16:39:06	PhD	CCNP	>8	Academia	Security objectives > application overview > application decomposition > threat identification > vulnerability identification
8/15/2014 7:05:50	Bachelors	CCNA		8 Industry and Academia	b. System characterisation > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI
8/15/2014 11:18:39	Masters	CompTIA Linux+		5 Industry	b. System characterisation > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI
8/15/2014 13:12:31	Master	CCNA		4 Academia	a. Security requirements > asset identification > threat identification > threat mitigation >
8/18/2014 10:46:32	Master	CCNA		8 Academia	b. System characterisation > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI

Figure 3-2: Expert Responses

### 3.3 Presentation and Discussion of Results

This section presents and discusses results of the exploratory study among IT security experts. The results are presented along 4 key themes:

1. Typical threat analysis process,
2. Threat analysis challenges,
3. Characteristics of an ideal threat analysis approach and
4. Ideal parameters for evaluation a threat analysis approach.

We will now treat these four key themes in more detail.

#### *Description of a Typical Threat Analysis Process for an Information System by the Respondents*

From the first stage expert interviews (Appendix 1, question 1), the respondents identified 3 generic threat analysis processes as:

1. “Identification of security objectives, assets, threats and threat mitigation”. The process can be categorized as attacker-centric given the fact that the steps that the analyst takes focus more on profiling threat agents and defining plans of mitigating the threats.
2. “System characterization, asset identification, security requirements definition, vulnerability identification, threat identification, threat likelihood evaluation, threat impact analysis, threat mitigation definition and return on investment (ROI) computation”. The process described by the experts can be categorized as a hybrid of attacker-centric and system-centric approaches. The experts’ descriptions indicate that threat analysts focus on both determination of system vulnerabilities and threat agent profiles.
3. “Identification of security objectives, application decomposition, threat identification and vulnerability identification”. This process can be viewed as hybrid of asset-centric and system-centric approach to threat analysis. Experts employing this approach focus more on identification of security requirements for each asset and determination of system vulnerabilities.

The threat analysis processes identified by experts corroborate those identified by earlier literature. According to Pendergrass et al (2013) and Schneier (1999) an ideal threat analysis process should involve understanding of information system features and threat agent profiles, determination of key assets and their security requirements, estimations of threat likelihood and assessment of the strength of security controls. Therefore, the results of this

study show that the experts were knowledgeable about ideal threat analysis procedures and they could therefore be relied on to provide valid responses to the study.

Consequently, the 3 generic threat analysis processes that emerged from the first stage expert interviews were subjected to a quantitative survey in order to establish the most ideal threat analysis process. The finding of the survey are summarized in Table 3-3.

Threat Analysis Process	Frequency	Percent (%)
Identification of security objectives, assets, threats and threat mitigation	1	10.0
System characterization, asset identification, security requirements definition, vulnerability identification, threat identification, threat likelihood evaluation, threat impact analysis, threat mitigation definition and return on investment (ROI) computation	6	60.0
Identification of security objectives, application decomposition, threat identification and vulnerability identification	3	30.0
Total	10	100.0

*Table 3-3: Typical Threat Analysis Process*

The majority of the respondents (6), described a typical threat analysis process as one that begins with system characterization and ends with computation of the Return on Investment (ROI) on the proposed mitigation controls. Processes that begin with definition of security objectives were less favored given the fact that one cannot define a security objective of unknown asset as observed by some experts during the interviews and supported by Shostack (2008).

### *Threat Analysis Challenges*

The researcher was interested in establishing the challenges security experts face in analyzing threats to healthcare information management systems. The results from the first stage expert interviews revealed the key challenges faced by experts during the analysis of threats to a healthcare information management system as:

- “Limited information on threat agents”,
- “Bias by security analysts”,
- “Lack of adequate knowledge on specific threats”,

- “Inability to quantify threat business impact”,
- “Limited formal collaboration among experts”,
- “Inability to logically estimate threat likelihood”,
- “Lack of a logical approach to incorporate background knowledge in the quantification of threat likelihood”,
- “Lack of automated threat analysis tools ”,
- “Limited access to documentation on healthcare information management systems”.

Participants also noted some of the other challenge encountered during the threat analysis process as “poor coordination among stakeholders” during the threat analysis process. One of the key informants observed that “most of the IS Managers in hospitals lack project management skills”, this often results into poor coordination of threat analysis activities in their organizations.

It was observed from the respondents that the key decisions that matter during threat analysis are decisions: on threat likelihood, threat impact and determining the cost-effectiveness of threat mitigation controls. The results of the initial study reveal that threat analysts have challenges of accessing key information to enable them to make decisions that matter. The observations are in line with Walsh (2011) and Bayne (2002) who also noted that lack of adequate information constrains decision making on threat likelihood, threat impact and cost-effectiveness of threat mitigation controls.

In order to find out the greatest challenges that affect security experts in the analysis of threats, the observations by the key informants from the first stage complemented with observations from literature were subjected to a quantitative survey in stage 2. Table 3-4 presents the quantitative findings on the challenges faced by the security experts during threat analysis.

A total of 8 challenges were identified, of which inability to quantify business threat impact, lack of knowledge to analyze threats and lack of information were cited as the key challenges faced by experts during threat analysis. It is interesting to note that lack of collaboration among experts was ranked low. This contradicts Ruiz et al., (2012) who cited lack of collaboration among experts as a major challenge. This could be attributed to the fact that in the Ugandan context, experts collaborate informally due to strong social ties as observed by one of the key informants to the study. The line of reasoning is supported by Shostack (2008), who observed that threat analysis involves a lot of informal interaction among experts. According to Bayne (2002, p2) “it is important that the threat assessment be

a collaborative process, without the involvement of the various organizational levels the assessment can lead to a costly and ineffective security measure”

Challenges	Frequency	Percent (%)
Inability to quantify business threat impact	9	24.3
Lack of knowledge to analyze threats	7	18.9
Lack of information on threat agents and system	6	16.2
Lack of logical approach to incorporate background knowledge in the quantification of threats	5	13.5
Natural bias of the analyst	4	10.8
Inability to logically estimate threat likelihood	4	10.8
Lack of collaboration among experts	2	5.4
<b>Total</b>	<b>37 (Multiple responses)</b>	<b>100.0</b>

*Table 3-4: Challenges Experts Face when Analyzing Threats*

#### *Characteristics of an Ideal Threat Analysis Approach for Healthcare Information Management Systems*

One of the key questions that the researcher set out to address, was to establish the characteristics of an ideal threat analysis approach for a healthcare information management system. To accomplish this, the security experts who participated in the first stage of the study were asked to define the desired characteristics of an ideal threat analysis approach. The following were their responses in no particular order of importance.

- “Provide a sequence of guidelines experts can follow to determine threat likelihood and impact”
- “Provide tools for evaluating threat likelihood based on definition of system characteristics”
- “Offer logical formulas for estimating threat impact, currently experts have to rely on their intuition”
- “Provide guidelines on relevant sources of information experts must examine and what they should look for”

To determine characteristics that are more preferred, the aforementioned responses complemented with observation from literature were subjected to a questionnaire survey among a broader group of security experts and Table 3-5 presents their responses.

Characteristics	Multiple Responses	
	Frequency	Percent (%)
Provides a step by step guideline on how to analyze threats	10	22.7
Provides a technique of computing threat likelihood	9	20.5
Provides a technique of computing threat impact	9	20.5
Provides guidelines on all relevant sources of information	6	13.6
Enables collaboration among IT security experts, business analysts and other actors	5	11.4
Provides recommendations on mitigation control and investment estimates	4	9.1
Enables aggregation of different expert computations and provides an average assessment	1	2.3
<b>Total</b>	<b>44(Multiple responses)</b>	<b>100</b>

*Table 3-5: Characteristics of an Ideal Threat Analysis Approach*

The respondents identified the key characteristics of an ideal threat analysis approach as one that: provides a step by step guide on how to analyze threats, provides a technique of computing threat likelihood, provides a technique of computing threat impact, provides guidelines on all relevant sources of information and enables collaboration among experts and other stakeholders. The observation from the exploratory study are in line with results in literature which indicate that, a good threat analysis approach should provide clear and concise recipes for identifying threats, evaluating threat likelihood, threat impact and determining cost-effectiveness of threat mitigation controls (Shawn et al., 2006; Walsh, 2011; NIST, 2012; Scandariato et al., 2013).

#### *Ideal Parameters for Evaluating a Threat Analysis Approach for HIMIS*

The choice of a threat analysis approach to use is one of the fundamental decisions the threat analyst must make and it has a big impact on the usefulness of threat models generated (Scandariato et al., 2013; Oladimeji et al., 2006). However, without clear guidelines on how to evaluate an approach, choosing an appropriate approach becomes difficult, as observed by Shostack (2008). Thus, the security experts who participated in the first stage of the study were asked to provide the factors that they rely on to evaluate the appropriateness of a threat analysis approach. Their responses include:

1. “ Clarity of guidelines and procedures ”
2. “ Clarity of concepts and terminologies ”
3. “ Convenience of use ”
4. “ Easy to learn”
5. “ Effectiveness in determining threat likelihood ”
6. “ Effectiveness in evaluation the impact of the threat ”
7. “Ability to cater of emerging threats”
8. “Reliability of conclusions”.

The expert responses can be categorized into 2 core parameters. The first 4 responses are about usability and the last four response are about usefulness. In order to establish the most important parameters that the experts consider relevant for evaluating a threat analysis approach, the results of first stage study were subjected to a survey. Table 3-6 presents the summary of the findings.

Parameters	Multiple Responses	
	Frequency	Percent (%)
Usefulness in determination of likely threats and their impact	10	43.5
Consistency of the generated assessment results	6	26.1
Based on ease of use	3	13.0
Based on learnability	3	13.0
Ability to cater for new and developing threats	1	4.3
<b>Total</b>	<b>23 (Multiple responses)</b>	<b>100</b>

*Table 3-6: Parameters for Threat Analysis Approach Evaluation*

The respondents identified: usefulness in determination of likely threat and impact, consistency of generated assessment results, ease of use and learnability as the key parameters for evaluating a threat analysis approach. These results are in line with observations made by Shostack (2008) and Scandariato et al. (2013) during the study of the STRIDE approach where it was established that the most important parameters for evaluating an approach are: usefulness, usability and completeness (completeness refers to the comprehensiveness of the activities and guidelines of an approach). In section 3.4, the requirements for an ideal threat analysis approach are discussed.



### 3.4 Requirements for an Ideal Threat Analysis Approach

The understanding and exploratory stages of this research resulted in the conceptualization of the threat analysis process as judgment process that begins with the understanding of the system features and ends with assessing the return on investment on threat mitigation controls. From the discussions so far it has been established that one key challenge that threat analysts face is to make utility maximizing decisions on: the likelihood of threats, threat impact and cost-effectiveness of threat mitigation controls (Walsh, 2011; Canon, 2011; Houlding et al, 2012). The difficulties in making decisions that matter is attributed to a number of factors, namely: lack of clear guidelines on information sources, poor information visualization, and lack of logical techniques of estimating threat likelihood and impact (Kordy et al., 2011; Ongtang et al., 2012).

The synthesis of literature indicate that information system managers in hospitals consider risks that information systems may expose the hospital too, when using an information system. Therefore, establishing the risk level can be achieved through the visualization of a risk impact in terms of business value (Walsh, 2011; Scandariato et al., 2013). Business value is a parameter that measures the degree at which the business has met the set goals. Business goals can be categorized in terms of process efficiencies or effectiveness of services produced. Therefore, enhancing the threat analysis process can be achieved through improving the efficiency of the process, or effectiveness of the services produced. Improving process efficiency and effectiveness heavily depends on making quality decisions on threat likelihood, threat impact and the effectiveness of threat mitigation controls (Shostack, 2008; Mockel & Abdallah, 2010; Walsh, 2011; Scandariato et al., 2013).

Basing on literature and results of the exploratory study, it was established that a threat analysis approach for information systems especially healthcare information systems must meet the following requirements if it is to address challenges faced by threat analysts.

- ***Provide step by step guidelines on how to analyze threats.*** The provision of systematic guidelines reduces the dependence on expert tacit knowledge in the assessment of threats resulting into rational decision making on threat likelihood, threat impact and cost-effectiveness of threat mitigation controls (Shawn et al., 2006; Walsh, 2011). The guidelines should provide relevant sources of information the analysts must examine and what they should look for.
- ***Provide recipes of computing threat likelihood.*** Logically ascertaining the likelihood of threats reduces chances of underestimating threats, hence resulting

into better decisions on threat mitigation controls (Sjouke & Oostdijk, 2006; Kordy et al., 2011).

- ***Provide a technique of computing threat impact.*** In order to justify investments in threat mitigation strategies, there is need to monetize the impact of a threat to the hospital.
- ***Provide guidelines on information sources.*** The credibility of the threat analysts' opinion on threat likelihood and impact depends on the type of information available. Thus the provision of guidelines on selecting reliable information sources improves that quality of information available to the threat analyst.
- ***Enable collaboration among IT security experts, business analysts and other actors.*** It has already been articulated that one of the key challenges of threat analysis is access to information to facilitate decision making. Thus, collaborating with other stakeholders increases chances of accessing critical information on threat agents and system vulnerabilities, which in turn enhances decision making on the likelihood of threats and their impact (Bayne, 2002; Vellani, 2006; Houlding et al, 2012; Ruiz et al., 2012).
- ***Provide recipes for determining cost-effective threat mitigation controls.*** Literature indicates that decision makers on IT investments in organizations particularly on information system security are guided by the cost-effectiveness of the controls. Therefore, a threat analysis approach that provides a logical assessment of cost-effectiveness of the controls is highly desired as also suggested by Vellani (2006) and Houlding et al. (2012).

Therefore in chapter 4, we present the Threat Nets Approach aimed at providing the aforementioned requirements.



## 4. The Threat Nets Approach

---

*In this chapter the Threat Nets Approach to address threat analysis challenges is discussed. The chapter first gives a general overview of the approach in section 4.1. Section 4.2 presents a typical threat analysis scenario highlighting the complexities threat analysts have to contend with when making decisions on threat likelihood and impact on a healthcare information system. The Threat Nets Approach is described following Sol's "ways of" framework (section 4.3), in terms of: the way of thinking (section 4.4), way of governance (section 4.5), way of modeling (section 4.6) and way of working (section 4.7). The approach prescribes guidelines and techniques of quantifying threat likelihood, impact and return on investment in threat mitigation controls. The approach is grounded in the service system and decision enhancement theories (section 4.4).*

### 4.1 General Overview of the Threat Nets Approach

The threat analysis process on an information system involves a number of actors including organization top management who are responsible for making decisions on IT investments. Others include: information system managers – responsible for coordinating the threat analysis process, security experts – responsible for conducting threat assessment and the business analysts - responsible for assessing threat business impact. Figure 4-1 presents a general overview of the Threat Nets Approach illustrating the interaction among actors during the process (a work flow diagram). The rows in Figure 4-1 represent actors, while the column represent stages of the process. A threat analysis process begins with a decision by top management of an organization represented by the Chief Executive Officer (CEO) authorizing the project manager to conduct threat analysis on an information system. During the coordination stage the project manager prepares terms of reference for security experts, identifies threat analysts to be engaged for the assignment and negotiate a contract. Thereafter, he provides all the necessary logistics to the analysts to facilitate them execute their task. To determine the cost-effectiveness of threat mitigation controls, the project manager has to receive reports from both the security expert and business analyst. The arrows in Figure 4-1 illustrate the progress from one activity to another. The black dot indicates the start of the process and the empty circle the end of the process. Rectangles with plus signs indicate compounded activities actors have to execute.

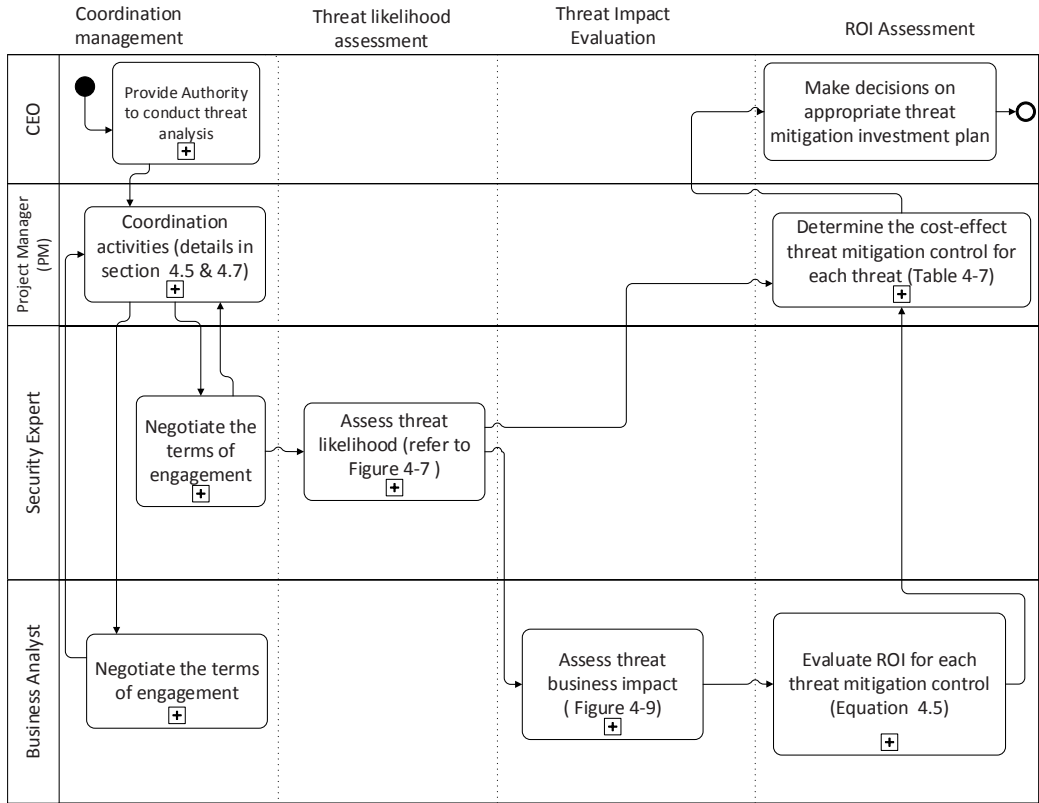


Figure 4-1: General Overview of the Threat Nets Approach (work flow diagram)

## 4.2 Threat Analysis Scenario

In order to demonstrate the interactions among actors and complexities encountered during a typical threat analysis process, this section presents a typical threat analysis scenario.

Case Hospital Kampala (CHK) serves over 420 patients per day. The hospital employs 10 doctors, 30 nurses, 8 lab technicians, 4 accounts and 4 pharmacists on fulltime basis. The hospital runs ClinicMaster an integral part of RPMS to automate patient services. ClinicMaster automates patient medical records, accounting, billing, insurance, admissions, drug inventory, laboratory, surgery, prescriptions, and service access (Kutegeka, 2014). Given the fact that ClinicMaster is central to the operation of Case Hospital Kampala, top hospital management through the Chief Executive Officer (CEO) commissions a threat analysis project to assess the nature, source and likelihood of threats to ClinicMaster. Furthermore, the top management would like to understand the potential business impact of threats on the operations of the hospital. On the other hand, the IS manager is interested in

understanding the type of mitigation controls, their effectiveness, and the Return on Investment (ROI). Thus, the IS Manager of Case Hospital Kampala who doubles as the Project Manager assembles a team of experts to undertake the threat analysis task.

The Project Manager prepares a project document that defines project objectives, scope and schedule. Furthermore, he assembles all relevant documents about ClinicMaster system including: user profiles, system design, operational architecture, previous security audit reports, information technology policies, and hardware inventory. Thereafter, the Project Manager shares the project document with security experts and business analysts during the project briefing.

In order to determine ClinicMaster's vulnerabilities, the security experts have to examine the completeness of each individual component of the ClinicMaster system i.e. governance (policies and standards), software (including hardware and network) and human resources (users and IT support team). Furthermore, the security experts have to review a number of documents both internal and external to determine system vulnerabilities and profiles of threat agents. Security experts evaluate threat likelihood based on: the history of vulnerability exploitation in related information systems, number of related security breaches in the public domain, ClinicMaster characteristics and potential attacker profiles. Thereafter, they propose appropriate threat mitigation controls.

Using security experts' reports (threat descriptions, their likelihoods and proposed mitigation controls), the business analysts assess the threat business impact based on brand damage, lost productivity, costs of recovery among others. Furthermore business analysts estimates the mitigation control costs for each threat. The reports of security experts and business analysts are then submitted to the Project Manager, who summarizes the reports before submitting these to the hospital top management. The hospital top management relies on the reports from the IS manager to make decisions on investments in threat mitigation strategies. Clearly, completing such a task requires good understanding of ClinicMaster design and operation, extensive scanning of literature in the public domain, sound techniques of computing threat likelihood, threat impact and return on investment on the proposed mitigation strategies.

### **4.3 The “Ways of” Framework**

A number of researchers (De Vreede & Briggs, 2005; Habinka, 2012; Knol, 2013) have successfully used Sol's “ways of” framework to describe approaches to address problems in various fields. The “ways of” framework provides an elegant style of articulating the Threat

Nets Approach in terms of: the way of thinking, the way of governance, the way of modeling and the way of working. Figure 4-2 presents the framework.

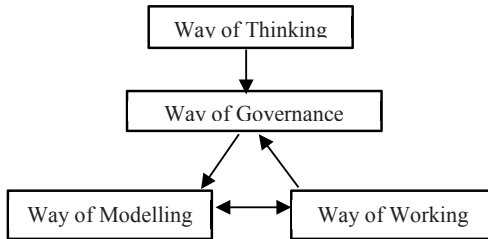


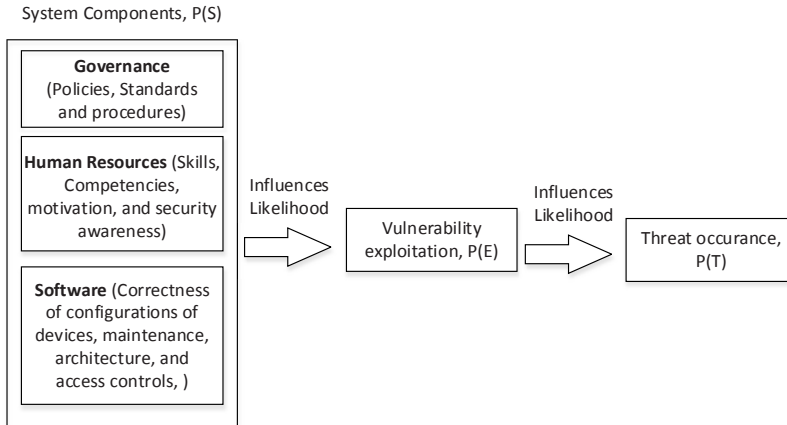
Figure 4-2: Sol's "Ways of" Framework (Sol, 1988)

#### 4.4 Way of Thinking

The way of thinking expresses the underlying philosophy upon which the Threat Nets Approach is built. From the discussion so far, it has been demonstrated that decisions on threat likelihood, threat impact and investments in threat mitigation depend on availability of information on the system vulnerabilities, threat agents, skills and knowledge of security experts (Shostack, 2008). On the other hand, the IS managers make decisions on threat mitigation strategies based on total investments costs in the strategy and its perceived effectiveness (Baynes, 2002). According to Stallings (2003), threat likelihood  $P(T)$  is directly proportional to the likelihood of vulnerability exploitation,  $P(E)$ . Logically the completeness of an information management system component (*governance, human resources and software*),  $P(s)$ , is inversely proportional to the likelihood of vulnerability exploitation,  $P(E)$ . That is to say, a system component ( $S$ ), with comprehensive security features leads to fewer vulnerabilities (Ruiz et al., 2012).

Figure 4-3 shows the interdependence between system characteristics, vulnerabilities and threats. Since a threat exploits a given vulnerability to breach a security service of a given asset, a threat can be described in terms of affected assets, vulnerabilities that can be exploited and security requirements breached. As illustrated in Figure 4-3, the weakness in the information system components (governance, human resources and software) influences the likelihood of vulnerability exploitation,  $P(E)$  which in turn influences the likelihood of threat occurrence,  $P(T)$ .

From the discussions so far, it is clear that a threat analysis process involves a number of actors with different skills, mainly security experts, business analysts, and IS managers/project managers.



*Figure 4-3: Relationship between System Characteristics and Vulnerabilities*

We observe that threat analysis is a multi-stage sequential process with actions and decisions of actors at one stage influencing the decisions of the next stage. Thus, the threat analysis process can be regarded as a service system in which actors (people) are specifically arranged to take actions which provide value to others. According to Alter (2012), there is little agreement among researchers about the definition of service. Alter (2012) describes services as “processes, performances, or experiences that one person or organization does for the benefit of another”. On the other hand, Vargo and Lusch (2004, p2) define a service as “the application of specialized competences (knowledge and skills) through deeds, processes and performances for the benefit of another entity or the entity itself”. Therefore, this study uses Alter’s (2012) definition of service and proposes the threat nets theory which suggests that the assessment of threats to information systems like RPMS should be based on three sequential aspects:

- Threat likelihood – the quantification of threat likelihood based on characteristics of system components and threat agents.
- Threat impact – what is the impact of a threat on business output?
- Return on Investment – what is the most cost-effective threat mitigation strategy?

Our threat nets theory suggests that assessing threats to information systems should follow a multi-stage process, with the ultimate goal of making decisions on threat mitigation controls. But the determination of cost-effective threat mitigation controls should be based on enhanced understanding of threats in terms of their likelihood and impact to an organization running the information system. Walsh (2011) recommends 6 parameters upon which organizations should use to evaluate a threat impact: 3 technical parameters



(integrity, confidentiality, availability) and 3 business parameters (financial impact, reputation and litigation). Thus, the threat nets theory departs from traditional threat analysis approaches that focus on threat identification and quantification of impact in technical terms only (integrity, confidentiality, availability of patient data). The paradigm shift is grounded in the understanding that the technical impact is inherently captured in the business impact through assessment of lost productivity and reputation (brand) damage. Therefore, the threat nets approach offers three decision enhancement services in the form of guidelines and techniques. These are:

1. Threat likelihood assessment service,
2. Threat impact evaluation service and
3. ROI assessment service.

We will now explain these 3 decision enhancement services in more detail.

### **Threat Likelihood Assessment Service**

According to Shawn et al. (2006), analyzing characteristics of individual components of an information system for vulnerabilities increases chances of discovering complex vulnerabilities in the information system. Therefore, providing clear guidelines and techniques of incorporating influences of vulnerability likelihoods (discovery and exploitation) on threat likelihood reduces the dependency on individual skills and knowledge, resulting into realistic assessment of threat likelihood to an information system (Fay, 2007; Mirembe & Muyebe, 2008; Shostack, 2008). Accordingly, Threat Nets Approach uses probability theory (Feller, 2008) and Attack trees (Schneier, 1999) to evaluate the likelihood of a given threat, resulting into the construction of a threat tree. A threat tree is a directed graph  $G$ ,  $G = (N, L)$  with  $N$  nodes and  $L$  edges. Unlike in attack trees, the nodes of a threat tree are objects with local information about the node and a method of computing the node likelihood. More formally;

#### **Definition 4.1**

A threat tree  $T$ , is a 3-tuple  $(N, \rightarrow, n_0)$ , where  $N$  is a finite set of nodes,  $\rightarrow$  is a finite set of links between pairs of nodes and a root node,  $n_0$ . Children of a node in a threat tree are refinements of the node, and leafs therefore represent actions that can no longer be refined. Since the goal of the threat tree is to determine the most likely passage the threat agents can exploit, only disjunctive refinement is supported.

**Definition 4.2**

A node,  $n_i$  in a threat tree  $T$ , is an object with attributes (Node name, Vulnerability Discovery, Threat agent profile, Child nodes influences, Parent node, Node weight, and Next child). The node has one method that computes the node likelihood.

The threat agent's profile (likelihood of vulnerability exploitation), likelihood of system vulnerabilities and influences of child nodes are represented as 3-tuple stochastic variables of a node. The likelihood of a threat  $T$  is then computed recursively over the root node  $n_0$  using Algorithm 1 described in the way of working (section 4.7).

**Threat Impact Evaluation Service**

Threat impact is assessed in terms of lost business value and costs of recovery. To evaluate threat impact, the Threat Net Approach utilizes value theory (Deberu, 1972) and the Interbrand approach (Keller, 2003). The value theory provides the understanding of what is valuable, why and to what degree people value things. The threat impact is computed using equation 4.4 under the way of working. In this case the value theory provides an understanding of how to assess lost business value. The Interbrand approach provides a framework of evaluating a brand value based on a number of factors including sales projections, market share, and brand stability.

**Return on Investment Assessment Service**

Information system managers and top management in organizations, use the Return on Investment (ROI) perspective to make decisions on the efficiency of investments in threat mitigation controls, that is to say make a decision among a number of mitigation control investment options. ROI measures the estimated benefits an organization like Case Hospital in our running example will get by investing in a given IT infrastructure. A high ROI means that the investment gains compare favorably to investment costs (Keen, 2011). ROI is unit less and is measured as a ratio of the difference between threat business impact and total investment costs over total investment for a given threat mitigation control as illustrated by equation 4.5 in section 4.7.

**4.5 Way of Governance**

One of the challenges cited by security experts during the exploratory study was poor process coordination by project managers (PM). The poor process coordination is in part due to poor project planning. Project planning is a process of establishing the project

objective, definition of service level agreements, assembling of resources, and establishment of reporting guidelines and monitoring the implementation of activities (Lewis, 2005). Furthermore, threat analysis is a complex process involving the interaction between people and processes which requires process management actions. Process management focuses on the coordination of activities among actors: security experts, business analysts, IS managers and organization top management. Thus, the way of governance articulates the managerial aspects of the Threat Nets Approach and it involves the definition of guidelines on how to initiate the threat analysis process and coordinate activities among actors during the process. The guidelines define tasks to be performed when planning threat analysis activities, assessing threat likelihood, evaluating threat impact and assessing ROI on threat mitigation controls. Table 4-1 presents the proposed guidelines to facilitate process initiation and coordination among actors.

Task	Guidelines	Actor
Process initiation	<ol style="list-style-type: none"> <li>1.1 The project manager must obtain all necessary approvals from management to undertake the threat analysis task</li> <li>1.2 Prepare a project document that, defines project objectives, scope, schedule, communication guidelines, and desired outcomes</li> <li>1.3 Establish the number of affected users and their profile.</li> <li>1.4 Prepare all relevant documents about the system under audit including: user manuals, technical manuals, system design documents, operational architecture, policies, network architecture, resource inventory, business continuity plans, disaster recovery strategies, and human resource profiles of system administrators</li> <li>1.5 Identify and engage consultants (security and business analysts) who are to undertake the project following organizational prescribed service procurement guidelines like the Public Procurement and Disposal Act (PPDA)</li> <li>1.6 Prepare a Service Level Agreement (SLA) between the experts/analysts and the client organization. The SLA should clearly define the desired quality of results, ethical considerations, schedules, scope, expert compensation plan, and management of disputes.</li> <li>1.7 Define a communication plan to facilitate communication and coordination among stakeholders. The guidelines should clearly state the nature of information to be communicated by individuals, channels to be used, expected response time among others. At bear minimal level, the following communication lines must be defined; Expert to PM, PM to Users, Experts to Users, and PM to CEO</li> <li>1.8 Define resource access guidelines for experts/analysts who are going to undertake the security audit</li> <li>1.9 Communicate to stakeholders about the project activities</li> <li>1.9.1Conduct a project briefing session for all stakeholders including; users, experts and management. During the briefing clarify issues like objectives and scope</li> </ol>	Project manager

	1.9.2 Handover all relevant documents to experts before the start of the threat modelling activities	
	2.1 Assess project objectives and scope to ascertain their feasibility 2.2 Seek clarification from the project manager if any 2.3 Determine the required documents and logistics to accomplish the task 2.4 Obtain relevant documents about the system. For example previous audit reports, policies, user profiles, system configurations, technical manual, network architecture, and procedures 2.5 Review, update and sign up on the Service Level Agreement 2.6 Create your preferred working schedule Notify the project manager about the schedule	Security expert
	3.1 Seek clarification from the project manager if any 3.2 Ensure that all relevant information is provided for the task 3.3 Draft and submit a working schedule to the project manager 3.4 Review, update and sign up on the Service Level Agreement 3.5 Create a working schedule	Business Analyst
Coordination	4.1 The project manager must enforce the SLA 4.2 Monitor the progress of activities against set outputs	Project Manager

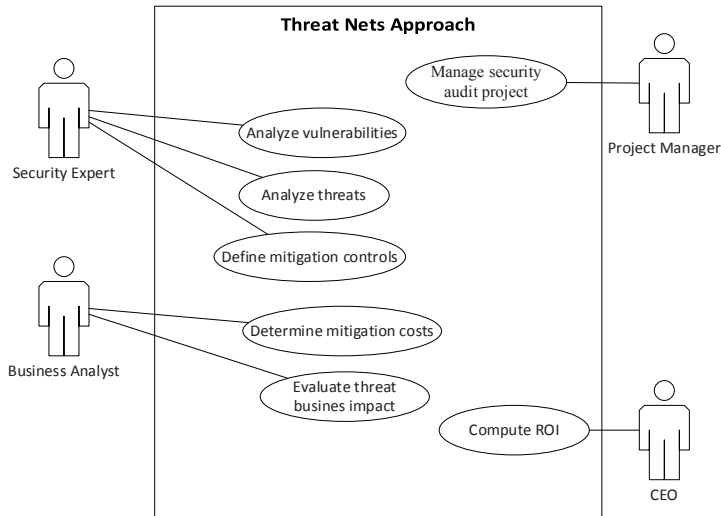
*Table 4-1: Guidelines to Facilitate Coordination during Threat Analysis*

## 4.6 Way of Modelling

The way of modelling describes concepts that are suitable for modelling relevant aspects of the Threat Nets Approach. Various concepts including use case diagrams, activity flow diagrams, sequence diagrams and component diagram are used to model the Threat Nets Approach. The models were constructed using the Unified Modelling Language (UML), a general-purpose modelling language (Rumbaugh et al., 2005). UML was selected because of its agility and extensive usage in various modeling tasks, making the artifacts easily understood by all actors. Attack trees are used to model threat propagation during threat likelihood analysis. A threat to an information management system is modeled in terms of asset, security requirement and vulnerability as introduced in the way of thinking (section 4.4). In the proceeding subsections we describe the modeling concepts used to model the approach.

### Use Case Modelling

In order to visualize the interaction between actors applying the Threat Nets Approach on an information systems, a use case diagram was used. A use case is a list of steps, typically defining interactions among actors to achieve a given goal (Rumbaugh et al., 2005). The actors include; project manager, security experts, business analysts and top managers who make investment decisions (Figure 4-4).



*Figure 4-4: Threat Nets Approach Use-Case Diagram*

The project manager is a person who initiates the threat analysis process by inviting security experts and business analysts to undertake a threat analysis exercise on a given information system. The security experts use the Threat Nets Approach to determine vulnerabilities, threats and define threat mitigation controls. The approach facilitates the security experts to compute threat likelihood using the threat likelihood assessment service introduced under the way of thinking in section 4.4. The business analysts use results of the security experts to estimate the business brand damage, lost productivity and evaluate the threat impact using the threat impact evaluation service. Using the threat impact measurements and costs of mitigations, the hospital top management computes the return on investment for the different mitigation controls so as to make a decision on suitable options.

## Activity Flow Diagrams

Threat analysis involves a series of activities as alluded to in earlier chapters. Therefore, activity diagrams are used to illustration activities within a given task. The compound tasks are: project planning, vulnerability analysis, threat analysis and threat quantification (Fay, 2007). The activity diagrams were constructed using the Unified Modelling Language (UML) (Rumbaugh et al., 2005). These are discussed in section 4.7 under the way of working.

### Sequence Diagram

Since threat analysis involves cooperation among actors, sequence diagrams were used to provide a graphical representation of interactions between communicating entities over time Figure 4-5. The sequence diagram typically shows the actor interaction during the execution of a given task. According to Rumbaugh et al. (2005), sequence diagrams are an outstanding technique of documenting usage scenarios, thus ideal for the representation of interaction among actors during threat analysis.

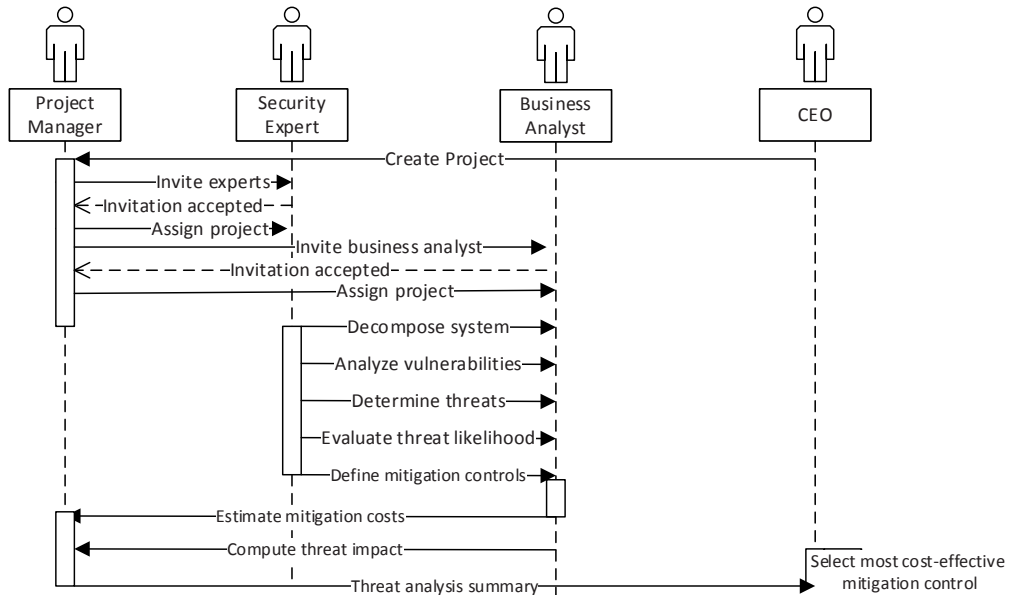


Figure 4-5: Threat Nets Approach Sequence Diagram

### Attack Trees

The phrase attack tree was coined by Schneier (1999) and it describes *the why and how the security of an information system can be compromised*. Attack trees provide simple semantics to allow refinements of threats into sub-goals the attacker must accomplish in order to breach the security of a given asset. Thus, Threat Nets Approach uses attack trees to illustrate the different pathways a threat can propagate. The attack tree were enhanced by incorporating scenario specific details like existence of system vulnerabilities and threat agent profiles.

## 4.7 Way of Working

The way of working represents activities that need to be undertaken when using the Threat Nets Approach to assess threat likelihood, threat impact and ROI of threat mitigation controls. Subsequent to the requirements discussed in chapter 2 and the way of thinking described in section 3.4, the Threat Nets Approach consists of 4 main activities which are; (1) threat likelihood assessment, (2) threat impact evaluation, (3) ROI assessment for mitigation controls, and (4) coordination management. While the first 3 activities are sequential to each other, coordination management is done throughout the threat analysis process as illustrated in Figure 4-6.



*Figure 4-6: Threat Nets Approach Activities*

The details of the 3 activities are discussed in the following sections.

### **Step 1: Threat Likelihood Assessment Service**

The threat likelihood assessment involves mainly 3 activities; information system vulnerability analysis, threat agent analysis and threat likelihood computation.

#### ***Information system vulnerability analysis***

The threat likelihood assessment service provides the security expert with guidelines on how to ascertain vulnerabilities in an information system. In addition, the threat likelihood assessment service provides a procedure of quantifying likelihood of information system vulnerability discovery based on the assessment of system components. Furthermore, it provides techniques of evaluating the likelihood of vulnerability exploitation based on the

assessment of the threat agent (s) profile. Vulnerability discovery refers to how easily a threat agent can discover a vulnerability in a given system component, while vulnerability exploitation refers to the ease of vulnerability exploitation by a threat agent.

Vulnerability analysis involves an extensive review of an information system architecture to ascertain design and configuration flaws (vulnerabilities). The vulnerability analysis involves the collection and comprehension of data from both the internal and external environments. The output of the vulnerability analysis is a descriptive list of vulnerabilities with their corresponding likelihoods of discovery.

To estimate the likelihood of vulnerability discovery, each component of an information system component (governance, human resources and software) is analyzed for design and operational flaws. The analysis is by way of assessing the completeness of elements in each component on a scale of 0.0 to 1.0 by the security expert. We adopt the scale of 0.0 to 1.0 since the assessment of elements follows a stochastic variable which represents the chances of finding weakness in the elements of a given system component. The completeness score (CS) measures the experts' judgment about the absence of design and implementation flaws in an element. Where 1.0 means "I am sure that there is no flaw" and 0.0 means "I am sure that there is a flaw". The component score S, which measures the completeness of an information system component is computed as the average of completeness scores (CS) of all elements in a given component. This is because components are assessed independent of each other. Since S is in the range of 0.0 to 1.0 it is interpreted as likelihood of vulnerability non-discovery  $P(S)$ . For that reason, the  $P(\text{not } S)=1-P(S)$  is considered as the likelihood of vulnerability discovery,  $P(D)$ . Considering the scenario introduced in section 4.2, Table 4-2 below illustrates a typical expert assessment of the governance component to determine the likelihood of vulnerability discovery,  $P(D)$  in the component.

Element	Completeness Score (CS)
Access control policy	0.90
Business continuity and disaster recovery	0.50
Telecommuting policy	0.00
E-mail policy	0.50
Use of third party applications policy	0.30
<b>Total CS</b>	<b>2.20</b>
<b><math>P(S)</math> [ Total CS/Number of elements]</b>	<b>0.44</b>
<b><math>P(D)= 1-P(S)</math></b>	<b>0.56</b>

*Table 4-2: Illustration of Vulnerability Assessment of the Governance Component*



### ***Threat agent analysis***

According to ISACA (2013), threat likelihood depends on the likelihood of vulnerability exploitation. That is to say, the likelihood,  $P(T)$  of a threat  $T$ , is directly proportional to the likelihood of vulnerability exploitation,  $P(E)$ . But the likelihood of vulnerability exploitation,  $P(E)$ , is dependent on the likelihood of vulnerability discovery,  $P(D)$ . Therefore, after evaluating the likelihood of vulnerability discovery, the security expert assesses the likelihood of vulnerability exploitation by threat agents. According to Houlding et al., (2012), likelihood of vulnerability exploitation depends on the threat agent profile, which include; threat agent motivation, threat agent tools and threat agent knowledge about an information system. Therefore, security experts employing the Threat Nets Approach have to assess the strength of each of element of the threat agent profile that make it likely for the agent to exploit system vulnerabilities. The elements are assessed also on a scale of 0.0 to 1.0.

Let  $x = \{P(M), P(T), P(K)\}$  be a 3- tuple of element scores for; motivation, threat agent tools and skills respectively for a given threat. Then, the likelihood of vulnerability exploitation by a threat agent,  $P(E)$  given profile  $x$  is computed as;

$$P(E) = P(M) + P(T) + P(K) - P(M)P(T) - P(M)P(K) - P(T)P(K) + P(M)P(T)P(K) \quad (4.1)$$

As illustrated in equation 4.1, the stochastic variable  $E$  depends on other stochastic variables  $M$ ,  $T$  and  $K$ .  $P(K)$  represents assessment of a threat agent skills on the scale of 0.0 to 1.0. Thus, let  $Y = \{P(D)_1, P(D)_2, P(D)_3\}$  be a 3-tuple for likelihoods of vulnerability discovery in the three components of; governance, human resource and software respectively. Then, the likelihood of vulnerability discovery in the entire information system,  $P(D)$  is computed as;

$$P(D) = P(D)_1 + P(D)_2 + P(D)_3 - P(D)_1P(D)_2 - P(D)_1P(D)_3 - P(D)_2P(D)_3 + P(D)_1P(D)_2P(D)_3 \quad (4.2)$$

Where  $P(D)_i$  measures the expert's opinion about the likelihood of flaws within a given system component for example governance.

*For example assume,  $P(D)_1, P(D)_2, P(D)_3$  of ClinicMaster components of; governance, human resource and software at Case Hospital are 0.56, 0.40 and 0.15 respectively. Therefore, the likelihood of vulnerability discovery in ClinicMaster system at Case Hospital  $P(D)$  is computed using equation 4.1.*

$$P(D) = (0.56 + 0.4 + 0.15 - 0.56 * 0.4 - 0.56 * 0.15 - 0.4 * 0.15 + 0.56 * 0.4 * 0.15) = 0.7756$$

*P(D) is always higher than the highest flaw likelihood due to the cumulative effect of individual flaws on the likelihood of vulnerability discovery. A P(D) value above 0.5 indicates that the threat is most likely and the likelihood increases as P(D) approaches the value of 1.*

To determine P(E), the security expert must provide an assessment of P(M) and P(T) based on the Intel's healthcare information management threat agents assessment framework (Houlding et al., 2012). Then P(E) is computed using equation 4.1.

*For example, assume a group of radical hackers targeting to steal patient medical records from the healthcare information system described in section 3.2, such a threat agent has a very high motivation, so we take P(M) of 0.9 and has capacity to assemble sophisticated tools to achieve their goals, so P(T) of 0.8. Using P(D) of 0.7084, we compute the likelihood of vulnerability exploitation using equation 4.2 as.*

$$P(E) = 0.9 + 0.8 + 0.7756 - 0.9 * 0.8 - 0.9 * 0.7756 - 0.8 * 0.7756 + 0.9 * 0.8 * 0.7756$$

$$P(E) = 2.4756 - 0.72 - 0.6980 - 0.6205 + 0.5584$$

$$\mathbf{P(E) = 0.9955}$$

Figure 4-7 illustrates the threat likelihood assessment activities.

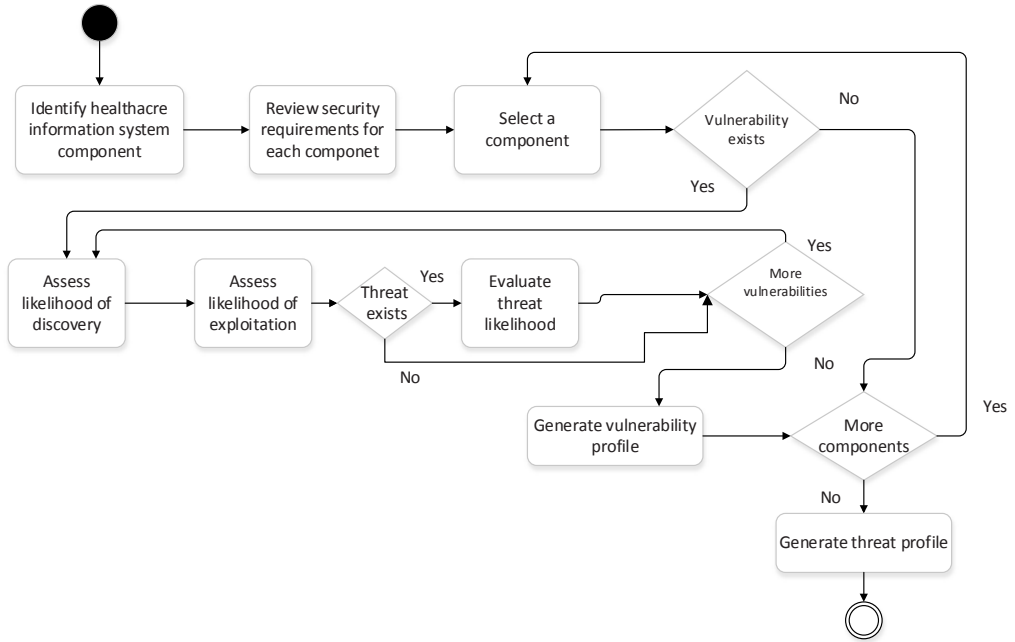


Figure 4-7: Threat Likelihood Assessment Service Activity Diagram

To accomplish the threat likelihood assessment activities illustrated in Figure 4-7, the following guidelines are proposed as described in Table 4-3.

Activity	Guideline	Actor
Step 1: Review security requirements	1.1 For each system component establish the desired security requirements. 1.2 Review relevant literature like standards, journals, security blogs, and conference papers to establish the ideal security requirements 1.3 Establish security requirements upon which the threat analysis will be based	Security expert
Step 2: Asses likelihood of vulnerability discovery	2.1 Asses the completeness of the governance framework 2.1.1 Determine if the organization has defined all the 11 information security policies recommended by the ISO 270002 standard (ISO27002, 2015) 2.1.2 Asses the completeness of each policy on the scale of 1 to 5, with 5 being the highest 2.2 Classify assets based on the degree of importance (critical, normal and basic) 2.3 Assess human resource competencies 2.3.1 Interview users to assess the degree of security awareness 2.3.2 Establish the regularity of security awareness training	Security expert

	<p>2.3.3 Establish the level of user adherence to policies</p> <p>2.3.4 Assess the competencies of users on the system</p> <p>2.3.5 Assess the competencies of IT administrators</p> <p>2.3.6 Assess the regularity of IT administrators' capacity development training</p> <p>2.4 Assess completeness of network and software controls</p> <p>2.4.1 Analyze the completeness of technical controls through interviewing system administrators, network penetration testing and system configuration reviews.</p> <p>2.4.2 Assess the completeness of technical controls, through system stress testing and network penetration</p> <p>2.4.3 Analyze user behavior and attitudes to determine motivation for compliance to policies</p> <p>2.4.4 Assess the users degree of security awareness through social engineering</p> <p>2.4.5 Conduct ethical hacking on system components</p> <p>2.4.6 Assess the enterprise architectures to determine exposure to natural disasters</p> <p>2.4.7 Assess the regularity of software updates</p> <p>2.4.8 Assess the reliability of software technical support</p> <p>2.4.9 Conduct a network scan to establish open ports</p> <p>2.5 Map out all unauthorized system input and output points</p> <p>2.6 Identify all probable vulnerabilities</p> <p>2.7 Classify vulnerabilities based on security services (Confidentiality, Integrity, Authentication, Availability, Non-Repudiation )</p> <p>2.8 Compute the likelihood of vulnerability discovery based on the completeness of scores of the system components</p>	
<p>Step 3: Asses likelihood of vulnerability exploitation (Threat agents analysis)</p>	<p>3.1 Scan the environment to ascertain emerging threats. Sources of information include; academic journals, conferences, books, CERT reports, News bulletins, social media, and IT security blogs</p> <p>3.2 Establish the profile of the threat agent factors in the environment. Threat agents' factors are events that influence the likelihood of threats and their impact. Use the OWASP framework to assess (OWASP-RRM, 2014)</p> <p>3.2.1 Estimate the skill levels. That is, how technically skilled is this group of threat agents? Use OWAP Security penetration skills (9), network and programming skills (6), advanced computer user (4), some technical skills (3), no technical skills (1)</p> <p>3.2.2 Determine the motivation. That is, how motivated is this group of threat agents to find and exploit a given vulnerability? Low or no reward (1), possible reward (4), high reward (9)</p> <p>3.2.3 Assess the opportunity, that is what resources and opportunities are required for this group of threat agents to find and exploit a given vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)</p>	Security expert

	<p>3.2.4 Estimate the size of the threat agents. That is how large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)</p> <p>3.3 Consult researchers and practitioners about existence of known threats and their level of prevalence</p> <p>3.4 Identify all possible threat goals (threats</p>	
Step 4: Threat likelihood evaluation	<p>4.1 Construct a threat tree (Figure 3-8)</p> <p>4.2 Incorporate background knowledge in the threat tree</p> <p>4.3 Evaluate threat likelihood using Algorithm 3-1</p>	Security expert

*Table 4-3: Threat Likelihood Assessment Guidelines*

### ***Threat Likelihood Assessment Service***

Once vulnerabilities have been identified, the security experts review the internal and external information system environment to establish the existence of threats. Consequently, the security expert defines a threat (goal) and refine each threat into sub-goals (Figure 4-8), resulting into the construction of a threat tree (Mirembe & Muyeba, 2008). The threat tree uses the structure of an attack tree to illustrate the different pathways a threat agent can follow to compromise a given information system (achieve the set goal). For each threat, the security expert incorporates the likelihood of vulnerability discovery and likelihood of vulnerability exploitation (threat agent profile) in the computation of likelihood of each node.

A threat tree demonstrates the different threat propagation pathways, highlighting the different tasks a threat agent must accomplish to breach the security of an information management system. A node in the threat tree indicates a goal or sub-goal the threat agent has to accomplish in order to breach the security of a given information system asset (Figure 4-8).

Let a node (P) be a root node and  $(w_1, w_2, w_3)$  be a 3-tuple of stochastic variables representing attributes of a root node (Algorithm 1). The likelihood of P, depends on  $w_1$ ,  $w_2$  and influence ( $w_3$ ) of any of its sub-nodes. To determine the likelihood of the threat P, a recursive algorithm is applied on node P (Algorithm 1).

The algorithm first traverses the threat tree until it finds the most left leaf node before recursively computing the likelihood of each node as illustrated in Figure 4-8. The threat tree processing algorithm (Algorithm 1) is presented below.

```

1. PROGRAM ThreatLikeliHood;
2.
3. TYPE
4.   W3_values = array [1..3] of Real;
5.
6.   Node = ^NodeRec;
7.
8.   NodeRec = RECORD
9.     Name : String;
10.    W_values : W3_values;
11.    LeftMostChild : Node;
12.    NextChild : Node;
13.    ParentNode : Node;
14.  END;
15.
16. {-----}
17. {Calculate the likelihood of a given node, what we call node weight}
18.
19. FUNCTION CalculateThisNode (P : Node) : Real;
20. VAR
21.   w1, w2, w3 : Real;
22. BEGIN
23.   w1 := P^.W_values[1];
24.   w2 := P^.W_values[2];
25.   w3 := P^.W_values[3];
26.
27.   CalculateThisNode := w1 + w2 + w3
28.                       - w1 * w2 - w1 * w3 - w2 * w3
29.                       + w1 * w2 * w3
30. END; {CalculateThisNode }
31.
32. {-----}
33. {Calculate the likelihoods of all nodes in a tree }
34.
35. FUNCTION Evaluate (N : Node) : Real;
36. VAR
37.   Max : Real;
38.   h : Real;
39. BEGIN
40.   IF T^.LeftMostChild = Nil THEN      { we have a single node without
      children }
41.     Evaluate := CalculateThisNode (N)
42.   ELSE BEGIN
43.     T := N;
44.
45.     { First we calculate the child influences parameter W3_values[3]
46.       by recursively processing the subtree of N }
47.     T := T^.LeftMostChild;      {we start with the leftmost child }
48.     Max := Evaluate (T);
49.     WHILE T^.NextChild <> Nil DO BEGIN {and then visit the other
      children }
50.       T := T^.NextChild;
51.       h := Evaluate (T);
52.       IF h > Max THEN Max := h
53.     END;
54.     N^.W3_values[3] := Max;
55.

```

```

56.    { Now we can evaluate node N itself }
57.    Evaluate := CalculateThisNode (N)
58.    END;
59.END; { Evaluate }
60.
61.{-----}
62.BEGIN
63.
64.END.

```

## *Algorithm 4-1: Threat Likelihood Computation along the Threat Path*

In the next section we discuss a typical Threat Net Approach likelihood computation based on the scenario introduced in section 4.2.

### **An example of determining threat likelihood (Figure 4-8)**

*Considering the scenarios discussed in section 4.2. Let A be the Threat to access a patient's medical records without authorization by a group of radical hackers. A can be achieved by blackmailing a doctor to reveal the patient's record (C) or by getting a password to ClinicMaster System (B). Getting a password can be achieved by pretending to be a doctor (D) or cracking the password (E). The likelihood of B depends on the likelihood of D or E as independent variables. Thus if likelihood of D and E is 0.44 and 0.46 respectively. Assuming that the likelihood of vulnerability discovery at node B is 0.2 and the profile of threat agent is 0.5 and the child influences on B is the 0.46. Then, the likelihood of number B is computed using equation 4.2, resulting into the 0.78 as likelihood of B. Assuming the likelihood of C is 0.46 and the likelihood of vulnerability discovery at A is 0.1 and the threat agent profile at A is 0.4. Applying algorithm 1 on node A results into 0.88 as the likelihood of node A. Given that B and C, are alternative threat progression routes, threats always exploit the most likely route, i.e. that one with the highest likelihood.*

The example provided illustrates the relevancy of background knowledge in the evaluation of threat likelihood. Without background knowledge the likelihood of threats could be unrealistically estimated. In general, threat likelihood values above 0.5 indicate a high chance of the threat occurring, while likelihood valves near 0.0 indicate a lower chance of the threat happening.

To minimize the influence of expert natural bias in the assessment of likelihoods, the Threat Nets Approach recommends at least 2 or more security experts assess the threat before the business analyst can determine the threat impact. While the number 3 may appear arbitrary, Nielsen and Mack (1994) suggested that when aggregating expert opinion, a small sample size can be appropriate.

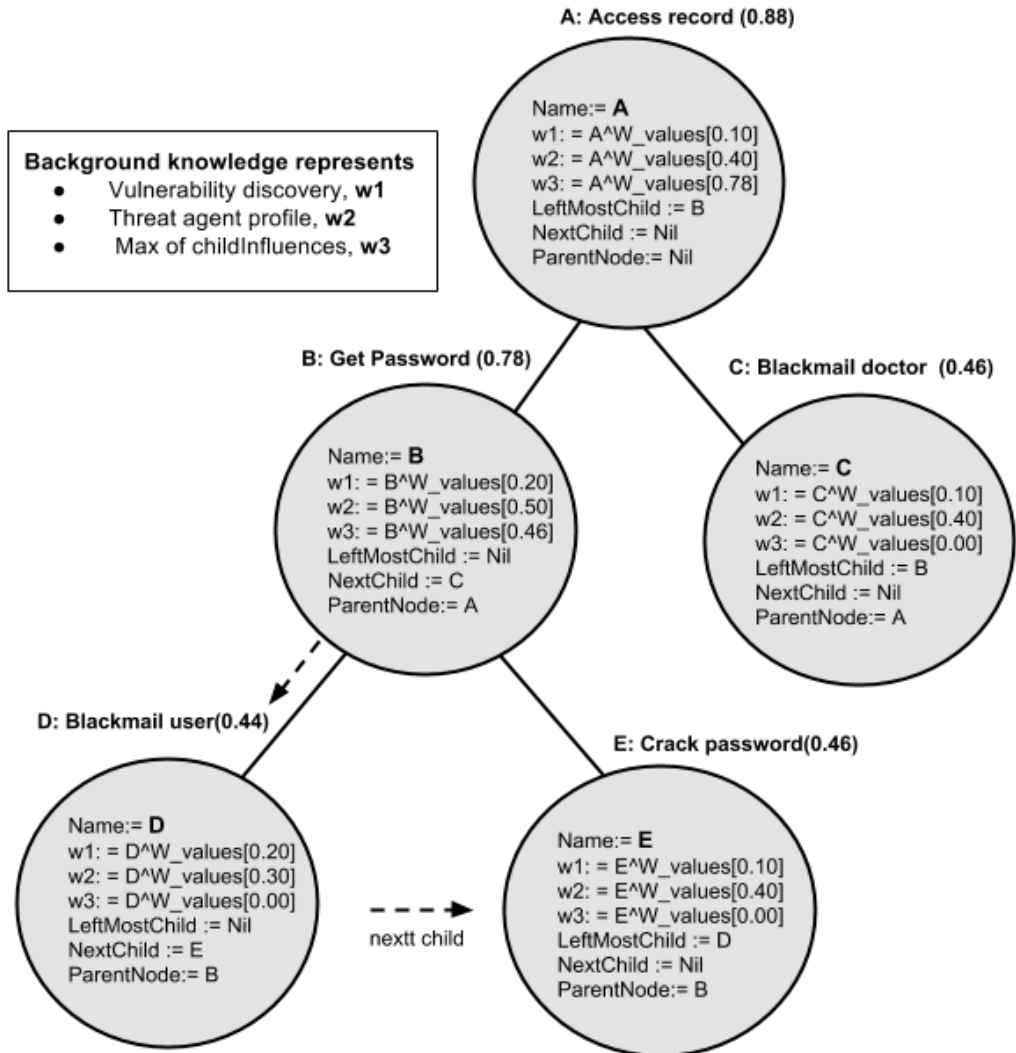


Figure 4-8: A Threat Tree Illustrating a Threat Progression

## Step 2: Threat Impact Evaluation Service

The threat impact evaluation service provides guidelines and tools of evaluating the Threat Business Impact (TBI). According to OWASP-RRM (2014) and Houlding et al.(2012) the impact of a threat on a healthcare information management system can be measured based on technical and business factors. Technical factors focus on estimating the impact on



confidentiality, integrity, authentication and availability of the system. While business factors aims at estimating the lost business value. Consequently, the Threat Nets Approach builds on OWASP framework to assess Threat Business Impact (TBI). The Threat Nets Approach proposes that, the Threat Business Impact be estimated from Lost Productivity, Brand Damage, and Cost of Recovery. To accomplish the task of threat impact evaluation, the following steps are followed as reflected in Figure 4-9 and described in Table 4-4.

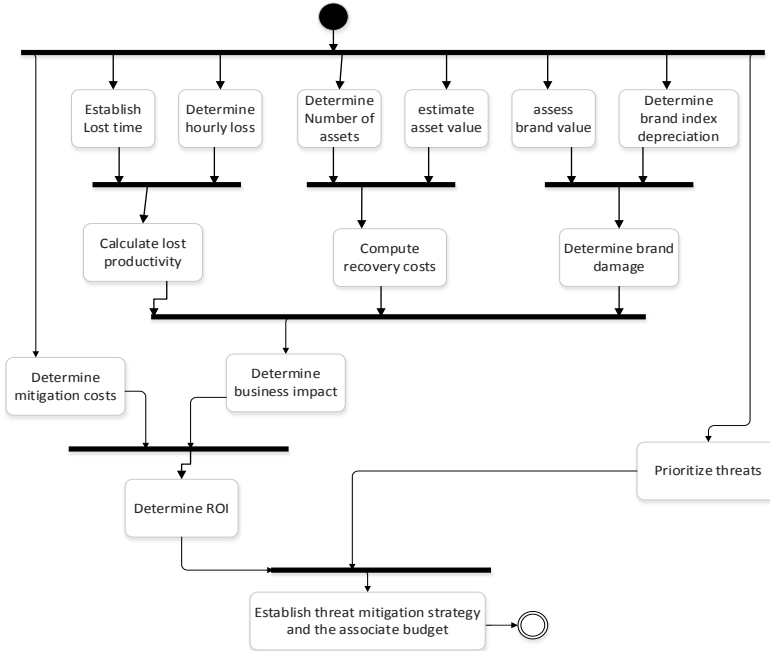


Figure 4-9: Threat Impact and ROI Evaluation Activity Diagram

Table 4-4 presents the proposed guidelines for conducting threat impact evaluation.

Task	Guidelines	Actor
Step 1: Mitigation control definition	1.1 Scan the environment to establish potential mitigation controls 1.2 Prescribe mitigation controls for each threat 1.3 Determine if controls are complementary to each other 1.4 Asses and rank the controls based on effectiveness on the scale of 1-5 1.5 Generate a threat analysis report that includes the vulnerabilities identified, threats likelihood, threat impact and mitigation controls 1.6 Communicate the threat analysis report to business analysts and the project manager for their action	Security expert
Step 2: Determine threat impact	1.1 Determine the lost productivity due to each threat 1.1.1Using employee performance data, estimate the lost productivity time	Business analyst

	per user 1.1.2 Review the human resource manual to determine hourly productivity rate for each category of users 1.2 Compute the total lost productivity 1.3 Determine the cost of recovery 1.3.1 For each threat estimate the cost of recovery in an event a threat occurs 1.3.2 Compute the total cost of recovery for all threats identified 1.4 Determine cost of mitigation controls 1.4.1 Survey the market to determine the costs for each mitigation control defined by security expert 1.4.2 Establish different permutation for the mitigation controls 1.4.3 For each permutation estimate the total costs 1.5 Using value theory (Deberu, 1972) estimate business brand value 1.5.1 Establish the brand value based on market position, sales, and brand loyalty 1.5.2 Using case studies and Keller Brand Index approach of related business, estimate the degree of threat impact on brand value 1.5.3 Estimate the brand value loss due to a given threat. 1.5.4 Using sales performance data, project the estimate sales on a given period say a year 1.6 Determine business impact by summing lost productivity, cost of recovery and brand damage (equation 3.4) 1.7 Generate a report for threat business impact	
Step 3: Determine appropriate threat mitigation controls	2.1 Rank threats based on the nature of assets, users involved, likelihood and impact 2.2 Rank mitigation controls based on their effectiveness as defined by the security expert 2.3 For each set of mitigation controls, compute the return on investment 2.3.1 Based on the nature of asset, threat likelihood and impact generate a threat priority list 2.3.2 Communication the final report to the CEO for decision making	Project manager

*Table 4-4: Guidelines for Conducting Threat Impact Evaluation*

### ***Lost Productivity Computational Model***

Lost Productivity (LP) is determined from total lost time per user category and hourly losses in business output. A user category refers to the group of information system users with similar job descriptions like doctors. Lost Productivity is determined in monetary terms (i.e., the unit of measure is currency). Let  $L = (l_1, l_2, \dots, l_n)$  be a set of hourly losses for each category of users  $l_i$  and let  $T = (t_1, t_2, \dots, t_n)$  be a set of lost time for each category of users. Then LP can be computed from;

$$\text{Lost Productivity (LP)} = \sum_{i=1}^{i=n} l_i t_i$$

### ***Cost of Recovery Computational Model***

The cost of recovery is estimated as the product of number of affected assets and the unit cost of restoration (asset value). Let  $A = (a_1, a_2, \dots, a_n)$  be a set of number of assets in each asset category and let  $V = (v_1, v_2, \dots, v_n)$  be a set of asset value or restoration cost per asset in the category. An asset category refers to a groups of information system assets with similar functionalities and roles like sensors in RPMS. Then, the Recovery Cost (RC) can be computed using;

$$\text{Recovery Cost (RC)} = \sum_{i=1}^{i=n} a_i v_i$$

### ***Brand Damage Computational Model***

Brand Damage (BD) is estimated from brand value loss considering known brand market share and loss of customer brand loyalty (Eyler, 2005). The Threat Nets Approach adapts Keller's interbrand brand index approach (Keller, 1998; Abratt & Bick, 2003) to estimate the brand value, upon which Brand Damage is estimated. The brand index approach is selected because it provides parameters of quantifying brand value loss (Abratt & Bick, 2003; Keller et al., 2011). Table 4-5 presents parameters adapted to measure brand valve with their associated weights. The weights are derived from the interbrand parameter framework discussed in Abratt and Bick (2003).

<b>Factor</b>	<b>Weight (%)</b>	<b>Description</b>
Market (M)	50	This factor measures extent to which a threat impacts on the market share of a given hospital. It can be estimated from project reduction in the number of new patient.
Customer loyalty and brand appreciation (S)	50	This measures patient loyalty to a given hospital. Specialized hospitals constantly command customer loyalty despite IT security concerns. This can be estimated from the patient feedback and number of patients switching from the hospital to other hospitals.
<b>Total</b>	<b>100</b>	

*Table 4-5: Brand Value Evaluation Factors*

Factors M and S are evaluated on the scale of 0.0 to 1.0. In estimating the brand index damage, it's assumed that before the threat the brand index (*Brand*) is 100. Therefore, a Brand Index Depreciation (*BID*) can be evaluated as;

$$\text{Brand Index Depreciation (BID)} = (M * 50) + (S * 50)$$

$$\text{Brand Damage (BD)} = \left(\frac{BID}{100}\right) * \text{Income} \dots\dots\dots (4.3)$$

*Income* measure the predicted value of sales in a given period attributed to brand value and is determined by the business analyst based on sales projection data for a given accounting period usually a month or 1 year.

#### ***Threat Business Impact Computational Model***

Threat Business Impact is measured as a monetary value

$$\text{Threat Business Impact} = LP + BD + RC \dots\dots\dots (4.4)$$

To minimize the influence of natural bias in TBI estimates, the Threat Nets Approach dictates that more than 1 business analysts must make individual evaluations. Then the final TBI is computed as the average of the individual business analyst's assessments. Table 4-6 illustrates a typical evaluation of threat business impact using a spreadsheet application for technical fault incident that made ClinicMaster system describe in section 4.2 unavailable to users for a period of 2-4 hours.

Threat Nets Approach: Threat Business Impact Assessment Computational Model						
Lost Productivity						
User category	Doctors	Nurses	Lab Technicians	Accountants	Pharmacist	
Number	10	30	8	4	4	
Lost time (hr)	4	4	2	2	4	
Hourly Business loss (USD)	36	2	10	5	300	
Loss value per user category (USD)	1,440	240	160	40	4,800	
Total lost productivity (USD)	6,680.00					
Cost of Recovery						
Asset category	Data	Software	Servers	Personal Computers	People	Network
Number of asset	-	1	-	-	-	-
Asset unit cost (USD)	-	3,000	-	-	-	-
Total cost per category (USD)	-	3,000	-	-	-	-
Total cost of recovery (USD)	3,000.00					
Brand Damage						
Brand Index parameters	Market Share	Customer Loyalty				
Brand depreciation score	0.1	0.09				
Projected income based on brand value in one month	75,000.00					
BID	9.50					
Brand damage (USD)	7,125.00					
Threat Business Impact (USD)	16,805.00					

Table 4-6: A Typical Threat Business Impact Evaluation

The input data in the threat business impact scenario in Table 4-6 is based on realistic estimates provided by a key informant following an incident when the servers crashed due to technical fault at a hospital in Kampala, Uganda in 2013.

### Step 3: ROI Evaluation for Threat Mitigation Controls

Top organization management, project managers and business analysts, use the Return on Investment (ROI) service to evaluate the efficiency of investments, that is to say compare the efficiency of a number of mitigation control investment options. ROI measures the estimated benefits an organization will get by investing in a given IT infrastructure (Keen, 2011). A high ROI means the investment gains compare favorably to investment costs. ROI

is unit less and is measured as a ratio of the difference between threat business impact (TBI) and total mitigation costs over total mitigation costs as illustrated by equation 4.5.

$$ROI = \frac{\text{Threat Business Impact (BI)} - \text{Total Mitigation Costs}}{\text{Total Mitigation Costs}} \dots\dots\dots (4.5)$$

Table 4-7 illustrates a typical ROI computation model for the scenario described in section 4.2.

Threat	Threat Description	Mitigations	Total Cost (USD)	Rank (1-10)	Threat Business Impact (USD) for 1 year	ROI
Threat1	Patient data is vulnerable to loss of integrity due to the use of doctor's profiles by lab technicians.	Install a cryptographic tool to check data integrity	15,000.00	7.00	80,000.00	4.33
		Conduct a security awareness training for users	2,000.00	6.00	80,000.00	39.00
Threat2	The availability of patient record is vulnerable to network failures due to the lack of redundancy	Mirror ClinicMaster servers to increase redundancy	50,000.00	7.00	201,660.00	3.03
		Use cloud services	8,000.00	8.00	201,660.00	24.21
Threat3	Patient data is vulnerable to unintended disclosure resulting into loss of confidentiality	Install Public Key Infrastructure (PKI) to encrypt patient data	20,000.00	8.00	100,000.00	4.00
		Train doctors and nurses on how to minimize patient data linkage through social engineering and passive attacks	4,000.00	7.00	100,000.00	24.00
		Strengthen the role based access control with biometric authentication for both patients and users	7,000.00	8.00	100,000.00	13.29

*Table 4-7: A Typical ROI Computational Model*

The computation model illustrated in Table 4-7 is extracted from a spread application (Microsoft Excel) used to analyze threat mitigation control options. The black cells shows the most cost-effective option based on ROI and mitigation control effectiveness rank.



## 5. Threat Nets Approach Evaluation

---

*This chapter describes the evaluation of the Threat Nets Approach to ascertain its completeness, usefulness and usability. The evaluation focused on establishing whether the extracted requirements and the proposed Threat Nets Approach were appropriate in addressing the threat analysis challenges. In section 5.1, the objectives of the evaluation are discussed. Section 5.2 presents the evaluation parameters and procedures starting with the selection of evaluators and describing the step by step activities of the evaluation process. In section 5.3 results of the evaluation are presented in relation to the requirements established in chapter 3. The chapter concludes with interpretation and discussion of evaluation results in section 5.4.*

### 5.1 Evaluation Objectives

An evaluation of the Threat Nets Approach was done in order to establish if the approach would enhance the decision making on threat likelihood, threat impact and threat mitigation control ROI analysis. Consequently, the approach was used by security experts and business analysts on two case studies in order to;

- 1 Assess the appropriateness of procedures and activities defined in the Threat Nets Approach (completeness of the approach).
- 2 Ascertain its usefulness in determination of threat likelihood.
- 3 Asses its usefulness in computation of threat business impact.
- 4 Asses its usefulness in evaluation of ROI on threat mitigation controls.
- 5 Asses the usefulness of coordination guidelines.
- 6 Determine the usability of the approach.

### 5.2 Evaluation Parameters and Procedures

To ascertain the completeness, usefulness and usability of the Threat Nets Approach, an expert evaluation was carried out. According to Rossi et al. (2004) and Hevner et al. (2004) design science researchers should meticulously evaluate their artefacts in order to make sound judgment about their utility. The evaluation process involved the design of an evaluation plan as suggested by Davis (1989). To attain objective judgments about the Threat Nets Approach with minimal bias, the evaluation involved the definition of suitable parameters upon which logical conclusions could be made (Hevner, et al. 2004; Phillips, 2004). Given the fact that threat analysis involves decision making about likelihood of threats, threat business impact and appropriateness of mitigation controls; *completeness, usefulness and usability* were considered as good parameters to evaluate the approach. The usefulness attribute addressed the value the approach adds to the threat analysis process,



while usability focused on its ease of use as perceived by actors (Preece et al., 1994). Completeness focused on assessing the comprehensiveness of the Threat Nets Approach activities and guidelines. Usability focused on understanding the perceived ease of use by both security experts and business analysts when analyzing threats (Endsley, 1988). Aspects of usability focused on gauging *the learnability, simplicity of theories, clarity of guidelines, and user satisfaction*.

On the other hand, usefulness focused on assessing the effectiveness of the approach in determining threat likelihood, threat business impact and ROI on threat mitigation controls. The line of reasoning is supported by Wang (2007) and Muniafu (2007), who reasoned that usefulness is the measure of the appropriateness of a design science artefact in addressing a given set of challenges.

### **Evaluation Procedure**

The evaluation of the Threat Nets Approach was conducted by domain experts (security experts and business analysts). The evaluation plan was designed based on the Situation Awareness Rating Technique (SART) suggested by Davis (1989). Situation Awareness Rating Technique is applied in the assessment of threats likelihood within a period of time and predicting their impact by experts (Endsley, 1998). SART was ideal for evaluating the Threat Nets Approach, given the fact that the evaluation exercise depended on domain experts (Davis, 1989).

The evaluation of the approach followed two steps; 1) case study analysis and 2) expert evaluation. During the case study evaluation, experts applied the approach on 2 case studies: Case Hospital and Mengo Hospital. The results of each expert analysis were subjected to a sensitivity analysis to establish whether different experts on the given case study would arrive at similar conclusions. This addresses the concerns of the reliability of the Threat Nets Approach in determining; threat likelihood, threat impact and cost-effectiveness of threat mitigation controls. During the expert evaluation the experts were given questionnaires to appreciate the approach in terms of: completeness, usefulness and usability.

### **Profile of Participants**

Fourteen participants were drawn from both the industry (11) and academia (3) of which 5 initially participated in the exploration study. A total of 9 participants were security experts and 5 were business analysts. Three business analysts were drawn from the insurance

industry of which 2 were insurance underwriters and 1 was a risk manager. The 3 business analysts from the insurance industry were accredited members of The Chartered Insurance Institute at the level of Associate Chartered Insurance Institute (ACII), while the other two were internal auditors. On the other hand, the security experts possessed one or more of the following industrial certifications of competence; Certified Information System Auditor (CISA), Certified Forensics Investigator (CFI), Certified Ethical Hacker (CEH), Cisco Certified Network Professional (CCNP), Cisco Certified Network Associate (CCNA) and Microsoft Certified System Engineer (MSCE). All security experts except one had good knowledge of the ClinicMaster healthcare information system design and operation from their previous works as information security auditors. The participants participated in two groups, one group analyzed Case Hospital and another one analyzed Mengo hospital. Table 5-1 presents the profile of the participants.

Case Hospital, N=9			Mengo Hospital, N=5
Profile	Category	Frequency	Frequency
Level of Education	PhD	1	0
	Masters	5	3
	Bachelors	3	2
Years of experience	4-6 Years	1	4
	7-10 Years	5	1
	Above 10 Years	3	0
Profession	Security experts	6	3
	Business analysts	3	2

*Table: 5-1: Profile of the Participants at Case and Mengo Hospitals*

Given the few numbers of domain experts, 14 was considered to be an ample sample size for the evaluation. Averagely, each security expert had a minimum of 6 years of experience in the field of information system threat analysis especially healthcare information management systems, while business analysts had over 5 years. The participants were purposively selected by virtue of their qualifications, knowledge about healthcare information system in particular ClinicMaster, and experience in healthcare information systems risk analysis.

### Evaluation Steps

Den Hengst et al. (2004) observed that to get quality results in an expert evaluation exercise, participants need to be reasonably knowledgeable about the problem domain and associated solutions and must show willingness to share their honest opinion. Therefore, participants

were individually approached to seek their willingness to participate in the evaluation exercise. Besides technical competencies, individual motivation to participate in the exercise was a key factor in selecting the participants.

After accepting to participate in the evaluation exercise, participants were individually introduced to the Threat Nets Approach underlying theories and the way of working. The process involved the distribution of the Threat Nets Approach to participants (Figure 5-1) and conducting individual orientation sessions.

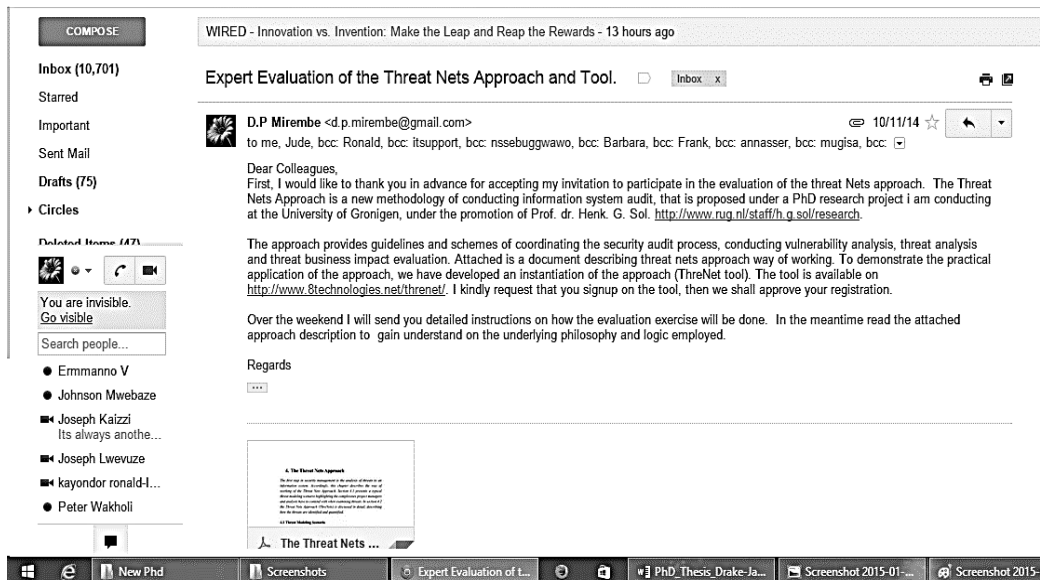


Figure 5-1: E-mail Sharing the Threat Nets Approach with Evaluators

The participants were given between 1 to 2 weeks to read and internalize the approach, before the orientation session was conducted. The orientation session focused on formal presentation of the Threat Net Approach to the participant and addressing any concerns raised. Each participant was trained on how to use the ThreNet tool and Microsoft Excel to evaluate the approach. The ThreNet tool was developed to facilitate the application of the approach and the details of the tool are discussed in Appendix 3. The orientation and training lasted for about 3 hours which included 2 hours of presentation and 1 hour of training on tools to be used. The activity was conducted from participants' offices.

The participants were then assigned a case study to analyze using the approach. The two case studies are described in the following section.

### **Case Study Descriptions**

Given the fact the case study was the main method for this study, the Threat Nets Approach was evaluated by domain experts on two case studies, namely; Case Hospital Kampala and Mengo Hospital.

#### **Case Hospital Case Description**

Case Hospital is one of the top 10 hospitals in Kampala, Uganda. The hospital boasts of about 100 beds for inpatient mainly for specialized care (Case-Hospital, 2014). The hospital serves over 450 outpatient per day. In the last 4 years the hospital has taken IT integration in the delivery of healthcare services as one of the leading strategies of transforming the hospital into a specialized center of excellence in the region. In the recent past, the hospital has acquired a number of business process automation systems including the ClinicMaster System. According to the IT manager Case Hospital, the hospital understands that automation is the future of healthcare service delivery, although it faces challenges of maintaining security of patient data and reliability of systems. The IT manager indicated that the perceived likelihood of threats and associated impact on the hospital are some of the key determinants of the decision to acquire an information system. At the time of conducting this research the hospital was conducting an internal security audit on ClinicMaster to assess the strength of their security controls and the likely impact of security breaches. It is important to note that the pilot ClinicMaster RPMS was also under implementation during the course of this study, and the analysts were allowed to assess the threats to RPMS service. While the hospital has acquired a number of information systems, the IT governance framework consisting of standards and policies are not well development.

During the application of the Threat Nets Approach, the security experts who had worked at Case Hospital as independent consultants were selected for the evaluation exercise. Relying on experts with prior knowledge about the system and the hospital reduced the need for active interaction with ClinicMaster end-users. Therefore, the IT manager provided documentation about the entire ClinicMaster system including number of users, policy framework and the description of the ClinicMaster implementation properties. Using the information provided, a case study for Case Hospital was created on the ThreNet tool (Appendix 3). The security experts used the tool to assess the threat likelihood while business analyst used a spreadsheet application to assess the threat impact and cost-effectiveness of the threat mitigation controls. The details are provided in the section “Threat Nets Approach Application”.

### **Mengo Hospital Case Description**

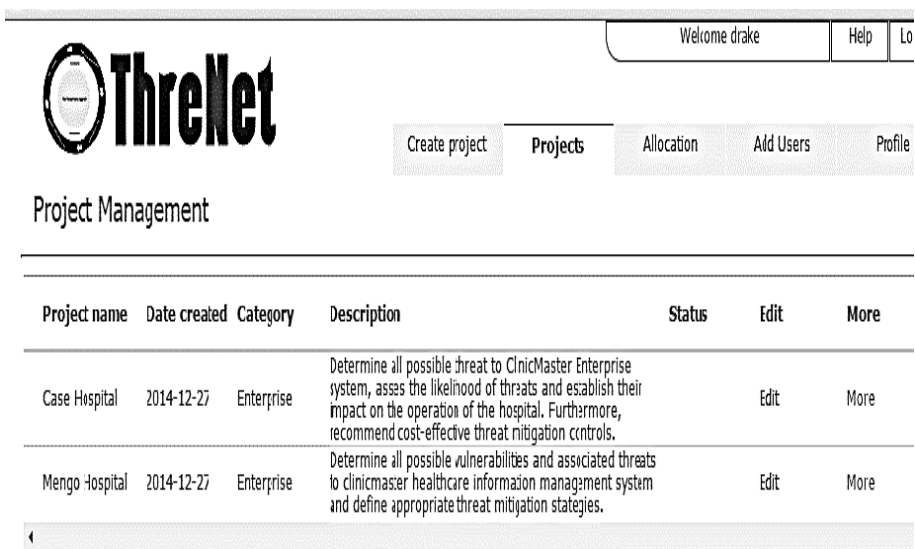
Mengo Hospital is one of the oldest hospitals in Kampala and it serves between 450 to 650 outpatients per day (Mengo-Hospital, 2014). The inpatient hospital department has about 300 beds. According to the IT Manager, the hospital has been running stand-alone information systems mainly in general administration for the last couple of years which have not provided the envisioned benefits. Therefore, in 2012 Mengo Hospital acquired the ClinicMaster System an enterprise system that integrates different departments that are involved in the delivery of services to patients. One member of the ICT committee at Mengo remarked that before the introduction of ClinicMaster, the average time to discharge an inpatient was about one and half hours. The delays were mainly due to the procedure that required every single department to clear the patient file by signing on the physical clearance form. But with the introduction of ClinicMaster, the process is down to a few minutes. The member of the ICT committee commented that “on discharge, patients have to just present their admission numbers in the Accounts department and their bill is readily available in the system”.

Just as it is at Case Hospital, Mengo Hospital takes the security of patient data and reliability of the ClinicMaster system very seriously. Accordingly, the hospital has constituted an IT department with 4 full time staff and part-time IT consultants. According to the IT Manager, the hospital has developed a fairly comprehensive IT governance framework which is aimed at preserving the reliability and integrity of records.

### **Threat Nets Approach Application on Case Studies**

Two threat analysis projects were created on the ThreNet tool and the relevant documents about each project (case study) were uploaded by the researcher who acted as the project manager. The documents contained information about the system architecture, user profiles, and governance framework refer to Figure 5-2.

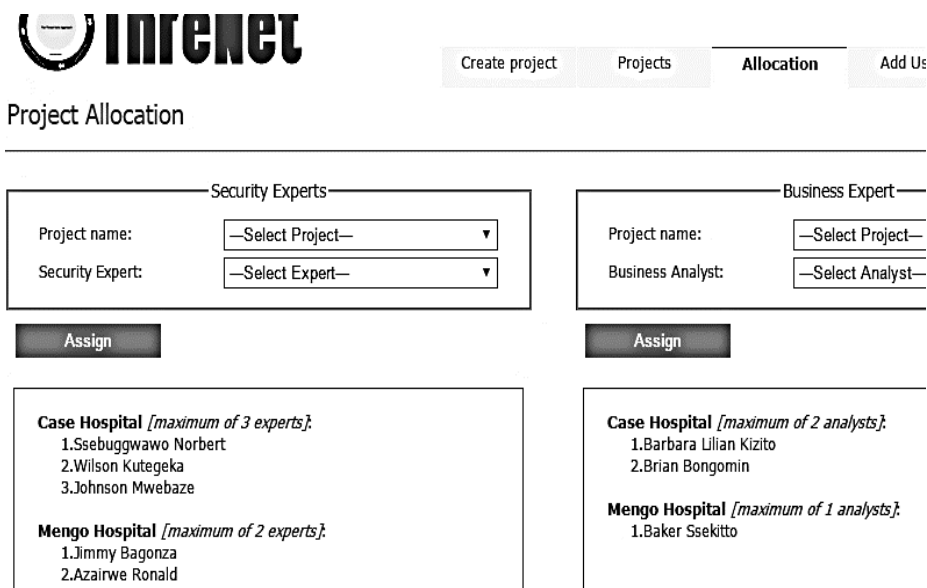
The participants were then assigned relevant roles for each case study either as security experts or business analysts in the ThreNet tool to facilitate the execution of their tasks (Figure 5-3).



The screenshot shows the ThreNet web application interface. At the top, there is a navigation bar with a logo on the left and user information on the right (Welcome drake, Help, Lo). Below the navigation bar is a secondary menu with buttons: Create project, Projects, Allocation, Add Users, and Profile. The main section is titled "Project Management" and contains a table of projects.

Project name	Date created	Category	Description	Status	Edit	More
Case Hospital	2014-12-27	Enterprise	Determine all possible threat to ClinicMaster Enterprise system, assess the likelihood of threats and establish their impact on the operation of the hospital. Furthermore, recommend cost-effective threat mitigation controls.		Edit	More
Mengo Hospital	2014-12-27	Enterprise	Determine all possible vulnerabilities and associated threats to clinicmaster healthcare information management system and define appropriate threat mitigation strategies.		Edit	More

Figure 5-2: Case Study Threat Analysis Projects Created in the ThreNet Tool



The screenshot shows the ThreNet web application interface for "Project Allocation". The navigation bar is similar to the previous screenshot, but the "Allocation" button is highlighted. Below the navigation bar, there are two main sections: "Security Experts" and "Business Expert". Each section has a form with "Project name" and "Expert" dropdown menus, and an "Assign" button. Below the forms, there are two boxes showing the assigned experts for each project.

**Security Experts**

Project name:

Security Expert:

**Assign**

**Business Expert**

Project name:

Business Analyst:

**Assign**

**Case Hospital** [maximum of 3 experts]:

- 1.Ssebuggwawo Norbert
- 2.Wilson Kutegeka
- 3.Johnson Mwebaze

**Mengo Hospital** [maximum of 2 experts]:

- 1.Jimmy Bagonza
- 2.Azairwe Ronald

**Case Hospital** [maximum of 2 analysts]:

- 1.Barbara Lilian Kizito
- 2.Brian Bongomin

**Mengo Hospital** [maximum of 1 analysts]:

- 1.Baker Ssekitto

Figure 5-3: Assignment of Roles to Threat Analysts'

Three weeks after introducing the participants to the approach and the ClinicMaster System, the participants were asked to conduct a threat analysis of the ClinicMaster healthcare information system installed at Case Hospital Kampala and Mengo Hospital, using the approach. Using the system decomposition link, the security expert assessed the completeness of each system component of; governance, human resource and software on the scale of 1 to 5 which is implicitly coded in the range of 0.2 to 1.0. Figures 5-4 and 5-5 illustrate the assessment of the completeness of the system components at Case Hospital and Mengo Hospital by experts.

Project Selection	System Description	Asset Identification	Vulnerability Identification	Security Requirements	Threat Analysis	Mi
Step 1 of 6: Case Hospital						
<div>Projects</div> <div>Select a project: Case Hospital ▼</div>		<div>System Description Guidelines</div> <ol style="list-style-type: none"> <li>1. Decompose the system into constituent features like; go software, data, network, hardware, and human reso</li> <li>2. From each feature identify all assets that need prote</li> </ol>				
<div>Project Details</div> <div>Project Identifier : 1</div> <div>Date of Initiation : 2014-12-27</div> <div>Category of Information System :Enterprise</div> <div>Description : Determine all possible threat to ClinicMaster Enterprise system, asses the likelihood of threats and establish their impact on the operation of the hospital. Furthermore, recommend cost-effective threat mitigation controls.</div> <div>Attachments 1.Clinic_Master_Brochure.docx</div>						
Software assessment	Governance assessment	Human resource assessment				
<div>Completeness of the IT security policy</div> <div>○ 1 ○ 2 ● 3 ○ 4 ○ 5</div>		<div>Completeness of the human physical and environmental security</div> <div>○ 1 ○ 2 ● 3 ○ 4 ○ 5</div>				
<div>Completeness of the human resource security policy</div> <div>○ 1 ○ 2 ● 3 ○ 4 ○ 5</div>		<div>Completeness of the communications and operations management</div> <div>○ 1 ○ 2 ● 3 ○ 4 ○ 5</div>				
<div>Completeness of the organizing information security policy</div> <div>○ 1 ● 2 ○ 3 ○ 4 ○ 5</div>		<div>Completeness of the access control policy</div> <div>○ 1 ● 2 ○ 3 ○ 4 ○ 5</div>				

Figure 5-4: Assessment of Completeness of ClinicMaster Components at Case Hospital

s.net/threNet/form22.php?name=Clinic master

8 • ajax

**Governance** **Human Resource** **Software** **Hardware**

**End Users** **IT Administrators** ☐ Not Applicable

Years of system use  
☐ 0-1 ☐ 2-4 ☐ 5-7 ☐ 8-10 ☐ 11 Above

Have had training about the information system in the past  
☐ Yes ☒ No

Level of ICT training  
☐ Basic ☒ Novice ☐ Intermediate ☐ Advanced ☐ Expert

Awareness of policies  
☐ Yes ☒ No

Level of competence in using the information system  
☐ Novice ☒ Entry ☐ Associate ☐ Professional ☐ Expert

Level of training in using the information system  
☐ Basic ☐ Novice ☒ Intermediate ☐ Advanced ☐ Expert

Level of ICT security awareness training  
☐ Basic ☐ Novice ☒ Intermediate ☐ Advanced ☐ Expert

Experience  
☒ 0-1 ☐ 2-4 ☐ 5-7 ☐ 8-10 ☐ 11 above

Industrial Certification  
☐ Novice ☒ Entry ☐ Associate ☐ Professional ☐ Expert

Level of competence in using the information system  
☐ Novice ☒ Entry ☐ Associate ☐ Professional ☐ Expert

Continuous capacity building  
☐ Never ☒ Rare ☐ Occasionally ☐ Frequent ☐ Very frequently

Terms of employment  
☐ Onsecondment ☐ Intern ☒ Part-time ☐ Consultant ☐ Full-time

About ThreNet | About Us | Help | Contact Us

*Figure 5-5: Assessment of Completeness of Human Resources ClinicMaster Component at Mengo Hospital*

For each threat identified, a security expert decomposes the threat into sub-goals, resulting into the construction of a threat tree. A threat tree is a structure that illustrates the different threat propagation pathways (Figure 5-6 and 5-7). Using likelihood of vulnerability, discoverability and exploitability, the expert computes the threat likelihood, refer to Appendix 3 for the code implementation. Figure 5-6 and 5-7 shows the interface used to compute the likelihood of unauthorized access to patient data at both Case and Mengo hospitals.



# The Threat Nets Approach to Information System Security Risk Analysis

www.8technologies.net/threnet/index.php?action=step51&name=Threat1

g Started ☐ Imported From Firef...

Select a Threat: Threat1

Threat Details

<b>Assets</b>	Patient data
<b>Vulnerability</b>	unauthorised access
<b>Threat agent</b>	disgruntled worker
<b>Security Requirement</b>	enhance privacy for patient data

1. Identify all possible threat goals (threats)
2. Decompose the threat goal into sub-goals
3. Determine the interdependence between sub-goals (independent or complimentary)
4. Follow a threat tree
5. Incorporate background knowledge in the threat tree
6. Evaluate threat likelihood
7. Compute the likelihood of each sub-goal using equation 4-1.

Level 1

☐ blackmail a nurse
 

Vulnerability discovery 
Threat Agent profile 
Possibility of Attack 
0.595

☐ AND  
☒ Or

☐ blackmail a doctor
 

Vulnerability discovery 
Threat Agent profile 
Possibility of Attack 
0.352

☐ AND  
☒ OR

☐ hacker the software
 

Vulnerability discovery 
Threat Agent profile 
Possibility of Attack 
0.271

Level 2

Vulnerability discovery 
Threat agent profile 
Possibility of Attack

☐ AND  
☐ OR

Vulnerability discovery 
Threat Agent profile 
Possibility of Attack

☐ AND  
☐ OR

Vulnerability discovery 
Threat Agent profile 
Possibility of Attack

Likelihood computation

88.8609 %

Figure 5-6: Computation of Likelihood of Unauthorized Access of Patient Data at Case Hospital

Project Management   System Description   Asset Identification   Vulnerability Identification   Security Requirements   **Threat Analysis**   Mitigation Controls

Step 5 of 6: Mengo Hospital

Threat Assessment

Select a Threat: Threat5

Threat Details

<b>Assets</b>	Patient data
<b>Vulnerability</b>	Unintended disclosure
<b>Threat agent</b>	Disgruntled employee
<b>Security Requirement</b>	preserve patient data confidentiality

Threat is likely to occur through blackmail a nurse

Level 1

blackmail doctor

Vulnerability discovery

Threat Agent profile

Possibility of Attack

0.352

AND

OR

blackmail system administrator

Vulnerability discovery

Threat Agent profile

Possibility of Attack

0.352

AND

OR

blackmail a nurse

Vulnerability discovery

Threat Agent profile

Possibility of Attack

0.488

local Disk (D:)   New Phd   Downloads   Step 5 - Google C...   PhD\_Thesis\_Drak...   PhD\_Thesis\_Drak...   Computation mo...

*Figure 5-7: Computation of Likelihood of Unauthorized Access of Patient Data at Mengo Hospital*

From the exploratory phase, it was observed that deeper threat trees don't necessary add value on the likelihood of threats. The line of reasoning is supported by Sjouke and Oostdijk (2006), who observed that deeper attacker pathways implicitly indicate low likelihood of threat occurrence. Thus, the ThreNet tool generates threat trees to a maximum depth of 3 refinement levels. Three refinement level are deemed optimal to convey all the relevant information about threat propagation pathways. Figure 5-8 shows security experts threat analysis report of authorized access of patient data at Case Hospital.

ies.net/threNet/reports/example05\_tables.php?project=1&user=kutegz

ed From Firef...

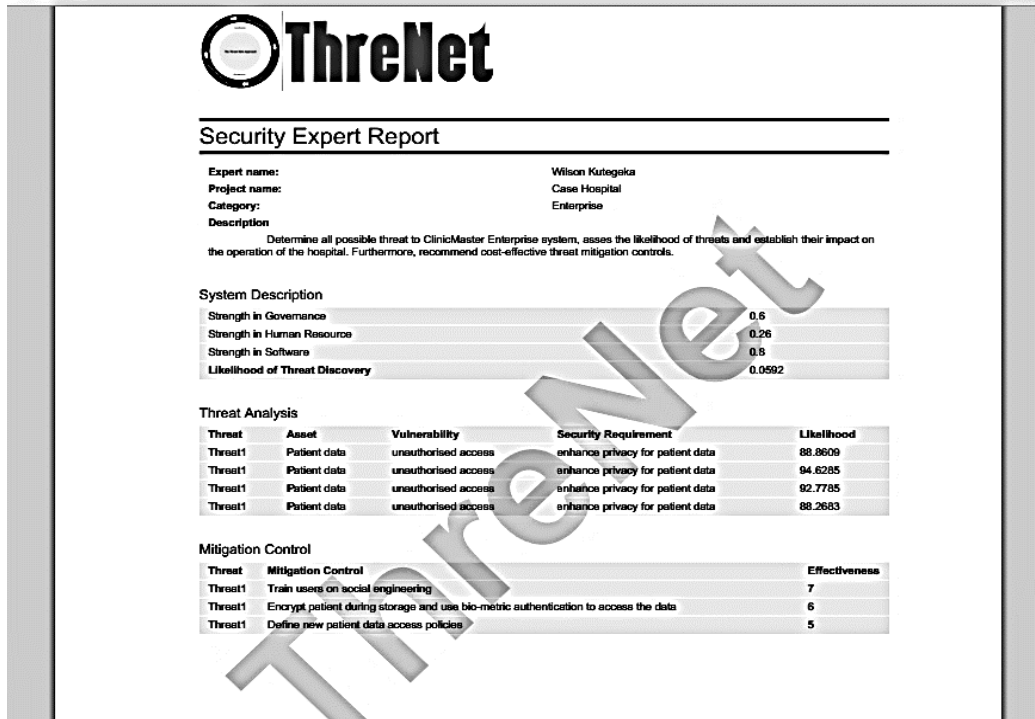


Figure 5-8: A Security Expert Report on Likelihood of Unauthorized Access to Patient Data

Business analysts mainly used Microsoft Excel to compute the threat business impact and the return on investment on threat mitigation controls. Figure 5-9 below illustrates the threat business impact analysis by a business analyst for lost network connectivity threat at Case Hospital, while Figure 5-10 illustrate the threat business impact analysis for lost connectivity at Mengo Hospital.

Microsoft Excel interface showing the Threat Nets Approach: TBI for Lost network connectivity at Case Hospital. The spreadsheet is displayed in the HOME tab, showing the ribbon with FILE, HOME, INSERT, PAGE LAYOUT, FORMULAS, DATA, REVIEW, and VIEW. The active cell is K10.

	A	B	C	D	E	F	G
1							
2	<b>Threat Nets Approach: TBI for Lost network connectivity at Case Hospital</b>						
3				BY:	Lilian Barbara Kizito		
4	<b>Lost Productivity</b>						
5							
6	<b>User category</b>	<b>Doctors</b>	<b>Nurses</b>	<b>Lab Techni</b>	<b>Accountants</b>	<b>Pharmacist</b>	
7	Number	10	30	8	4	4	
8	Lost time (Hrs)	4	4	2	2	4	
9	Hourly Business loss (USD)	36	2	10	5	300	
10	<b>Loss value per user category (USD)</b>	<b>1,440</b>	<b>240</b>	<b>160</b>	<b>40</b>	<b>4,800</b>	
11							
12	<b>Total lost productivity (USD)</b>						<b>6,680.00</b>
13	<b>Cost of Recovery</b>						
14	<b>Asset category</b>	<b>Data</b>	<b>Software</b>	<b>Servers</b>	<b>Personal Computers</b>	<b>People</b>	<b>Network</b>
15	Number of asset	-	1	-	-	-	-
16	Asset unit cost (USD)	-	3,000	-	-	-	-
17	<b>Total cost per asset category (USD)</b>	<b>-</b>	<b>3,000</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>-</b>
18							
19	<b>Total cost of recovery (USD)</b>						<b>3,000.00</b>
20							
21	<b>Brand Damage</b>						
22	<b>Brand Index parameters</b>	<b>Market Share</b>	<b>Customer Loyalty</b>				
23	Brand depreciation score	0.1	0.09				
24	Projected income						75,000.00
25	BID						9.50
26	<b>Brand damage</b>						<b>7,125.00</b>
27							
28	<b>Threat Business Impact (USD)</b>						<b>16,805.00</b>

Figure 5-9: Assessment of Threat Business Impact Lost Network Connectivity at Case Hospital

## The Threat Nets Approach to Information System Security Risk Analysis

Computation

FILE	HOME	INSERT	PAGE LAYOUT	FORMULAS	DATA	REVIEW	VIEW
Paste Cut Copy Format Painter		Calibri 10 B I U		A A A		Wrap Text Merge & Center	
Clipboard		Font		Alignment		General	
K19 : <input type="text"/>							
	A	B	C	D	E	F	G
1							
2	<b>Threat Nets Approach: TBI for Lost network connectivity at Mengo Hospital</b>						
3				BY:	Baker Ssekito		
4	<b>Lost Productivity</b>						
5							
6	<b>User category</b>	Doctors	Nurses	Lab Technicians	Accountants	Pharmacist	
7	Number	15	56	14	9	7	
8	Lost time (Hrs)	4	4	2	2	4	
9	Hourly Business loss (USD)	25	2	10	5	300	
10	Loss value per user category (USD)	1,500	448	280	90	8,400	
11							
12	<b>Total lost productivity (USD)</b>						<b>10,718.00</b>
13	<b>Cost of Recovery</b>						
14	<b>Asset category</b>	Data	Software	Servers	Personal Computers	People	Network
15	Number of asset	-	1	-	-	-	-
16	Asset unit cost (USD)	-	3,000	-	-	-	-
17	<b>Total cost per asset category (USD)</b>	-	3,000	-	-	-	-
18							
19	<b>Total cost of recovery (USD)</b>						<b>3,000.00</b>
20							
21	<b>Brand Damage</b>						
22	<b>Brand Index parameters</b>	Market Share	Customer Loyalty				
23	Brand depreciation score	0.07	0.02				
24	Projected income						75,000.00
25	BID						4.50
26	<b>Brand damage</b>						<b>3,375.00</b>
27							
28	<b>Threat Business Impact (USD)</b>						<b>17,093.00</b>
29							
30							
31							

*Figure 5-10: Assessment of Threat Business Impact of Lost Connectivity Threat at Mengo Hospital*

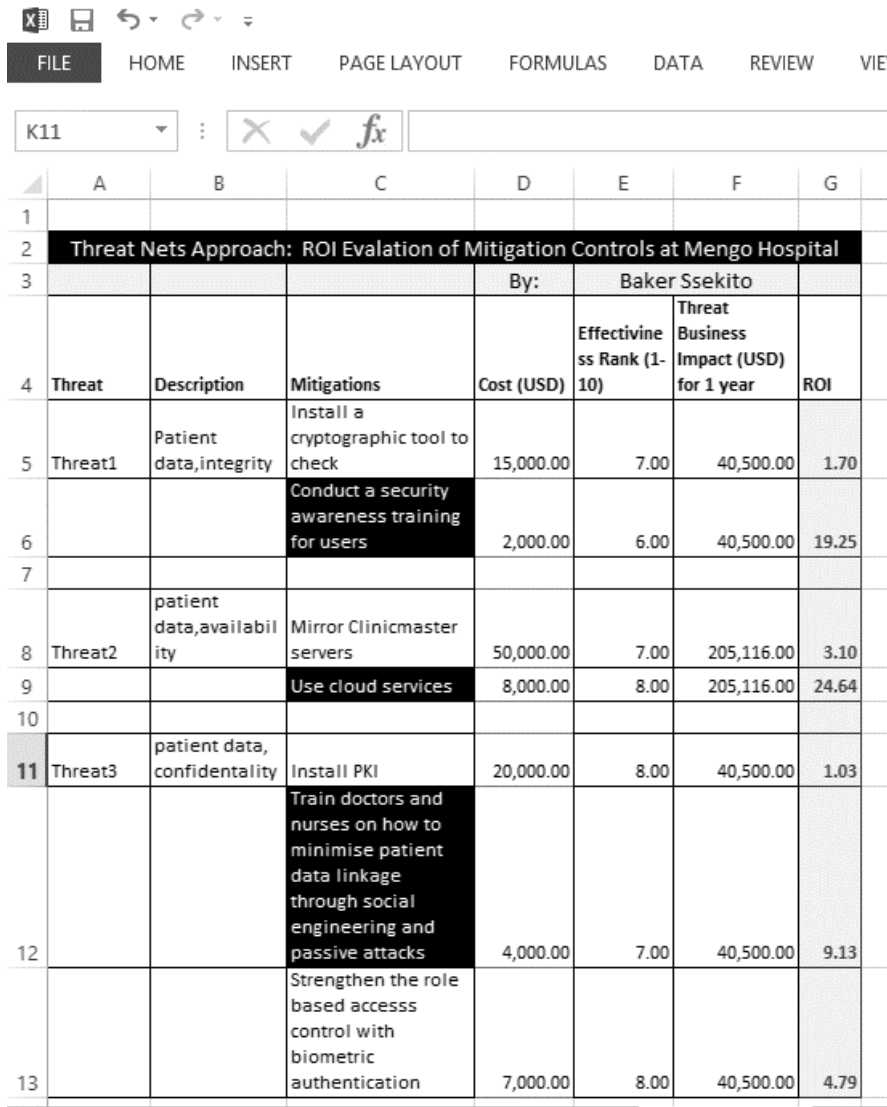
The business analysts used a spreadsheet application to assess the cost-effectiveness of the proposed threat mitigation controls at both Case and Mengo Hospitals. Figures 5-11 and 5-12 demonstrates the computation of the ROI for some threats at the two hospitals respectively.

<div> <div> <div>X</div> <div>Save</div> <div>Undo</div> <div>Redo</div> <div>Eraser</div> </div> <div> <div>FILE</div> <div>HOME</div> <div>INSERT</div> <div>PAGE LAYOUT</div> <div>FORMULAS</div> <div>DATA</div> <div>REVIEW</div> <div>VIEW</div> </div> </div> <div> <div>J9</div> <div>:</div> <div>X</div> <div>✓</div> <div>fx</div> </div>								
	A	B	C	D	E	F	G	H
1								
2	Threat Nets Approach: ROI Evaluation of Mitigation Controls at Case Hospital							
3				By:	Analyst 2			
4	Threat	Description	Mitigations	Cost (USD)	Effectiveness Rank (1-10)	Business Impact (USD) for 1 year	ROI	
5	Threat1	Patient data,integrity	Install a cryptographic tool to check	15,000.00	7.00	85,500.00	4.70	
6			Conduct a security awareness training for users	2,000.00	6.00	85,500.00	41.75	
7								
8	Threat2	patient data,availability	Mirror Clinicmaster servers	50,000.00	7.00	201,660.00	3.03	
9			Use cloud services	8,000.00	8.00	201,660.00	24.21	
10								
11	Threat3	patient data, confidentiality	Install PKI	20,000.00	8.00	85,500.00	3.28	
12			Train doctors and nurses on how to minimise patient data linkage through social engineering and passive attacks	4,000.00	7.00	85,500.00	20.38	
13			Strengthen the role based access control with biometric authentication for both patients and users	7,000.00	8.00	85,500.00	11.21	
14								

Figure 5-11: Service for Assessing Cost-Effectiveness of Threat Mitigation Controls at Case Hospital

The results in Figure 5-11 shows that the cost-effective strategy for mitigating threat 1 is to conduct a security an awareness training for users, while for threat 2, the best strategy is the use of cloud services to increase service reliability.

## The Threat Nets Approach to Information System Security Risk Analysis



	A	B	C	D	E	F	G
1							
2	<b>Threat Nets Approach: ROI Evaluation of Mitigation Controls at Mengo Hospital</b>						
3				By:	Baker Ssekito		
4	<b>Threat</b>	<b>Description</b>	<b>Mitigations</b>	<b>Cost (USD)</b>	<b>Effectiveness Rank (1-10)</b>	<b>Threat Business Impact (USD) for 1 year</b>	<b>ROI</b>
5	Threat1	Patient data,integrity	Install a cryptographic tool to check	15,000.00	7.00	40,500.00	1.70
6			Conduct a security awareness training for users	2,000.00	6.00	40,500.00	19.25
7							
8	Threat2	patient data,availability	Mirror Clinicmaster servers	50,000.00	7.00	205,116.00	3.10
9			Use cloud services	8,000.00	8.00	205,116.00	24.64
10							
11	Threat3	patient data, confidentiality	Install PKI	20,000.00	8.00	40,500.00	1.03
12			Train doctors and nurses on how to minimise patient data linkage through social engineering and passive attacks	4,000.00	7.00	40,500.00	9.13
13			Strengthen the role based access control with biometric authentication	7,000.00	8.00	40,500.00	4.79

*Figure 5-12: Service for Assessing Cost-Effectiveness of Threat Mitigation Controls at Mengo Hospital*

The participants were then asked to fill in the evaluation questionnaire about the completeness, usability and usefulness of threat nets approach via Google drive. During the evaluation week, security experts were given 3 days to complete and submit their evaluation, after which the business analysts evaluated the threat business impact. Using the

ThreNets tool, the researcher coordinated the participants. Figure 5-13 illustrates the online questionnaire.

gle.com/forms/d/1p-Hx1fgMrtseUAltj8Y69GJ\_aBeCkNZ0iF4GX2Ddzw/edit  
ted From Firef...

1 Questionnaire ☆ ■

Responses (5) Tools Add-ons Help Last edit was made seconds ago by anonymous

inge theme View responses View live form

### Threat Nets Approach Completeness evaluation

**The guidelines provided are complete**

☐ Strongly disagree  
☐ Disagree  
☐ Neutral  
☐ Agree  
☐ Strongly agree

**The approach captures all relevant information**

☐ Strongly disagree  
☐ Disagree  
☐ Neutral  
☐ Agree  
☐ Strongly agree

Figure 5-13: Online Questionnaire

The participants' responses were captured in a spreadsheet database via Google drive as illustrated in Figure 5-14.

	A	B	C	D	E	F	G	H	I	J
1	Timestamp	Highest level of Qu	Professional Qualifica	Industry	Years of FI	Place of work	The guidelines provided	The approach capture	The processes are co	The approach is easy to l
2										
3	10/21/2014 18:13:1	Bachelors	computer programmer		4-6	Industry	Agree	Agree	Strongly agree	Strongly agree
4	10/23/2014 12:59:1	PhD	Systems/Networks Management & Administrat	7-10		Both industry and acad	Strongly agree	Strongly agree	Agree	Strongly agree
5	10/23/2014 14:55:1	Bachelors	CCNA		4-6	Both industry and acad	Neutral	Agree	Agree	Strongly agree
6	10/25/2014 13:02:1	Masters	Software Developer		>10	Industry	Agree	Agree	Strongly agree	Neutral
7	10/27/2014 19:27:1	Masters	MSc. Computer Science		>10	Both industry and acad	Agree	Agree	Agree	Agree

Figure 5-14: Participants' Responses



## Evaluation Tools

The main tools for evaluation were questionnaires which consisted of 3 sections (see Appendix 4 and 5). The first section captured the evaluators' background to create the necessary disparity in the data. The second section focused on the completeness, usability and usefulness of the artifact. Section two was composed of closed ended statements that were arranged on a five point Likert scale to measure the respondents' perceived attitude to a given statement. The five point scale ranged from strongly disagree (1), disagree (2), neutral (3), agree (4), to strongly agree (5). The third section contained open-ended questions intended to capture any information that the respondents wanted to communicate to supplement the closed-ended part.

The closed ended questions were formulated as statements that were aimed at focusing the respondents to explicitly express their opinion. The statements were positively formulated for clarity and consistency as suggested by Sauro et al., (2011) and Brinkman (2009). The statements were formulated based on the 3 threat analysis parameters of; usefulness, usability and completeness as discussed in chapter 2. It is important to note that the threat analysis parameters upon which the questionnaire statements are based were derived from literature study and expert interviews.

The evaluation tools were tested for both reliability and validity. The reliability test focused on examining the internal consistency of statements, using Cronbach's Alpha. According to Brown (2002), Sekaran (2003) and Field (2005) Cronbach's alpha value above 0.7 indicates good reliability of the instrument. In our case the two instruments (Security Expert and Business Analysts tools) yielded Cronbach's Alpha coefficient ( $\alpha$ ) of 0.842 and 0.786 respectively. The Cronbach's Alpha coefficients were generated using the statistical package for social scientists (SPSS). The high Cronbach's Alpha coefficients for both tools indicated good internal consistence, implying that the tools could be relied on to provide consistent answers to the study questions as suggested by Sekaran (2003) and Brinkman (2009).

On the other hand, the instrument validity focused on establishing the clarity and completeness of statements in the tool. According to Mugenda and Mugenda (1999), validity of a tool refers to the extent to which a research tool measures what it is intended to measure. Each tool was reviewed by 3 experts who did not participate in the final evaluation to assess the validity of the statements. After the expert opinion, a Content Validity Index (CVI) was computed for each expert using the formula;

$$CVI = \frac{\text{Number of items declared valid by the experts}}{\text{Total number of items on the tool}}$$

The initial tool for security experts had 23 items (statements) and the following were the individual expert reviewer content validity index scores; 0.87, 0.91 and 0.91. Therefore, the average CVI for the 3 experts was 0.90.

The initial tool for business analysts had 24 items (statements) and the following were the individual expert reviewer content validity index scores; 0.83, 0.88 and 0.88. Therefore, the average CVI for the 3 experts was 0.86.

According to Amin (2005) a research tool with a CVI above 0.7 is valid and acceptable. Therefore, with CVI's of 0.90 and 0.86 respectively, the tools were valid.

### 5.3 Evaluation Results

This section presents results of the Threat Nets Approach evaluation by both security experts and business analysts. The results are presented in two steps, namely; the sensitivity analysis of the experts' results and analysis of their appreciation of the approach.

#### Analysis of Security Experts Results

From the exploratory and understanding phases of this research it was established that one of the key parameters of evaluating the usefulness of a threat analysis approach for healthcare information system is the consistency of the experts' results. Tables 5-2 and 5-3 show the conclusions of experts on the likelihood of unauthorized access of patient data at Case Hospital Kampala and Mengo Hospital respectively.

Security Expert	Likelihood of vulnerability discovery P(D)	Likelihood of vulnerability exploitation, P(E)	Likelihood of unauthorized access to patient data
a	0.46	0.84	0.872
b	0.59	0.86	0.925
c	0.56	0.88	0.928
d	0.58	0.94	0.941
<b>The mean (<math>\mu</math>)</b>	<b>0.55</b>	<b>0.88</b>	<b>0.916</b>
<b>Standard deviation (<math>\sigma</math>)</b>	<b>0.06</b>	<b>0.04</b>	<b>0.030</b>

*Table 5-2: Results of Expert Assessment of Likelihood of Unauthorized Access to Patient Data at Case Hospital Kampala*

Security Expert	Likelihood of vulnerability discovery P(D)	Likelihood of vulnerability exploitation, P(E)	Likelihood of unauthorized access to patient data
a	0.233	0.443	0.563
b	0.352	0.482	0.593
c	0.321	0.483	0.627
<b>The mean (<math>\mu</math>)</b>	<b>0.302</b>	<b>0.469</b>	<b>0.594</b>
<b>Standard deviation (<math>\sigma</math>)</b>	<b>0.062</b>	<b>0.023</b>	<b>0.032</b>

*Table 5-3: Likelihood of Unauthorized Access to Patient Data at Mengo Hospital*

The results in Table 5-2 and 5-3 show that the conclusions of the security experts who used the threat likelihood assessment service were consistent in both case studies. This implies that the recipes provided by the approach enable the security experts to arrive at consistent conclusions on threat likelihood of a given threat.

Table 5-4 and 5-5 illustrate the results of the threat business impact analysis for unauthorized access to patient data at both Case and Mengo Hospitals.

Business Analyst	Lost Productivity (LP)	Cost of Recovery (CR)	Brand Damage	Threat Business Impact (TBI)
a	0	2,000	7,840	9,840
b	0	4,000	6,520	10,520
c	0	2,500	6,910	9,410
<b>Mean (<math>\mu</math>)</b>	<b>0</b>	<b>2,833</b>	<b>7,090</b>	<b>9,923</b>
<b>Standard deviation (<math>\sigma</math>)</b>	<b>0</b>	<b>1,040.83</b>	<b>678.16</b>	<b>559.67</b>

*Table 5-4: Business Analysts Conclusions on the Impact of Unauthorized Access to Patient Data at Case Hospital Kampala*

Business Analyst	Lost Productivity (LP)	Cost of Recovery (CR)	Brand Damage	Threat Business Impact (TBI)
a	0	3,000	7,125	10,125
b	0	4,200	6,500	10,700
c	0	2,500	6,820	9,320
<b>Mean (<math>\mu</math>)</b>	<b>0</b>	<b>3,233</b>	<b>6,815</b>	<b>10,048</b>
<b>Standard deviation (<math>\sigma</math>)</b>	<b>0</b>	<b>873.69</b>	<b>312.53</b>	<b>693.19</b>

*Table 5-5: Business Analysts' Conclusions on Impact of Unauthorized Access to Patient Data at Mengo Hospital*

The results in Table 5-4 and 5-5 indicate that the decisions of business analysts who used the threat business impact evaluation service to assess the impact of unauthorized access to patient data at Case Hospital Kampala and Mengo Hospital were consistent. This suggests that the approach enables business analysts to arrive at consistent conclusions on the impact of a threat to the hospital.

### Analysis of Experts' Appreciation of the Threat Nets Approach

Tables 5-6, 5-7 and 5-8 provide the quantitative questionnaire results of the experts' appreciation of the approach for both Case and Mengo hospitals. The results are presented in form of mean ( $\mu$ ), standard deviation ( $\sigma$ ) and mode (M). Data were collected on a five-point Likert scale of; 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree. The questionnaires were tested for reliability and yielded a Cronbach's alpha coefficient ( $\alpha$ ) of 0.842 and 0.786 respectively. This implies that the questionnaires had a high internal consistency and were therefore reliable as suggested by Sekaran (2003). Table 5-6 and 5-7 presents results of security experts' appreciation of the Threat Nets Approach.

Case Hospital, N=6				Mengo Hospital, N=3		
Statements	$\mu$	$\sigma$	M	$\mu$	$\sigma$	M
<b>Completeness</b>						
The guidelines provided are complete	4.00	0.63	4	4.22	0.51	4
The approach captures all relevant information	4.17	0.42	4	4.00	0.72	4
The activities are systematically described	4.50	0.55	4	4.15	0.65	4
<b>Grand Mean</b>	<b>4.22</b>	<b>0.53</b>		<b>4.12</b>	<b>0.63</b>	
<b>Usability</b>						
The approach is easy to learn	4.33	0.82	4	4.00	0.62	4
Guidelines are clear	3.83	0.75	4	4.13	0.52	4
Theories are simple to interpret	3.50	0.84	4	3.80	0.67	4
Activity sequences are logical	4.17	0.75	4	4.10	0.82	4
The approach is easy to apply in the analysis of threats	4.67	0.52	5	4.52	0.53	5
<b>Grand Mean</b>	<b>4.10</b>	<b>0.74</b>		<b>4.11</b>	<b>0.63</b>	

*Table 5-6: Quantitative Security Experts' Results from Two Case Studies on Completeness and Usability*

Case Hospital, N=6				Mengo Hospital, N=3		
Statements	$\mu$	$\sigma$	M	$\mu$	$\sigma$	M
<b>Usefulness</b>						
The threat likelihood assessment service helps the expert to logically determine threat likelihood	4.33	0.52	4	4.12	0.45	4
Analysis of individual system component helps the expert to easily identify hidden vulnerabilities	4.33	0.52	4	4.00	0.41	4
Guidelines are useful in identifying all possible threat agents	3.33	0.82	4	3.52	0.82	4
The approach is helpful in linking system characteristics to the likely vulnerabilities	3.67	1.51	4	3.88	1.02	4
The approach is helpful in linking threat agent profile to threat likelihood	4.00	0.63	4	4.22	0.72	4
The threat likelihood technique improves the determination of threat likelihood	3.33	1.03	3	3.21	1.00	3
The approach improves coordination among actors	4.00	0.89	4	4.21	0.90	4
The approach enhances decision making on threat likelihood, threat impact and threat mitigation controls	3.67	0.52	4	3.82	0.62	4
The approach can be used on all threat analysis scenarios in a hospital	3.50	0.58	3	3.80	0.56	4
The approach improves the efficiency of threat analysts	4.17	0.41	4	4.00	0.55	4
The approach addresses all core threat analysis activities	3.50	0.55	3	3.80	0.42	4
The approach does address the key challenges in the industry	4.00	0.89	4	4.17	0.42	4
I can recommend this approach to other experts	4.50	0.55	4	4.40	0.47	4
<b>Grand Mean</b>	<b>3.87</b>	<b>0.72</b>		<b>3.93</b>	<b>0.64</b>	

Table 5-7: Quantitative Security Experts' Results from Two Case Studies on Usefulness

According to the results presented in Tables 5-6 and 5-7, the rating of the security experts on completeness of the Threat Nets Approach was positive at both Case and Mengo hospitals. The security experts noted that the approach provided complete recipes and activities were correctly described. The security experts also observed that, the approach was usable as it provided simple, clear and logical concepts which were easy to interpret and learn. The results in Table 5-7 further reveal that the approach is useful. The respondents indicated that the approach was useful in quantifying threat likelihood in healthcare information systems, and improving the efficiency of the security experts. The security experts agreed that the approach does address key challenges in the industry. However, the security experts noted that the approach could not be used to identify all possible threats nor could it be applied on every threat analysis case. Overall the results suggest that the approach is useful in enhancing decision making on threat likelihood and definition of threat mitigation controls.

Table 5-8 presents results of business analysts' opinion on completeness, usability and usefulness of the Threat Nets Approach.

Case Hospital, N=3				Mengo Hospital, N=2		
Statements	$\mu$	$\sigma$	M	$\mu$	$\sigma$	M
<b>Completeness</b>						
The approach captures all relevant information	3.67	0.58	4	3.80	0.45	4
The guidelines provided are complete	3.67	0.58	4	3.80	0.45	4
Activities for assessing threat impact are correctly described	3.67	0.58	4	3.82	0.45	4
<b>Grand Mean</b>	<b>3.67</b>	<b>0.58</b>		<b>3.81</b>	<b>0.45</b>	
<b>Usability</b>						
The guidelines to evaluate threat business impact are easy to learn	4.33	0.58	5	4.21	0.52	5
The terminologies are consistent with those in the industry	4.67	0.58	5	4.75	0.52	5
The guidelines are clear	4.67	0.58	5	4.75	0.52	5
The theories are simple to interpret	3.67	0.58	4	3.81	0.52	4
Activity sequences are logical	4.00	1.00	4	4.21	0.52	4
The concept are easy to apply in the evaluation of threat impact	3.67	0.58	4	3.81	0.52	4
<b>Grand Mean</b>	<b>4.16</b>	<b>0.65</b>		<b>4.26</b>	<b>0.52</b>	
<b>Usefulness</b>						
The guidelines are helpful in the quantification of threat impact	4.00	0.00	4	4.12	0.52	4
The scheme for computing lost productivity is very helpful	4.67	0.58	5	4.70	0.52	5
The scheme for computing cost of recovery is very helpful	4.67	0.58	5	4.70	0.52	5
The brand index approach is very helpful in the evaluation of brand depreciation	3.67	0.58	4	3.72	0.52	4
The scheme for evaluating threat business impact is very helpful	4.00	0.00	4	4.00	0.00	4
The scheme for evaluating ROI is very helpful	4.00	0.00	4	4.12	0.52	4
The coordination guidelines improves coordination among actors	4.33	0.58	4	4.21	0.52	4
The threat impact assessment service can be used to assess the impact of risks on organizations in other sectors	4.33	0.58	4	4.41	0.52	4
The approach improves the efficiency of the business analyst	4.00	0.00	4	4.21	0.52	4
The threat business impact service addresses all core aspects of risk impact quantification	3.67	0.58	4	3.70	0.52	4
The threat business impact scheme does address the key challenges in the industry	3.67	0.58	4	3.70	0.52	4
I can recommend this approach to other business analysts	4.00	1.00	4	4.00	0.00	4
<b>Grand Mean</b>	<b>4.08</b>	<b>0.42</b>		<b>4.13</b>	<b>0.43</b>	

Table 5-8: Results of Evaluation by Business Analysts

Results in Table 5-8 suggest that business analysts were positive about the completeness of the approach in determining threat business impact. The responses further reveal that the approach provides simple, clear and complete guidelines for evaluation of threat business impact. Results in Table 5-8 indicate that the approach is useful in the determination of threat business impact as it provides procedures for computation of lost productivity, brand damage, and recovery costs. This finding is supported by an observation from one of the participants in this study who indicated that “the quantification of threats business impact will help information system managers articulate the value of IT investments in boardrooms”. However, business analysts observed that the brand depreciation procedure is a bit restrictive and it might not be applicable to public organization whose market share is defined by the nature of services offered which are sought after despite negative brand publicity, for example the Mulago Hospital Heart Institute in Kampala. Overall the results suggest that the Threat Nets Approach is useful in the quantification of threat business impact.

### **5.4 Interpretation and Discussion of Results**

The results of the evaluation of the Threat Nets Approach show that the approach provides complete guidelines and procedures for evaluating threats to information systems. According to Shawn et al (2006) and Mirembe et al (2008), an ideal threat analysis approach should provide clear guidelines on how to evaluate threats in a logical manner. The Threat Nets Approach defines services on how to identify and quantify threats to an information system. The approach also provides procedures of coordinating actors during the threat analysis processes. The provision of simple, clear and complete procedures improves the efficiency of security analysts (security experts and business analysts) as indicated by the results in Tables 5-6, 5-7 and 5-8. The guidelines not only improve the efficiency of experts, but also improve the quality of their conclusions as observed from the results of security experts and business analysts’ sensitivity analysis (Table 5-2 and 5-4).

The results of the study among security experts and business analysts reveal that the approach was usable given the fact that it provided; simple, clear and logical procedures that were easy to learn and interpret. The business analysts found the approach more usable than security experts as indicated by the results in Tables 5-6, 5-7 and 5-8. The differences in the usability experience could be attributed to the differences in task complexity between business analysts and security experts. Security experts’ tasks are more complex compared to business analysts as they involve reasoning with uncertainty and heavily rely on experts’ tacit knowledge. During the understanding phase of the approach, it was noted that most of the current threat analysis approaches lack tools to facilitate their application, hence their

slow adaption in the industry. Accordingly, the ThreNet tool was developed to facilitate the use of the Threat Nets Approach in addressing the threat analysis challenges discussed in chapter 2 and 3. The high positive response on the Threat Nets Approach could in part be attributed to the ThreNet tool that aided participants in conducting threat analysis on case studies. Having an approach that is usable is a very significant attribute as literature indicates (Shawn, 2006) the adaption of any approach or system largely depends on its usability.

It was established from the evaluation results that the Threat Nets Approach was useful in determining threats and quantifying their impact on hospitals. It is worth noting that current approaches in literature do not provide schemes for combining threat analysis and quantification of threat business impact. The current practices as alluded to by key informants' document threats as mere information security concerns with no linkage to business impact. Therefore, visualizing threats in terms of business value (i.e. impact on performance of the business in value creation) will result into better understanding of threats and enhance decision making on IT healthcare infrastructure investments in hospitals. The Threat Nets Approach provides schemes for quantifying lost business value in case the threat occurs, estimating cost of recovery from a threat and quantifying the return on investment in threat mitigation controls. Business analysts observed that, estimating accurate brand value for a public hospital can be problematic since most market research organizations mainly focus on commercial enterprises which are affected by negative brand publicity. For example, a monopoly specialized hospital like the Heart Institute of Mulago Hospital, Kampala cannot easily loose patients due to threats to her information systems. It was suggested that in such cases, other less restrictive brand value estimate approaches could be adopted. Alternatively brand damage can be omitted in the evaluation of threat business impact in cases where threats have no impact on brand value.





## 6. Epilogue

---

*Understanding threats, evaluating their likelihood and impact on a hospital is essential in making decisions of adopting a healthcare information system like RPMS. It emerged during the research that threat analysts face a number of challenges including insufficient information on system vulnerabilities and threat agents, lack of guidelines on how to determine threat likelihood and impact, natural bias of threat analysts and poor coordination among actors. Therefore, without a systematic approach, identifying and quantifying threats becomes problematic. Accordingly, the objective of this research was to develop a threat analysis approach which could enhance decision making on threat likelihood, threat impact and value for money on analysis of threat mitigation controls. Consequently, this chapter provides an overview of the research (section 6.1) and discusses the key research contributions (section 6.2). In section 6.3 challenges encountered during the research are discussed. Section 6.4 provides directions for further research in the field of healthcare information systems threat analysis in particular and security management in general.*

### 6.1 Thesis Overview

The initial spark to the research was provided by reports about the failures of the healthcare system in Uganda to address the growing demand for healthcare services (Schneider et al., 2006; Lukwago, 2010). Consequently, the research began with the understanding of healthcare service delivery challenges in general and the approaches being developed to address them. The initial studies revealed that hospitals are strengthening the outpatient case management as a means of addressing the increasing demand for healthcare services (Totten et al., 2013). However, outpatient case management is faced with a number of challenges including; lack of information on patient medical history, inability to monitor patient recovery, and non-adherence by patients to prescription among others (Hickam et al., 2013). Consequently, hospitals are exploring innovative ICTs like ambulatory wireless sensor networks (RPMS) to address the fore mentioned challenges (Jin & Meng-Chu, 2010).

### Reflection on the Research Problem, Objective and Questions

Given the stringent regulatory requirements concerning the processing and storage of patient data, understanding the risks to healthcare information systems is one of the core functions of information systems managers in hospitals. Literature indicates that the adoption of RPMS by hospitals is being hampered by the perceived security threats of: loss of privacy and integrity of patient records, and reliability of service (Gao Pesto, et al., 2008; Jin &

Meng-Chu, 2010; Kartsakli, et al., 2013; Mirembe & Muyebe, 2009). But making decisions on likelihood of such threats and evaluating their impact requires an extensive analysis of threat agents and the healthcare information system under review.

Thus, without a systematic approach to conduct threat analysis, security analysts are constrained by lack of sufficient information on the information system and threat agents. The lack of sufficient information results into inaccurate decision making on the likelihood of threats and their impact on the hospital (Moshaddique & Kyung-sup, 2011). Theoretically, security analysts are assumed to have sufficient information about healthcare information systems and threat agents to make sound decisions on likelihood of threats and their associated impact on the hospital and the patient. However, given the complexity of the threat analysis process and the dynamic nature of threat agent profile, security analysts have to rely on their experience to determine the likelihood of threats and their associated impact (Walsh, 2011). Bayne (2002) notes that it is the lack of sufficient information and knowledge about system characteristics and threat agents that often results into inaccurate understanding of threat likelihood and impact. Therefore, for threat analysts to make sound decisions on threat likelihood, impact and cost-effectiveness of threat mitigation controls, they need a logical approach which provides recipes for: assessing system vulnerabilities, threat agent profiles and coordinating of actors during the threat analysis process (Oladimeji et al., 2006; VMWARE, 2013).

In chapter 2 and 3 we pointed out that the current threat analysis approaches can be categorized into 3 categories, namely: asset-centric, threat-centric and attacker-centric. Attacker-centric approaches are those that focus on profiling the attacker motivation, goals and capabilities. System-centric approaches focus on identification of system vulnerabilities. Asset-centric threat analysis approaches focus on risk assessment and approximation at asset level (Shostack, 2008). We observe that most of the approaches described in literature do not provide sound techniques of assessing threat likelihood, threat impact and the cost-effectiveness of threat mitigation controls. In addition, they lack a logical scheme of evaluating the influence of system characteristics on the likelihood of threats.

This research sought to contribute to a better understanding of threats to information systems in general and healthcare information systems in particular through the provision of 3 threat analysis decision enhancement services, namely: threat likelihood assessment service, threat business impact evaluation service and threat mitigation controls ROI evaluation service. The development of the 3 services was based on the reasoning that the slow adoption of RPMS by hospitals is in part due to perceived risks owed to the lack of a sound threat analysis approach.

Accordingly, the main objective of this design science research was to develop a threat analysis approach that would enhance decision making on threat likelihood, threat impact and value for money analysis of threat mitigation controls. It is envisioned that improved understanding of threats to healthcare information systems like RPMS will result into increased adoption of RPMS technologies in the delivery of healthcare services. In order to accomplish the research objective, the researcher set the following research questions;

1. What challenges do threat analysts face? The purpose of this question was to gain an understanding from theory and practice of the challenges that threat analysts encounter during the threat analysis process. Chapters 2 and 3 provides the answers to this research question. The answers are derived from the literature and expert survey. The results suggest that threat analysts face challenges of: inadequate information on system vulnerabilities and threat agents, lack of techniques of incorporating system characteristics in the assessment of threat likelihood, and lack of sound techniques of evaluating threat impact and the cost-effectiveness of threat mitigation controls.
2. What are the key steps in analyzing threats to healthcare information management systems? The intention of this question was to formulate a theory regarding effective threat analysis in healthcare information systems. The question was answered in chapters 2 and 3. The first part of the question is answered in chapter 2 which provides background theories which are relevant to the threat analysis problem. The study revealed that threat analysis is a decision process that involves making decisions on threat likelihood, threat impact and cost-effectiveness of threat mitigation controls. Therefore, a threat analysis enhancement approach proposed in this thesis is anchored on the decision enhancement theory of Keen and Sol (2012) and the risk management theory of Kwo-Shing et al. (2003). The approach provides 4 process enhancement recipes, namely: threat likelihood assessment, threat impact evaluation, ROI assessment of threat mitigation controls and coordination management. The approach is grounded in the threat nets theory which suggests that the assessment of threats to information systems like RPMS should be based on three sequential aspects:
  - Threat likelihood – the quantification of threat likelihood based on characteristics of system components and threat agents.
  - Threat impact – what is the impact of a threat on business output?
  - Return on Investment – what is the most cost-effective threat mitigation strategy?

3. What would be the key characteristics of an ideal threat analysis approach? The aim of the question was to enable the formulation of activities and concepts in form of services that would enhance decision making and coordination during threat analysis. This question is answered in chapter 4 with a detailed description of the Threat Nets Approach following Sol's (1982) "Way of" framework. While the development of the Threat Nets Approach was inspired by the challenges in healthcare information systems, the approach proposed in this thesis is generic and can be applied to other information systems.
4. What are the appropriate parameters for evaluating a threat analysis approach? The purpose of the question was to establish the parameters of evaluating the utility of the approach. The question is answered in chapters 2, 3 and 4. In chapter 3, a survey among IT security experts was conducted to ascertain the parameters which the experts considered relevant for evaluating the utility of a threat analysis approach. The parameters identified by the respondents were: usefulness in determining likelihood of threats and their associated impact, consistency of threat profiles generated, ease of use, and learnability. The parameters suggested by experts are supported by Shostack (2008) and Scandariato et al. (2013) who arrived at similar conclusions during the assessment of the STRIDE approach. In chapter 5, the aforementioned parameters were used to evaluate the Threat Nets Approach. During the assessment of the evaluation tools, experts again found the parameters to be relevant.

### **Reflection on the Research Approach**

In order to address the key research question of this study, which is "How can information systems threat analysis be enhanced", this design science research adopted an interpretivism research philosophy with a pragmatic epistemological stance. The interpretivism philosophy is appropriate given the fact that the research involved learning through understanding the problem domain, developing, and applying the Threat Nets Approach. The research followed the inductive hypothetical research strategy of Sol (1982) to develop the threat nets theory and the associated approach. The inductive-hypothetic strategy often starts with a set of observations from which patterns are extracted to formulate a theory which is later tested and generalized (Gonzalez & Sol, 2012). The strategy was executed in five phases, namely the: initial, abstraction, theory formulation, implementation and evaluation phases.

The initial phase (the empirical description) was aimed at understanding the underlying threat analysis challenges, requirements for the approach, and establishing the variables needed for evaluating the approach (problem domain definition). The empirical description

was achieved through an extensive exploratory study, which involved literature review and semi-structured interviews among IT security experts in Uganda. Information from the initial phase was analyzed and it resulted into the abstraction of the essential aspects of the threat analysis process and the associated threat analysis approach requirements (abstraction phase). From the abstraction phase, the threat nets theory and the associated approach were developed. The Threat Nets Approach is described using Sol's (1982) "Ways of" framework in terms of "way of thinking", "way of governance", "way of modeling" and "way of working". To facilitate the application of the approach by security analysts, a web based ThreNet tool was implemented.

In order to ascertain whether the Threat Nets Approach enhances the threat analysis process, a case study based evaluation by experts was conducted at Case Hospital Kampala and Mengo Hospital. The evaluation focused on gauging the completeness, usability, and usefulness of the approach. The respondents rated the approach as being very usable. Citing the clarity of recipes and terminologies. The results of the evaluation further revealed that the approach provided complete recipes and concepts for assessing threat likelihood, threat impact and ROI on threat mitigation controls. The respondents also observed that the approach was very useful in enhancing decision making on likelihood of threats, threat impact and evaluation of cost-effectiveness of proposed threat mitigation controls. The results of the evaluation further revealed that the proposed coordination recipes indeed enhanced coordination among actors during the threat analysis process. The sensitivity analysis of the experts' results revealed that experts applying the approach arrived at consistent results, indicating that the approach minimizes the impact of individual bias when making decisions on; likelihood of a threat, threat impact and cost-effectiveness of threat mitigation controls.

## **6.2 Contributions to Society and Knowledge**

This research makes a number of contributions to society and to the body of knowledge. In order to establish requirements for an ideal threat analysis approach, the research begun with the understanding of the existing approaches, thereby identifying their limitations which included; lack of recipes to guide the process, lack of techniques to evaluate threat likelihood and threat business impact. The identification of threat analysis challenges addressed the first research question. Therefore, the study make a contribution to literature on threat analysis in healthcare information systems.

Key to information system security management is the understanding and evaluation of threats. From the exploratory phase of the research, requirements for a threat analysis approach were established as;

- Provision of step by step guidelines on how to analyze threats
- Provision of techniques to evaluate threat likelihood
- Provision of techniques to evaluate threat business impact
- Provision of recipes to facilitate coordination among IT security experts, business analysts and other actors
- Provision of recipes for evaluating the cost-effectiveness of threat mitigation controls.

Accordingly, the Threat Nets Approach is proposed to provide the fore mentioned services. The identification of requirements, formulation of the threat nets theory and the development of the Threat Nets Approach, addresses research questions 2, 3 and 4 of the thesis.

The Threat Nets Approach provides recipes on how to analyze threats to healthcare information management systems like ClinicMaster. The approach incorporates information system background knowledge (vulnerabilities and threat agent profile) in evaluation of threat likelihood and threat business impact. The threat nets theory and approach are key contributions to the field of information systems security as the field progresses towards the development of automated threat analysis tools. To the best of our knowledge, the Threat Nets Approach is one of the first attempts of visualizing the impact of information system threats on an organization in terms of lost brand value, lost productivity and cost of recovery. The approach combines concepts from system-centric, attacker-centric and asset-centric approaches, creating a high-breed threat analysis approach. The threat nets theory and the Threat Nets Approach are contributions to the body of knowledge.

Besides providing a sound threat analysis approach, this research provides the ThreNet tool (Appendix 3) to facilitate the application of the approach. The tool addresses the practical challenges of coordinating actors during the threat analysis process. The ThreNet tool also provides recipes to the security experts on how to infer threat likelihood from system features. In addition, the ThreNet tool implements schemes of computing likelihood of vulnerabilities and threats, threat business impact and return on investments in threat mitigation controls. Furthermore, the research proposes parameters for evaluating any threat analysis approach as deliberated in chapter 2 and 3 of this thesis. Accordingly, the ThreNet tool is a contribution to society.

### 6.3 Research Limitations

The major challenge was to get hold of security experts and business analysts for both exploratory and evaluation activities. The majority of the participants are busy people with strict and often unpredictable work schedules. The consequence of this limitation was mitigated by flexible scheduling of activities by the researcher in order to accommodate participants schedules. Another strategy used to mitigate this challenge was to source for participants in excess of the desired minimal numbers.

Another challenge was to get hospitals to act as cases study sites. Most hospitals cited the sensitivity of their information and the dangers associated with potential information leakage about weakness in their current healthcare information system management practices. This challenge was minimized by working directly with the supplier of ClinicMaster healthcare information. The supplier had direct access to the people who matter and offered guarantee to IS managers at the two hospitals that the research activities would not modify or attempt to manipulate the system.

### 6.4 Conclusions and Future Works

The section presents the researchers' reasoning about the utility of the Threat Nets Approach and outlines concepts that need further investigation.

From the discussions so far, it is clear that healthcare information system threat analysts need a pragmatic approach that provides recipes on how to evaluate threats to an information management system like RPMS. Accordingly, this thesis provides a solution in form of "the Threat Nets Approach", which offers clear and concise recipes for identifying system vulnerabilities and threat agents, evaluating threat likelihood and threat business impact. The approach also provides recipes for assessing the cost-effectiveness of the different threat mitigation controls. The results of the evaluation exercise show that the approach does address the critical challenges in the areas of information systems risk analysis. The respondents observed that the approach does provide complete recipes for analyzing threats to information systems. The respondents also noted that the recipes are usable and useful in enhancing decision making on threat likelihood, impact and on the return on investment. Basing on the positive responses on completeness, usability and usefulness by both security experts and business analysts, we conclude that the Threat Nets Approach proposed by this study enhances the threat analysis process, hence the objective of the research was achieved. However, further investigation needs to be done on the following;



**Recommendation 1:** The Threat Nets Approach was evaluated by ten experts to ascertain its completeness, usefulness and usability. Ten is relatively a small number to rely on generalized results of the study. Therefore, there is need to have the approach evaluated by a large number of security experts and business analysts. A large diverse number of test users often improves the quality of conclusions as it minimizes local context limitations like natural bias by respondents.

**Recommendation 2:** There is need to have the approach evaluated by experts who have not been exposed to the ThreNet tool in order to ascertain their appreciation of the approach. Their results would be compared with our results to gauge the usefulness of the approach independent of the ThreNet tool.

**Recommendation 3:** Special attention needs to be given to the threat business impact evaluation service, in order to identify other computational models for estimating brand depreciation. The brand depreciation technique used in this study relied on estimation of patient royalty based on follow-up visits and brand appeal based on number of new patients registered in a given period of time. There is need to investigate the performance of other less restrictive brand estimation techniques in evaluating brand damage such as those suggested by Abratt and Bick (2003).

**Recommendation 4:** There is need to have the approach evaluated by security experts and business analysts from other countries/regions to determine whether they would arrived at similar conclusions about the utility and usability of the approach. It is important to note that lack of collaboration among experts was ranked low in our study (p.35): This contradicts Ruiz et al., (2012) who cited lack of collaboration among experts as a major challenge. This could be attributed to the fact that in the Ugandan context, experts collaborate informally due to strong social ties as observed by one of the key informants to the study.

## References

---

- Abratt, R. & Bick, G. (2003). Valuing brands and brand equity: Methods and processes. *Journal of Applied Management and Entrepreneurship*, 8, 21-39.
- Ajzen, I. (1991). The theory of planned behavior 50. *Organizational Behavior and Human Decision Processes*, 50(1), 179–211.
- Alasdair, L., Adshead, S. & Ellen, B. (2008). *Technology in the NHS: Transforming patient's experience of care*. London: The King's Fund.
- Allen, S. L. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization Science*, 2(4), 342–365.
- Alter, S. (2012). Challenges for service science. *Journal of Information Technology Theory and Application*, 13(2), 22-37.
- Amin, M. (2005). *Social Science Research: Conception, Methodology and Analysis*. Kampala: Makerere University Printery.
- Amiyo, M. R. (2012). Decision enhancement and business process agility . *PhD Thesis*. Groningen, The Netherlands : University of Groningen .
- Anderson, R., Chan, H. & Perrig, A. (2004). Key infection: Smart trust for smart dust. *Proceedings of the Network Protocols, 12th IEEE International Conference* (pp. 206 - 215). IEEE Computer Society.
- Aregu, R. (2014). Market and price decision enhancement services for farmers in Uganda. *PhD Thesis*. Groningen, The Netherlands : University of Groningen.
- Ash, J. S., Berg, M. & Coiera, E. (2004). Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *Journal of the American Medical Informatics Association*, 11(2), 104-112.
- Baynes, J. (2002). *An Overview of Threat and Risk Assessment*. SANS Institute. Retrieved on October 11, 2014, from <http://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76>.
- Borsotto, M., Savell, C., Reifman, J., Reed, W., Gavin, N. & Crick, J. (2004). Life-Signs determination model for warfighter physiological status monitoring. *Publication RTO-MP-HFM-109-28*. NATO Research and Technology Organization.
- Boutayeb, A. (2006). The double burden of communicable and non-communicable diseases in developing countries. *Transactions of the Royal society of Tropical Medicine and Hygiene*, 100(3), 191-199.
- Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Resaerch in Psychology*, 3(2), 77-101.
- Brian, W. (2013). Emerging trends in healthcare. Retrieved on March 28<sup>th</sup>, 2015 from <http://www.pwc.com/gx/en/healthcare/emerging-trends-pwc-healthcare.jhtml>.
- Brinkman, W. P. (2009). Design of a questionnaire instrument. *Handbook of Mobile Technology Research Methods*, 31-57.

- Brooke, P. J. & Paige, R. F. (2003). Fault trees for security system design and analysis. *Computers & Security*, 23(3), 256 - 264.
- Brown, J. D. (2002). The Cronbach alpha reliability estimate. *JALT Testing & Evaluation SIG Newsletter*, 6(1), 17 - 18.
- Burrell, G., & Morgan, G. (1979). Sociological paradigms and organisational analysis. (Vol. 248). London: Heinemann.
- Cannon, D. L. (2011). *CISA Certified Information Systems : Study Guide*. Wiley.
- CAQ. (2014). *Professional judgment resource*. 1155 F Street NW Suite 450 Washington, DC 20004: Center for Audit Quality. Retrieved from [www.thecaq.org](http://www.thecaq.org).
- Case-Hospital. (2014). *Patient care*. Retrieved on October 15<sup>th</sup>, 2014, from <http://casemedcare.org/patient-care/>.
- Chan, H., Perrig, A. & Song, D. (2003). Random key predistribution schemes for sensor networks. *Proceedings of the 2003 IEEE Symposium on Security and Privacy* (p. 197). Washington, DC, USA: IEEE Computer Society.
- ChipCon. (2014). *Chipcon*. Retrieved on November 10<sup>th</sup>, 2014, from <http://focus.ti.com/docs/prod/folders/print/cc2420.html>.
- Cohen, L., Manion, L. & Morrison, K. (2007). *Research methods in education 6th edition*. London: Routledge.
- Cornish, F. & Gillespie, A. (2009). A Pragmatist approach to the problem of knowledge in health psychology. *Journal of Health Psychology*, 14(6), 800–809.
- Dalal, S., Beunza, J. J., Volmink, J., Adebamowo, C., Bajunirwe, F., Njelekela, M. & Holmes, M. D. (2011). Non-communicable diseases in sub-Saharan Africa: what we know now. *International Journal of epidemiology*, 40(4), 885-901.
- Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information. *MIS Quarterly*, 13(3), 319-340.
- De Vreede, G. J. & Briggs, R. O. (2005). Collaboration engineering: designing Repeatable processes for high-value collaborative tasks. *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS'03)*. pp 17c.
- Debreu, G. (1972). Theory of value: an axiomatic analysis of economic equilibrium. Cowles Foundation - Yale University.
- Dolev, D. & Yoa, A. C. (1981). On the security of public key protocols. *In Proceedings, the 22nd IEEE Annual Symposium on Foundation of Computer Science*, 350-357.
- Endsley, M. R. (1988). Situation Awareness Global Assessment Technique (SAGAT). *National Aerospace and Electronics conference* (pp. 789-795). IEEE.
- Eyler, R. (2005). Brand damage valuation: theory and practice. *International Journal of Wine Marketing*, 17(2), 21-29.
- Ezell, B., Farr, J. & Wiese, I. (2000). Infrastructure risk analysis model. *Journal of Infrastructure Systems*, 114-117.
- Fay, J. (2007). *Encyclopedia of Security Management* (Second ed.). Elsevier Inc.

- Feller, W. (2008). *An introduction to probability theory and its applications* (Vol. 2). John Wiley & Sons.
- Field, A. P. (2005). *Discovering statistics using SPSS*. London: Sage.
- Flowers, P. (2009). Research philosophies-importance and relevance. *M.Sc. Thesis*. Cranfield University.
- Gao Pesto, T., Selavo, C., Yin Chen, L., Jeong Gil, K., Hyun Lim, J. & Welsh, M. (2008). Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results. *008 IEEE Conference on Technologies for Homeland Security*, (pp. 187-192). Waltham, MA.
- Gavish, B. & Gerders, J. (1998). Anonymous mechanism in group decision support systems communication. *Decision Support Systems*, 28(4), 297-328.
- Gillon, R. (1994). Medical ethics: four principles plus attention to scope. *British Medical Journal*, 184(309).
- Goldkuhl, G. (2012). Pragmatism vs Interpretivism in qualitative information systems research. *European Journal of Information Systems*, 21(2), 135-146.
- Gonzalez, R. A. & Sol, H. G. (2012). Validation and design science research in information systems. research methodologies, innovations and philosophies in software systems engineering and information systems. *IGI Global*, 403-426.
- Guba, E. G. & Lincoln, Y. (1994). Competing paradigms in qualitative research. In Denzin, N. K. and Lincoln, Y. S. (eds), *Handbook of Qualitative Research* (pp. 105-17). Thousand Oaks, CA: Sage.
- Habinka, A. D. B. (2012). A decision enhancement studio for starting a miners enterprise in Uganda. *PhD Thesis*. Groningen, The Netherlands: University of Groningen.
- Den Hengst, M. & De Vreede, G. (2004). Collaborative business engineering: a decade of lessons from the field. *Journal of Management Information System*, 20(4), 85-113.
- Hernandez, D. (2014). Big data healthcare: the pros and cons of remote patient monitoring. MedCity News. Retrieved on April 5<sup>th</sup>, 2014, from <http://medcitynews.com/2014/03/big-data-healthcare-pros-cons-remote-patient-monitoring/>.
- Herrick, D. M., Linda, G. & Goodman, J. C. (2010). *Health information technology: benefits and problems*. Washington: National Center for Policy Analysis. Retrieved on December 2<sup>nd</sup>, 2011, from <http://www.ncpa.org/pdfs/st327.pdf>.
- Hevner, A. (2007). The three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2), 87-92.
- Hevner, A. & Chatterjee, S. (2010). *Design research in information systems: theory and practice*. Springer Science & Business Media.
- Hevner, A., March, S., Park, J. & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 8(1), 75-105.
- Hickam, H., Jessica, W. W., Jeanne-Marie, G., Buckley, D., Makalapua, M. & Somnath, S. (2013). Outpatient case management for adults with medical illnesses and complex

- care needs. *13-EHC031-EF(99)*. 540 Gaither Road, Rockville, MD 20850: U.S. Department of Health and Human Services.
- HIPAA. (2014). *Health Insurance Portability and Accountability Act (HIPAA)-1996*. Retrieved on August 25<sup>th</sup>, 2014 from <http://www.hipaa.org/>
- Hirschheim, R. (1992). Information systems epistemology: an historical perspective. *Information Systems Research: Issues, Methods and Practical Guidelines* (pp. 9-33). Henley-on-Thames: Alfred Waller Ltd.
- Hoffer, J., George, J. & Valacich, J. (2008). *Modern Systems Analysis and Design* (4th ed.). Prentice hall.
- Hookway, C. (2012). *The pragmatic maxim: essays on peirce and pragmatism*. Oxford : Oxford University Press.
- Houlding, D., Casey, T. & Rosenquis, M. (2012). *Improving healthcare risk assessments to maximize security budgets*. Intel Corporation.
- Hyla, T., El Fray, I., Maćków, W. & Pejaś, J. (2012). Long-term preservation of digital signatures for multiple groups of related documents. *IET Information Security*, 6(3), 219-227(8).
- ISO27002. (2015). *Introduction to ISO 27002 Standard*. Retrieved Jan 2015, from <http://www.27000.org/index.htm>.
- Jin, S. C., & Meng-Chu, Z. H. (2010). Recent advances in wireless sensor networks for health monitoring. *International Journal of Intelligent Control and Systems*, 15(4), 49-58.
- Jong-wook, L. (2013). Global health improvement and WHO: shaping the future. *The Lancet*, 362(9401), 2083-2088.
- Kambourakis, G., Klaoudatou, E. & Gritzalis, S. (2007). Securing medical sensor environments: The CodeBlue Framework Case. *Second International Conference on Availability, Reliability and Security (ARES'07)*.
- Karen, D. & Prokesch, S. (2013). Mega trends in global health care. *Harvard Business Review*. Retrieved from <http://hbr.org/web/extras/insight-center/health-care/globaltrends/1-slide>.
- Kartsakli, E., Antonopoulos, A., Tennina, S., Lalos, A., Mekikis, P. & Alonso, L. (2013). Enhancing quality of life with wireless sensor technology. Newsletter: IEEE Life Sciences.
- Keen, J. M. (2011). *Making technology investments profitable: ROI road map from business case to value realization* (2 ed.). New Jersey: John Wiley & Sons.
- Keen, P. G. & Sol, H. G. (2008). Decision enhancement services – rehearsing the future for decisions that matter. Amsterdam: IOS Press.
- Keller, K. L. (1998). *Strategic brand management: building, measuring, and managing brand equity*. New Jersey: Prentice Hall.
- Keller, K. L. (2003). Brand synthesis: the multidimensionality of brand knowledge . *Journal of Consumer Research* , 29.

- Keller, K. L., Parameswaran, M. G. & Jacob, I. (2011). *Strategic brand management: building, measuring, and managing brand equity*. Pearson Education India.
- Kilpinen, E. (2008). Pragmatism as a philosophy of action. *First Nordic Pragmatism Conference*. Helsinki, Finland.
- Kinfu, Y., Dal Poz, M. R., Mercer, H. & Evans, D. B. (2009). The Health worker shortage in Africa: are enough physicians and nurses being trained? *Bulletin of the World Health Organization*, 87(3), 225-230.
- Kirch, D., Henderson, M. & Dill, M. J. (2012). Physician workforce projections in an era of healthcare reform. *Annual Review of Medicine*, 63, 435-445.
- Klein, H. & Myers, M. (1999). A set of principles for conducting and evaluating interpretive field studies. *MIS Quarterly*, 23(1), 67-93.
- Knol, A. J. (2013). Decision enhancement for sourcing & sharing in the Dutch government . *PhD Thesis*. Groningen, The Netherlands : University of Groningen.
- Konde-Lule, J., Gitta, S., Okuonzi, S. & Matsiko, C. W. (2007). Access to healthcare in rural Uganda. iHEA 2007 6th World Congress: Explorations in Health Economics Paper.
- Kordy, B., Mauw, S., Radomirović, S. & Schweitzer, P. (2011). Foundations of Attack–Defense Trees. In P. A. Degano (Ed.), *Formal Aspects of Security and Trust*. pp. 80-95. Springer Berlin Heidelberg.
- Kumar, P. & Lee, H. (2011). Security issues in healthcare applications using wireless medical sensor networks: A Survey. *Sensors*, 12(1), 55-91.
- Kurt, J. (1994). An introduction to the theoretical aspects of coloured Petri Nets. *A Decade of Concurrency, Lecture Notes in Computer Science*, 230-272.
- Kutegeka, K. W. (2014). *ClinicMaster software features*. Retrieved from [www.clinicmaster.net](http://www.clinicmaster.net).
- Kwo-Shing, H., Yen-Ping, C., Chao, L. R. & Jih-Hsing, T. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243-248.
- Lanzi, A., Balzarotti, D., Kruegel, C., Christodorescu, M. & Kirda, E. (2010). Access miner: Using system-centric models for malware protection. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 399-412.
- Levy, Y. & Ellis, T. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, 9, 181-212.
- Lewis, J. P. (2005). *Project planning, scheduling and control*, 4E. McGraw-Hill Pub. Co.
- Lukwago, D. (2010). *The tragedy of Uganda's healthcare system: The ase of Paminya Health Center III, Nebbi District*. Kampala: Advocates Coalition for Development and Environment (ACODE). Retrieved on June 10<sup>th</sup>, 2013, from [http://www.acode-u.org/documents/infosheet\\_9.pdf](http://www.acode-u.org/documents/infosheet_9.pdf).
- Mack, L. (2010). The philosophical underpinnings of educational research. *Polyglossia*, 19, 5-11.



- Maher, D., Sekajugo, J., Harries, A. D. & Grosskurth, H. (2010). Research needs for an improved primary care response to chronic non-communicable diseases in Africa. *Tropical Medicine & International Health*, 15(2), 176-181.
- Maisel, W. H. & Kohno, T. (2010). Improving the security and privacy of implantable medical devices. *New England Journal of Medicine*, 362, 1164-1166.
- Maseruka, J. (2010). Uganda has only 2,000 doctors. Kampala, Uganda: The New Vision. Retrieved November 2014, from <http://www.newvision.co.ug/D/8/13/717871>.
- McDermott, J. (2001). Attack net penetration testing. *Proceedings of the 2000 workshop on New Security Paradigms*, 15-21.
- Meingast, M., Roosta, T. & Sastry, S. (2006). Security and privacy issues with healthcare information technology. *Proceedings of the 28th IEEE EMBS Annual International Conference*, 5453-5458.
- Mengo-Hospital. (2014). *Mengo Background*. Retrieved from <http://mengohospital.org/the-hospital/background/>.
- Mirembe, D. P. & Muyeba, M. (2008). Threat modelling revisited: improving expressiveness of attack net. *In the Proceedings of the 2nd UK European Modelling Symposium (Sept 8-10)*, 93-98.
- Mirembe, D. P. & Muyeba, M. (2009). Security issues in ambulatory wireless sensor networks (AWSN): Security Vs Mobility. *CCIR'09: Proc. of the 5th Annual International Conference on Computing and ICT Research*, 289-301.
- MobiHealth. (2014). *Innovative Mobile Service Application in Health care*. Retrieved from <http://www.mobihealth.org>.
- Mockel, C. & Abdallah, A. (2010). Threat modeling approaches and tools for securing architectural designs of an e-banking application. *Sixth International Conference on Information Assurance and Security (IAS)*, 149-154.
- MoH. (2010). Uganda clinical guidelines 2010, national guidelines on management of common conditions. *UCG 2010*. Kampala, Uganda: Ministry of Health, Uganda.
- Moshaddique, A. A. & Kyung-sup, K. (2011). Social issues in wireless sensor networks with healthcare perspective. *The International Arab Journal of Information Technology*, 8(1), 52-59.
- Mugenda, O. & Mugenda, A. G. (1999). *Research methods: qualitative and quantitative approaches*. Nairobi: ACTS Publishers .
- Muniafu, S. M. (2007). Developing ICT-enabled services in transition countries: a studio-based approach for logistics brokering. *PhD Thesis* . Delft: Delft University of Technology.
- MyAppSecurity (2012). 3 Approaches to Threat Modeling. Retrieved July 17th, 2015, from <http://myappsecurity.com/approaches-to-threat-modeling/>.
- Nielson, J. & Mark, R. L. (1994). *Usability inspection methods*. New York: John Wiley.

- NIST. (2012). Guide for conducting risk assessments. *NIST Special Publication 800-30*. United States of America. Retrieved November 2014, from [http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\\_30\\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf).
- Oladimeji, E., Supakkul, S. & Chung, L. (2006). Security threat modeling and analysis: a goal-oriented approach. *In Proc. of the 10th IASTED International Conference on Software Engineering and Applications (SEA 2006)*, 13-15.
- Ongtang, M., McLaughlin, S., Enck, W. & McDaniel, P. (2012). Semantically rich application-centric security in Android. *Security and Communication Networks*, 5(6), 658--673.
- Orlikowski, W. & Baroudi, J. (1991). Studying information technology in organizations: research approaches and assumptions. *Information Systems Research*, 2(1), 1-8.
- OWASP. (2014). *Threat risk modeling*. Retrieved on September 2<sup>nd</sup>, 2014, from [http://www.owasp.org/index.php/Threat\\_Risk\\_Modeling](http://www.owasp.org/index.php/Threat_Risk_Modeling).
- OWASP-RRM. (2014). *OWASP risk rating methodology*. Retrieved September 26, 2014, from [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology).
- Pacific Health Information Network. (2011). Health Information Systems (HIS). Retrieved on November 12, 2014, from <http://phinnetwork.org/Resources/HIS.aspx>.
- Pardue, J. H. & Patidar, P. (2011). Threats to healthcare data: a threat tree for risk assessment. *Issues in Information Systems*, 12(1), 106-113.
- Paté-Cornell, M. E. (1984). Fault trees vs event trees in reliability analysis. *Risk Analysis*, 4(3), 177-186.
- Pendergrass, J. C., Heart, K., Ranganathan, C. & Venkatakrishnan, V. (2013). A threat table based approach to telemedicine security. *Transactions of the International Conference on Health Information Technology Advancement*, 104-111.
- Pfleeger, C. & Pfleeger, S. (2003). *Security in computing* (Third ed.). Prentice Hall.
- Phillips, C. & Laura, P. (1998). A graph-based system for network-vulnerability analysis. *NSPW '98: Proceedings of the 1998 workshop on New security paradigms*, 71-79.
- Phillips, R. A. (2004). The design dimensions of e-learning. *In Proceedings of the 20th Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education*. Perth: Australasian Society for Computers in Learning in Tertiary Education. 781-790.
- Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S. & Carey, T. (1994). *Human-computer interaction*. New York: Addison Wesley Publishing Company.
- PTA Technologies. (2014, November 26). *The PTA threat analysis and risk assesment process*. Retrieved on September 15<sup>th</sup>, 2014, from <http://www.ptatechnologies.com/PTA3.htm>
- Rahman, F. F. (2005). Keys issues of remote patient monitoring. Frost & Sullivan. Retrieved on September 15<sup>th</sup>, 2014, from <http://www.frost.com/sublib/display-market-insight.do?id=31225662>



- Republic of Uganda. (2011). *National information security strategy*. Kampala: Republic of Uganda.
- Rorty, R. (1999). *Philosophy and social hope*. London: Penguin.
- Rossi, P. H., Lipsey, M. W. & Freeman, H. E. (2004). *Evaluation: a systematic approach* (7th ed.). Thousand Oaks: Sage.
- Ruiz, G., Heymann, E., César, E. & Miller, B. P. (2012). Automating threat modeling through the software development life-cycle. *XXIII Jornadas de Paralelismo*. Paper92
- Rumbaugh, J., Jacobson, I. & Booch, G. (2005). *The unified modelling language reference manual*. Boston: Addison-Wesley.
- Saitta, P., Larcom, B. & Eddington, M. (2005). Trike v.1 Methodology Document [Draft]. Retrieved Feb 2014, from [http://www.net-security.org/dl/articles/Trike\\_v1\\_Methodology\\_Document-draft.pdf](http://www.net-security.org/dl/articles/Trike_v1_Methodology_Document-draft.pdf)
- Saitta, S., Kripakaran, P., R. B. & Smith, I. (2010). Feature selection using stochastic search: an application to system identification. *Journal of Computing in Civil Engineering*, 24(1), 3-10.
- Samy, G. N., Ahmad, R. & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, 16(3), 201-209.
- Saunders, J. (2007). A dynamic risk model for information technology security in a critical infrastructure environment. Retrieved on April 10<sup>th</sup>, 2012, from [www.johnsaunders.com/papers/riskcip/riskconference.htm](http://www.johnsaunders.com/papers/riskcip/riskconference.htm)
- Sauro, J. & Lewis, J. (2011). When designing usability questionnaires, does it hurt to be positive? *Proceedings of the International Conference on Human Factors in Computing Systems (CHI)*, 2215-2224.
- Scandariato, R., Wuyts, K. & Joosen, W. (2013). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, 1-18.
- Schneider, H., Blaauw, D., Gilson, L., Chabikuli, N. & Goudge, J. (2006). Health systems and access to antiretroviral drugs for HIV in Southern Africa: Service Delivery and Human Resources Challenges. *Reproductive Health Matters*, 14(27), 12-23.
- Schneier, B. (1999). Modeling security threats: Attack Trees. *Dr. Dobbs's Journal*, 1-9.
- Schneier, B. (2000). *Secrets and lies: Digital Security in a Networked World*. Wiley.
- Sekaran, U. (2003). *Research methods for business* (4th ed.). Hoboken, NJ: John Wiley & Sons.
- Sharon, S., Jennifer, N. E. & Diana, R. (2012). Sensor networks for medical care using electronic health records to improve quality and efficiency: The experiences of leading hospitals. *17*(1608).
- Shawn, H., Scott, L., Tomasz, O. & Adam, S. (2006). Uncover security design flaws using the STRIDE approach. MSDN Magazine: Microsoft Inc.

- Shnayder, V., Chen, B., Lorincz, K., Fulford Jones, T. & Welsh, M. (2005). *Sensor networks for medical care*. Division of Engineering and Applied Sciences: Harvard University.
- Shostack, A. (2008). Experiences threat modeling at Microsoft. *Modeling Security Workshop*. Dept. of Computing, Lancaster University, UK.
- Sim, S. & Gallardo-Valencia, R. (2013). *Finding source code on the web for remix and reuse*. Springer.
- Sjouke, M. & Oostdijk, M. (2006). Foundations of attack trees. *8th Annual International Conference on Information Security and Cryptology (ICISC'05)*, 186-198.
- Smith, K. (2006). Simplifying ajax-style web development. *Computer*, 39(5), 98-101.
- Smith, M. J. (1998). *Social Science in Question*. London: Sage.
- Sol, H. G. (1982). Simulation in information systems development. *PhD Thesis*. University of Groningen.
- Sol, H. G. (1988). Information systems development: a problem solving approach. *Proceedings of the Symposium and Systems Analysis and Design*. Atlanta.
- Stallings, W. (2003). *Network security essentials, applications and standards* (Second ed.). Pearson Hall.
- Steffan, J. & Schumacher, M. (2002). Collaborative attack modeling. *SAC '02: Proceedings of the 2002 ACM Symposium on Applied Computing*, 253-259.
- Tachakra, S., Wang, X., Robert, S. & Song, Y. (2003). Mobile e-health: the unwired evolution of telemedicine. *Telemedicine Journal and E-Health*, 9(3).
- Tongco, M. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research & Applications*(5), 147-158.
- Totten, M. A., Jesse, W., Makalapua, M., Hickam, D. & Jeanne, M. G. (2013). Outpatient case management for adults with medical illnesses and complex care needs: future research needs. Oregon Evidence based Practice Center: U.S. Department of Health and Human Services.
- UN. (2004). World population to 2300. *Report*. New York: The Department of Economic and Social Affairs, United Nations.
- Undercoffer, J., Avancha, S., Joshi, A. & Pinkston, J. (2002). Security for sensor networks. Baltimore County, Baltimore, MD 21250: Dept of Computer Science and Electrical Engineering, University of Maryland.
- Vandenburg, M. (2008). Using Google maps as an interface for the library catalogue. 26(1), 33-40.
- Vargo, S. & Lusch, R. (2004). Evolving to a new dominant logic for marketing. *Journal of Marketing*, 68, 1-17.
- Vellani, K. H. (2006). Strategic hospital security: risk assessments in the environment of care. USA: Threat Analysis Group, LLC.

- Venable, J. (2006). The role of theory and theorising in design science research. *In Proceedings of the First International Conference on Design Science in Information Systems and Technology* (pp. 1-18). Claremont: Chatterjees and Hevner A, Eds.
- Vesely, W., Goldberg, F., Roberts, N. & Haasl, D. (1981). *Fault tree handbook*. Washington, DC 20555-0001: U.S. Nuclear Regulatory Commission.
- VMWARE. (2013). *How risk analysis streamlines decision making for major IT initiatives*. VMware, Inc. Retrieved on November 10, 2014, from <http://www.vmware.com/files/pdf/accelerate/vmware-how-risk-analysis-streamlines-decision-making-for-major-it-initiatives.pdf>
- Walsh, J. (2002). *Asset protection and security management handbook*. Taylor & Francis.
- Walsh, T. (2011). *Security risk analysis and management: an overview (Updated) AHIMA Practice Brief*. American Health Information Management Association.
- Walters, J., Liang, Z., Shi, W. & Chaudhary, V. (2006). Wireless sensor network security: a survey. *Security in Distributed, Grid and Pervasive Computing*, 17.
- Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J. & Fu, C. (2010). Cloud computing: a perspective study. *New Generation Computing*, 28(2), 137-146.
- Wang, Y. (2007). A studio based approach for business engineering and mobile services. *PhD thesis*. Delft: Delft University of Technology.
- Weisberg, H. F., Krosnick, J. A. & Bowen, B. D. (1989). *An introduction to survey research and data analysis* (2nd ed.). (F. Scott, Ed.) Glenview, IL.
- Westervelt, R. (2011). Developing IT risk management decision-making criteria an ongoing challenge. Retrieved on November 10<sup>th</sup>, 2014, from <http://searchsecurity.techtarget.com/news/1280099782/Developing-IT-risk-management-decision-making-criteria-an-ongoing-challenge>
- WHO. (2012). WHO global health expenditure Atlas. *Report*. 211 Geneva 27, Switzerland: WHO Press.
- WHO. (2013). World health statistics 2013. *Report*. Geneva, Switzerland: WHO Press.
- Widenius, M. & Axmark, D. (2002). *MySQL reference manual: Documentation from the Source*. O'Reilly Media, Inc.
- Xbow. (2014). *MICAz wireless system fact sheet*. Retrieved on September 15<sup>th</sup>, 2014, from <http://www.xbow.com/Products/productdetails.aspx?sid=174>
- Xiao-jun, Z., Wei, H. & Xu, O. (2006). The construction of the tourism website based on PHP+MYSQL. *Sci-Tech Information Development & Economy*, 23(142), 1-16.
- Yin, R. (2003). Case study research design and methods, applied social research methods. *Sage publications Internationals Educational and professional Publisher*, 5(1), 1-94.
- Zigbee-Alliance. (2014). *ZigBee Wireless Sensor Applications for Health, Wellness and Fitness*. Retrieved on October 5<sup>th</sup>, 2014, from <http://www.zigbee.org>

## Appendices

---

### Appendix 1: Exploratory Study Unstructured Interview Guide

This appendix presents the sample interview guide which was used to collect data of stage one during the exploratory phase.

#### **Research Question: How can threat analysis be enhanced?**

**Preamble:** This exploratory study seeks to understand the current threat analysis approaches employed by information security experts in identifying threats, determining their likelihood and their impact on hospitals. Furthermore, the study seeks to understand challenges security analysts face during the threat analysis process and desired features of an appropriate threat analysis approach. This research is conducted within the PhD research project entitled securing ambulatory wireless sensor networks at the University of Groningen, The Netherlands. The research is facilitated by Prof. dr. Henk G. Sol of the University of Groningen and Prof. dr. Jude Lubega of the Uganda Technology and Management University.

#### **Background information.**

1. Highest level of education
2. Professional Qualifications
3. Years of experience in information system security
4. Place of work

#### **Understanding threat analysis.**

1. Describe a typical threat analysis process?
2. Which approaches do you use to analyze threats?
3. Which key decisions threat analysts have to make?
4. What challenges do threat analysts face to make the important decisions?
5. In your opinion, how should threat analysis be undertaken?
6. What would be the characteristics of an ideal threat analysis approach?
7. How can a threat analysis approach be evaluated?
8. In your opinion, is threat analysis important when acquiring a healthcare information system? And why?
9. Generally, how can threat analysis be enhanced?

## Appendix 2: Exploratory Study Questionnaire

This appendix presents a copy of the survey questionnaire which was used to collect data from experts during the second stage of the exploratory student.

### Research Question: How can threat analysis be enhanced?

There is a slow adoption of healthcare information systems particularly, ambulatory wireless sensor technologies in healthcare service mainly due to perceived risks. Therefore, this exploratory study seeks to understand the current threat analysis approaches employed by information security experts in identifying threats, determining their likelihood and their impact on hospitals. Furthermore, the study seeks to understand challenges security analyst face during threat analysis process and desired features of an appropriate threat analysis approach. This research is conducted within the PhD research project entitled securing ambulatory wireless sensor networks at the University of Groningen, The Netherlands. The research is facilitated by Prof. dr. Henk G. Sol of the University of Groningen and Prof. dr. Jude Lubega of the Uganda Technology and Management University.

#### Background information.

1. Highest level of education .....
2. Professional qualifications .....
3. Years of experience in healthcare information system security .....
4. Place of work: ☐ Industry .... ☐ Acad ☐ a ☐ Both academia and industry

#### Understanding threat modelling.

1. Select one option that best describes a typical threat analysis process?
  - a. Security requirements > asset identification > threat identification > threat mitigation >
  - b. System characterization > asset identification > security requirements > vulnerability identification > threat identification > threat likelihood > threat impact analysis > mitigation definition > ROI
  - c. Security objectives > application overview > application decomposition > threat identification > vulnerability identification
  - d. Others: .....
2. For the option selected above in 1, would you like to provide more information to back up your selection?
3. What challenges do threat modelers face? **(Select all that apply)**
  - a. Lack of information on vulnerabilities and threat agents

- b. Lack of knowledge to analyze threats
  - c. Natural bias of the analyst
  - d. Inability to quantify threat business impact
  - e. Inability to logically estimate threat likelihood
  - f. Lack of a logical approach to incorporate background knowledge in the quantification of threats
  - g. Lack of collaboration among experts
  - h. Any other...
4. How should threat analysis be undertaken?
- a. Single IT security expert analysis
  - b. Collaborative approach among IT security experts in a focus group
  - c. Collaborative approach among IT security experts using collaborative tool
  - d. Collaborative approach between IT experts and business analyst in a focused group
  - e. Collaborative approach between IT experts, business analyst and other stakeholders using a collaboration tool
  - f. Others: .....
5. What are the key decisions threat analyst make and how can these decisions be enhanced?
6. What would be the characteristics of a good threat analysis approach? **(Select all that apply)**
- a. Must define all relevant sources of information
  - b. Provide a step by step guidelines on how to model threats
  - c. Provide a mechanism of computing threat likelihood
  - d. Provide a mechanism of computing threat impact
  - e. Enable collaboration among IT security experts, Business analyst and other Stakeholders
  - f. Enable aggregation of different expert computations and provide an average assessment
  - g. Provide recommendations on mitigation control and investment estimates

- h. Others .....
- 7. How can a threat analysis approach be evaluated?
  - a. Based on ease of use
  - b. Based on learnability
  - c. Usefulness in determination of likely threats and their impact
  - d. Consistency of the generated assessment results (reliability)
  - e. Others: .....
- 8. Kindly suggest any relevant threat analysis insights that might have not been captured in questions1-5 above

.....  
.....  
.....

Thank you for participating in this research

**Drake Patrick Mirembe (PhD Student, University of Groningen)**

Appendix 3: ThreNet Tool Description

To evaluate and support the Threat Nets Approach, a ThreNet tool was developed. In the following sections, ThreNet tool design, architecture, and functionalities are discussed. The tool is hosted on <http://8technologies.net/threnet>

ThreNet Tool Data Flow Diagrams

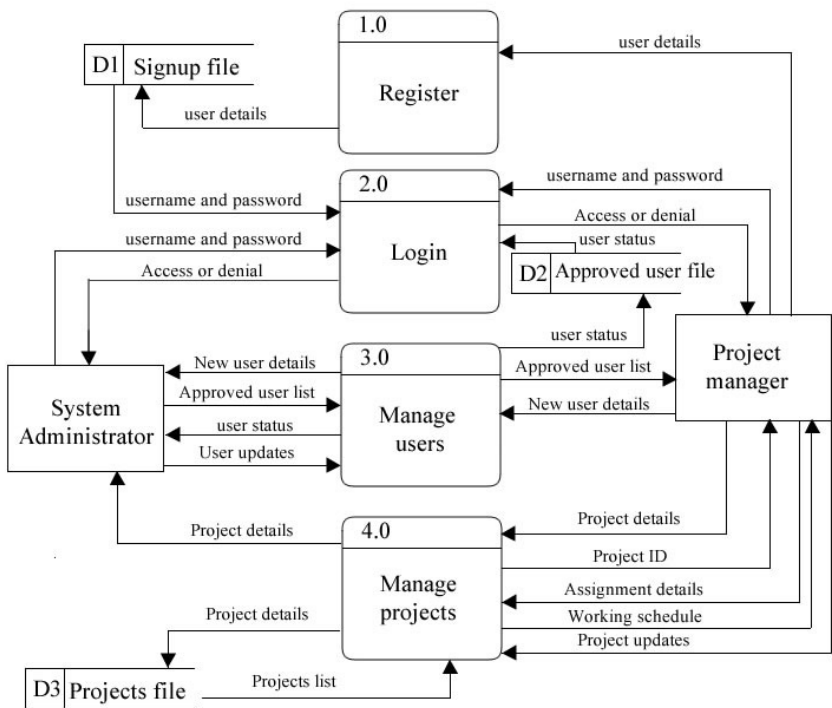


Figure A3-1: A Data Flow Diagram for Projects Management Module

Figure A3-1 illustrates the pattern of information flow under the projects management module. The module is designed to enhance management of threat analysis projects. The project manager signs up by inputting his user details which are stored in the sign up file. This information is later used to authenticate the user. During login, the project manager or administrator provide their usernames and passwords and in case of failure, an “access denied” notification is displayed on the login screen, otherwise the user is granted access to the system. When granted access, the administrator can create new users, edit profiles of existing users and approve user signup requests. Authenticated project managers can view a



list of the registered users and can assign users to projects. Besides assigning users to projects, a project manager can create and update project information.

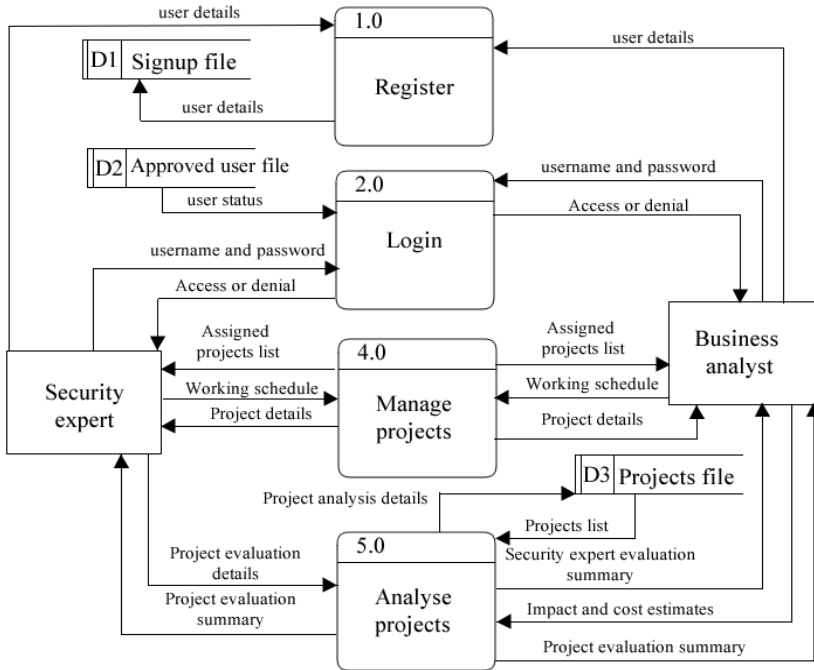


Figure A3-2: A Data Flow Diagram for Vulnerability and Threat Analysis

Figure A3-2 illustrates the interaction between ThreNet tool and the analysts (security experts and business analyst).

On registration, the security expert and business expert provide their user details to the system and they are stored in the sign up table. The stored information is later used to authenticate users. If approved by the administrator, the user (the security or business experts) appears in the approved table. During login, an approved user provides login details which are compared with those in the approved table. If the login details match, access to the system is granted, otherwise an “access denied” message is displayed on the login interface.

When the user is logged in, they can now analyze projects which have been assigned to them. The user will be able to view all the assigned projects, upload their work schedules and input their assessments into the system.

## Implementation Technologies and Considerations

The motivation to implement the ThreNet tool was to support the Threat Nets Approach. During the implementation, decisions on implementation technologies were made.

**Technology Platforms:** The decision was made to build the ThreNet tool based on open source technologies. The choice of open source technologies was inspired by the fact that open source technologies have a large community of developers' hence better support (Sim & Gallardo-Valencia, 2013). Accordingly, My Structured Query Language (MySQL) server was used to implement the ThreNet tool database because of its efficiency in record access and ease of use (Xiao-Jun, 2006; Widenius & Axmark, 2002). The ThreNet tool is designed to be easy to use, thus simplicity of user interfaces is critical to achieve that requirement. For that reason, Hyper Text Mark-up Language (HTML5), Asynchronous JavaScript, extensible Mark-up Language (AJAX) and PHP were used to develop the user interfaces. AJAX was used because it makes web servers more responsive to user inputs (Smith K. , 2006). AJAX allows partial processing of webpages, a critical feature in processing complex ThreNet tool pages (Vandenburg, 2008). JavaScript being a client-side scripting language was used to implement service requests and submissions between the web browser and the web server.

It is worth noting that the Threat Nets Approach is dynamic and allows analysts to update threat assessments on new evidence. In addition, the approach involves coordination among stakeholders. Accordingly, a client-server architecture was chosen to implement the ThreNet tool that is accessible from anywhere at any time. The client-server architecture coupled with web-based technologies make the ThreNet tool available to stakeholders on any internet enabled device. The flexibility of tool access allows security experts and business analysts to update their evaluations as they get new information. The server side of the ThreNet tool was hosted on the Google cloud service to increase the reliability and responsiveness (Wang, et al., 2010) .

## ThreNet Tool Functionality and Description

Hoffer et al. (2008) suggests that developers of studios and tools should provide sufficient documentation about their artifacts in order to facilitate user adoption. Therefore, functionalities of the ThreNet tool are described in this section. Figure A3-3 shows the landing page of the ThreNet tool, which offers introductory information about the Threat Nets Approach in general and ThreNet tool in particular under the link "About ThreNet". The interface provides a self-help user manual via the "Help" link on the bottom of the

page. Registered users can access the tool functionalities via the login interface and prospective users can register via a “Signup” link.



Figure A3-3: The ThreNet Tool Login Interface

## The Administrator Module

The administrator module provides interfaces for the ThreNet tool administrator to manage users. Using the interfaces the administrator can add new users, edit user profiles, assign privileges and revoke user rights. Figure A3-4 illustrates the layout of the interface.

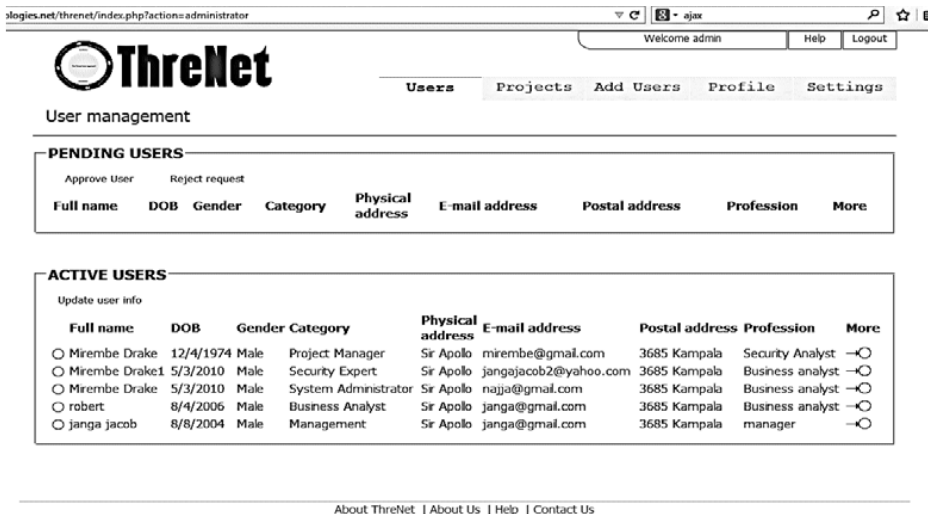


Figure A3-4: The ThreNet Tool Administrator Interfaces

The Project Manager Module

The module provides interfaces for the project manager to create and edit projects. Using the “New Project” interface the project manager uploads all relevant documents about the project and provides background information like project objectives and scope. Each project is created with a unique project ID used to track the project. Using the “Assign Users” link, the project manager assigns analysts (security experts and business analysts) to the project. Using the “Projects” link, the project manager can update existing projects. The project manager interfaces also provides guidelines of how the project should be created. Figure A3-5 shows the layout of the project manager interface. The category field in Figure A3-5 is user defined and describes the nature of the project. For example, if the threat analysis project is focusing on risk analysis for the network, then the category is set to networking.

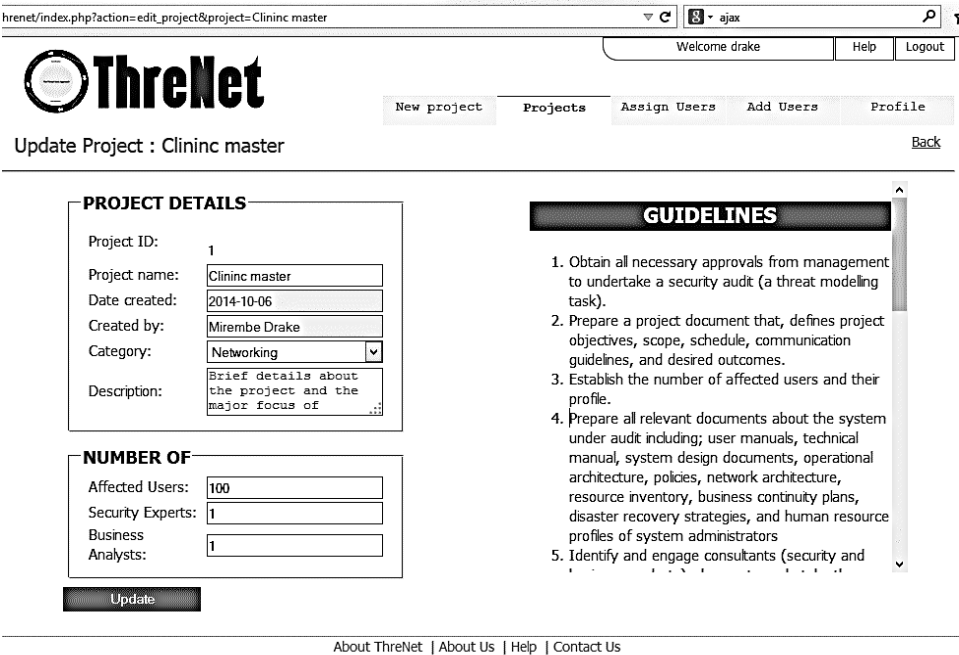


Figure A3-5: Project Creation Interface

Security Expert Module

The security expert module provides interfaces and functionalities to facilitate the vulnerability and threat analysis activities. Using interfaces provided, the security expert identifies system vulnerabilities and threats. The module is basically divided into four major

sections: the system decomposition, vulnerability identification, threat analysis, and mitigation control. The interfaces of the system decomposition allows security experts to identify various system features and evaluate their completeness. From completeness scores likelihood of vulnerabilities can be estimated. From each system feature, assets that need protection are identified and their associated vulnerabilities established. Subsequently, the security expert defines security requirements that are necessary to address the identified vulnerabilities using the security requirement user interface. Then, the tool automatically generates a threat goal (Threat), which is the combination of asset, vulnerability and security requirement. That is to say, an objective an attacker must achieve to breach the security of a given asset. Figure A3-6 illustrates features of the main interface. Using interfaces via the mitigation control link, the security expert defines appropriate threat mitigation controls.

The screenshot displays the ThreNet web application interface. At the top, the URL is `www.8technologies.net/threnet/form22.php?name=Case%20Hospital`. Below the header, there's a navigation bar with tabs: Project Selection, System Description, Asset Identification, Vulnerability Identification, Security Requirements, Threat Analysis, and Mitigation Controls. The current step is "Step 1 of 6: Case Hospital".

The main content area is divided into two columns. The left column contains a "Projects" dropdown menu with "Case Hospital" selected. Below it, the "Project Details" section lists:
 

- Project Identifier : 1
- Date of Initiation : 2014-12-27
- Category of Information System : Enterprise
- Description : Determine all possible threat to ClinicMaster Enterprise system, asses the likelihood of threats and establish their impact on the operation of the hospital. Furthermore, recommend cost-effective threat mitigation controls.
- Attachments : 1.Clinic\_Master\_Brochure.docx

The right column features a "System Description Guidelines" box with two numbered instructions:
 

1. Decompose the system into constituent features like; governance, software, data, network, hardware, and human resources
2. From each feature identify all assets that need protection

Below these sections, there are three tabs for assessment: "Software assessment", "Governance assessment", and "Human resource assessment". The "Software assessment" tab is active, showing a Likert scale for "Completeness of the IT security policy" with radio buttons for 1, 2, 3, 4, and 5. The "Human resource assessment" tab is also visible, showing a Likert scale for "Completeness of the human physical and environmental security" with radio buttons for 1, 2, 3, 4, and 5.

Figure A3-6: The Security Expert Main Interface

Under the system decomposition link in Figure A3-6, the security expert assess the completeness of each system feature on the Likert scale. Figure A3-7 shows interface used to assess the completeness of system features.

es.net/threNet/form22.php?name=Clininc master

ajax

GovernanceHuman ResourceSoftwareHardware

End Users

Years of system use

☐ 0-1☐ 2-4☐ 5-7☐ 8-10☐ 11 Above

Have had training about the information system in the past

☐ Yes☒ No

Level of ICT training

☐ Basic☒ Novice☐ Intermediate☐ Advanced☐ Expert

Awareness of policies

☐ Yes☒ No

Level of competence in using the information system

☐ Novice☒ Entry☐ Associate☐ Professional☐ Expert

Level of training in using the information system

☐ Basic☐ Novice☒ Intermediate☐ Advanced☐ Expert

Level of ICT security awareness training

☐ Basic☐ Novice☒ Intermediate☐ Advanced☐ Expert

Save

IT Administrators

Not Applicable☐

Experience

☒ 0-1☐ 2-4☐ 5-7☐ 8-10☐ 11 above

Industrial Certification

☐ Novice☒ Entry☐ Associate☐ Professional☐ Expert

Level of competence in using the information system

☐ Novice☒ Entry☐ Associate☐ Professional☐ Expert

Continuous capacity building

☐ Never☒ Rare☐ Occasionally☐ Frequent☐ Very frequently

Terms of employment

☐ Onsecondment☐ Intern☒ Part-time☐ Consultant☐ Full-time

Save

continue

About ThreNet | About Us | Help | Contact Us

Figure A3-7: Interface for Assessing Completeness of System Features

For each threat identified, a security expert decomposes the threat into sub-goals, resulting into the construction of a threat tree. A threat tree is a structure that illustrates the different threat propagation pathways (Figure A3-8). Using likelihood of vulnerability discoverability and exploitability, the expert computes the threat likelihood. Figure A3-8 shows the interface used to construct the threat tree.

From the exploratory phase, it was observed that deeper threat trees don’t necessary add value on the likelihood of threats. The line of reasoning is supported by Sjouke and Oostdijk (2006), who observed that deeper attacker pathways implicitly indicate low likelihood of threat occurrence. Thus, the ThreNet tool generates threat trees to a maximum depth of 3 refinement levels. Three refinement levels are deemed optimal to convey all the relevant information about threat propagation pathways.

# The Threat Nets Approach to Information System Security Risk Analysis

Project Management   System Description   Asset Identification   Vulnerability Identification   Security Requirements   Threat Analysis   Mitigation Controls

Step 5 of 6: Mengo Hospital

Threat Assessment

Select a Threat: Threat5

Threat Details

<b>Assets</b>	Patient data
<b>Vulnerability</b>	Unintended disclosure
<b>Threat agent</b>	Disgruntled employee
<b>Security Requirement</b>	preserve patient data confidentiality

Threat is likely to occur through blackmail a nurse

Level 1

blackmail doctor ☐

Vulnerability discovery ▼

Threat Agent profile ▼

Possibility of Attack ▼

0.352

☐ AND

☐ OR

blackmail system administrator ☐

Vulnerability discovery ▼

Threat Agent profile ▼

Possibility of Attack ▼

0.352

☐ AND

☐ OR

blackmail a nurse ☐

Vulnerability discovery ▼

Threat Agent profile ▼

Possibility of Attack ▼

0.488

local Disk (D:)   New Phd   Downloads   Step 5 - Google C...   PhD\_Thesis\_Drak...   PhD\_Thesis\_Drak...   Computation mo...

Figure A3-8: Threat Decomposition

## Business Analyst Module

The business analyst module is accessible via the login page when a user logs in with business analyst privileges.

**Threat agent**

disgruntled worker

**Security Requirement**

minimize unauthorized accessed to patient data

Attachments:

Impact Computation

Lost Productivity

User Category	Number of affected users	Lost time(Hrs)	Hourly losses(USD)	Sub-total
Doctors	10	4	36	1440
Nurses	30	4	2	240
Lab Technicians	8	2	10	160
Accountants	4	2	5	40
Pharmacists	4	4	300	4800

Save

Cost of Recovery

Assets type	Number of assets	Unit cost	Sub-total
Data	0	0	0
Servers	0	0	0
Software	1	3000	3000
Network	0	0	0
People	0	0	0

Save

Brand damage estimate

Lost market share: 0.1

Customer loyalty: 0.1

Estimated Income for brand value 75000 USD

**Brand Index Damage:** 10

Save

Results

Lost productivity: 6680

Total cost of recovery: 3000

Brand damage: 7500

Total business impact: 17180

Refresh

Figure A3-9: Threat Business Impact Interface



The business analyst interface offers access to all projects the analyst has been assigned. From the landing page, the business analyst can update projects under the pending projects link by selecting a given project. View the threats and the associated mitigation controls. Using the impact section of the interface, the business analyst inputs the estimates of brand damage index, lost productivity time, estimated brand value, cost of recovery and hourly rates. Thereafter, computes the threat business impact (Figure A3-9). In Figure A3-9 the total business impact is USD17, 180 meaning the business will lose that much in terms of lost productivity, brand value and cost of recovery from a given threat.

Manager’s Module

The manager’s module provides interfaces where decision makers in an organization can view the project status, threats, proposed mitigation controls and threat impact. Using data from the business analyst module, managers can explore the “what if scenarios” on Return on Investment (ROI). Figure A3-10 illustrates the interface managers use to evaluate the ROI.

es.net/thretnet/index.php?action=manage3&name=Threat1

ajax

PROJECT DETAILS

Project ID:  
Date created:  
Category:  
Description:  
Attachments:

each set of mitigation control using equation 4.5.  
3. Determine allocation budget and funds release  
schedule

Threat Analysis

Assets	Vulnerability	Security Requirement	mitigation control(s)	Type	Select
data	Stolen by members	not stolen	cane them	Not Complementary	<input type="radio"/>
data	Stolen by members	not stolen	protect it	Not Complementary	<input type="radio"/>
data	Stolen by members	not stolen	use passwords	Not Complementary	<input type="radio"/>
data	Stolen by members	has to be protected			<input type="radio"/>

Compute

ROI computation

Likelihood

Affected users

Business Impact

Mitigation Cost

Return on Investment

%

24200104

Figure A3-10: Interface for Computing ROI



## **Appendix 4: Threat Nets Approach Evaluation Questionnaire for Security Experts**

This appendix presents a copy of the evaluation questionnaire that was used to collect data from security experts during the evaluation of the Threat Nets Approach.

### **Threat Nets Approach Evaluation Questionnaire for Security Experts**

From our exploratory work, it was observed that security analysts faces a number of challenges when modelling threats to information system. Some of the challenges include, lack of information, natural bias of analyst, inability to logically link existence of vulnerabilities to threats, lack of collaboration among stakeholders and inability to measure the threat impact in a pragmatic way. Therefore, the Threat Nets Approach and tool was developed to address the aforementioned. Therefore, this evaluation exercise seeks to gauge Threat Nets Approach completeness, usability and usefulness. As one of the key stakeholders, we are seeking your opinion on the completeness, usability and usefulness of the approach at enhancing threat analysis challenges stated above. This research is conducted within the PhD research project titled securing ambulatory wireless sensor networks at the University of Groningen, The Netherlands. The research is facilitated by Prof. dr. Henk G. Sol of the University of Groningen and Prof. dr. Jude Lubega of the Uganda Technology and Management University.

#### **Background information.**

1. Highest level of education .....
2. Professional qualifications .....
3. Industry: Business analyst ☐ IT security expert ☐
4. Field experience .....
5. Place of work: ☐ Industry . ☐ Academia ☐ Both academia and industry

**Threat Nets Approach Completeness, Usability and usefulness evaluation**

	<b>Evaluation statement</b>	<b>Strongly disagree (1)</b>	<b>Disagree (2)</b>	<b>Neutral (3)</b>	<b>Agree (4)</b>	<b>Strongly agree (5)</b>
	<b>Completeness</b>					
1	The approach captures all relevant information					
2	The guidelines provided are complete					
3	The processes are correctly described					
	<b>Usability</b>					
1	The approach is easy to learn					
2	Guidelines are clear					
3	Guidelines are simple to interpret					
4	Process sequences are logical					
5	The approach is easy to apply in the analysis of threats					

	<b>Usefulness</b>					
1	Vulnerability process helps the expert to easily identify sources of information					
2	System decomposition makes it easy to identify hidden vulnerabilities					
3	Guidelines are useful in identifying all possible threat goals					
4	The approach is helpful in linking system features to the likely existence of vulnerabilities					
5	The approach is helpful in linking vulnerability to threat likelihood					
6	The approach is useful in determining all possible threats					
7	The approach improves collaboration among stakeholders					
8	The approach enhance the threat analysis process					
9	The approach can be used on all threat analysis scenarios					
10	The approach improves the efficiency of the threat analysts					
11	The approach addresses all core threat analysis processes					
12	The approach does address the key challenges in the industry					
13	I can recommend this approach to other experts					

**Additional Information**

## The Threat Nets Approach to Information System Security Risk Analysis

Kindly share any observations and recommends that you think can improve the Threat Nets Approach

.....  
.....

We thank you very much for your contributions.

**Drake Patrick Mirembe (PhD Student, University of Groningen)**

**Appendix 5: Threat Nets Approach Evaluation Questionnaire for Business Analysts**

This appendix presents the evaluation questionnaire that was used by the business analysts to assess the approach.

**Threat Nets Approach Evaluation Questionnaire for Business Analysts**

From our exploratory work, it was observed that security analysts faces a number of challenges when modelling threats to information system. Some of the challenges include, lack of information, natural bias of analyst, inability to logically link existence of vulnerabilities to threats, lack of collaboration among stakeholders and inability to measure the threat impact in a pragmatic way. Therefore, the Threat Nets Approach and tool was developed to address the aforementioned. Therefore, this evaluation exercise seeks to gauge Threat Nets Approach completeness, usability and usefulness. As one of the key stakeholders, we are seeking your opinion on the completeness, usability and usefulness of the approach at enhancing threat analysis challenges stated above. This research is conducted within the PhD research project titled securing ambulatory wireless sensor networks at the University of Groningen, The Netherlands. The research is facilitated by Prof. dr. Henk G. Sol of the University of Groningen and Prof. dr. Jude Lubega of the Uganda Technology and Management University.

**Background information.**

- 1. Highest level of education .....
- 2. Professional qualifications .....
- 3. Industry: Business analyst ☐ IT security expert ☐
- 4. Field experience .....
- 5. Place of work: ☐ Industry . ☐ Academia ☐ Both academia and industry

**Threat Nets Approach Completeness, Usability and usefulness evaluation**

	Evaluation statement	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly agree (5)
	<b>Completeness</b>					
1	The approach captures all relevant information					
2	The guidelines provided are complete					
3	The processes are correctly described					
	<b>Usability</b>					
1	Guidelines to evaluate threat business impact are easy to learn					
2	The terminologies are consistent with those in the industry					
3	The guidelines are clear					
4	The guidelines are simple to interpret					
5	Process sequences are logical					

	<b>Usefulness</b>					
1	The guidelines are helpful in the quantification of threat business impact					
2	The scheme of for computing lost productivity is very helpful					
3	The scheme for computing cost of recovery is very helpful					
4	The brand index approach is very helpful in the evaluation of brand depreciation					
5	The scheme for evaluating threat business impact is very helpful					
6	The scheme for evaluating ROI is very helpful					
7	The coordination guidelines improves coordination among stakeholders					
8	The threat business impact can be used to assess impact of risks on organizations in other sectors					
9	The approach improves the efficiency of threat business impact quantification					
10	The threat business impact scheme addresses all core aspects of risk analysis					
11	The threat business impact scheme does address the key challenges in the industry					
12	I can recommend this approach to other business analysts					
13	The guidelines are helpful in the quantification of threat business impact					

**Additional Information**

Kindly share any observations and recommends that you think can improve the Threat Nets Approach

.....  
 .....

We thank you very much for your contributions.

## List of Acronyms

---

AAMC	Association of American Medical Colleges
BID	Brand Index Depreciation
CEO	Chief Executive Officer
CERT	Computer Emergence Response Teams
CHK	Case Hospital Kampala
CIL	ClinicMaster International Ltd
CISA	Certified Information Systems Auditor
CS	Completeness Score
GDSS	Group Decisions Support Systems
GUI	Graphical User Interface
HIS	Hospital Information System
HTML	Hyper Text Mark-Up Language
ICDL	International Computer Driving License
ICT	Information Communication Technology
IS	Information System
ISACA	Information Systems Audit and Control Association
ISM	Information Systems Manager
ISO	International Standards Organization
IT	Information Technology
ITM	Information Technology Manager
ITU	International Telecommunication Union
LP	Lost Productivity
MH	Mengo Hospital
MoH	Ministry of Health, Uganda
MySQL	My Structure Query Language
NCD	None-Communicable Diseases
OCMS	Outpatient Case Manager Scheme
PM	Project Manager
PPDA	Public Procurement and Disposal Act
PS	Personal Server
ROI	Return on Investment
RPMS	Ambulatory Wireless Sensor Networks
SART	Situation Aware Rating Technique
SLA	Service Level Agreement
SPSS	Statistical Package for Social Scientists
STRIDE	Spoofting, Tampering, Repudiation, Information Disclosure, Denial of service and Elevation of privileges

TBI	Threat Business Impact
ThreNet	the Threat Nets Approach
UML	Unified Modelling Language
UN	United Nations
UTAMU	Uganda Technology and Management University
WHO	World Health Organization

## Summary

---

Information management systems like Remote Patient Monitoring Systems (RPMS) provide capabilities of collecting, analyzing and disseminating vital patient data to healthcare service providers. The timely availability of reliable patient data enables healthcare service providers to deliver services to remote patients, hence; lowering cost of services, improving compliance to prescription, and improving monitoring of recovering patients. Clearly, healthcare information systems like RPMS have a potential to address the growing demand for healthcare services due to the increasing and aging world population. However, utilization of RPMS in such mission critical situations raises concerns about the impact of their failures on the patient and the hospital. Thus, identifying RPMS vulnerabilities, associated threats, evaluating threat likelihood and impact are crucial tasks in the RPMS adaption decision process. Furthermore, senior management in hospitals is always concerned with finding optimal investment options. In that regard, the assessment of the cost-effectiveness of information system threat mitigation strategies is key in the IT adaption decision process. It is evident that assessing threat likelihood, evaluating the threat business impact and determining a cost-effective threat mitigation strategy requires a pragmatic approach to guide the execution of the different activities.

Consequently, current information system threat analysis approaches were analyzed in order to determine existing gaps, establish requirements of an ideal threat analysis approach and define parameters of evaluating the utility of a threat analysis approach. It was established that current threat analysis approaches do not provide sound techniques of incorporating knowledge of system characteristics in the assessment of threat likelihood. Furthermore, current approaches do not provide a logical technique of quantifying threat business impact. The lack of logical techniques of linking system characteristics and discoverability of vulnerabilities to the likelihood of threats and computation of threat business impact often results into subjective conclusions on threat likelihood and impact, which do not add value on how best to manage threats.

Accordingly, the Threat Nets Approach is proposed to enhance threat analysis in information systems like RPMS. The approach offers systematic guidelines on how to analyze threats in a logical manner. The approach is organized into 4 service recipes: the threat likelihood assessment service, threat impact evaluation service, ROI on threat mitigation controls assessment service and coordination management. The threat likelihood assessment service offers recipes of incorporating system vulnerabilities and threat agents' knowledge in the determination of threat likelihood. The approach also offers a techniques of computing threat business impact and evaluating the cost-effectiveness of threat



mitigation controls. Unlike the current approaches that rely only on security experts to analyze threats, the approach proposes that analysis of threats to information systems be done by both security experts and business analysts. It was observed from the exploratory study that most security analysts are ill-equipped to make authoritative judgment on the impact of threats to the business given their lack of knowledge on business value.

The Threat Nets Approach requires one or more security experts to assess the threat likelihood before business analysts can evaluate the threat impact. The line of reasoning is adopted to minimize limitations associated with the natural bias of experts. The approach proposes that threat analysis of information systems like RPMS should be conducted following 3 sequential activities: threat likelihood assessment, threat business impact evaluation and ROI assessment of proposed threat mitigation strategies. The threat likelihood step is concerned with the identification of system vulnerabilities, threat agents and evaluation of threat likelihood. The step involves the assessment of likelihood of vulnerability discovery and exploitation by threat agents. The threat likelihood service offers recipes of incorporating expert knowledge on system vulnerabilities in the computation of threat likelihood. The threat business impact analysis step focuses on evaluating the impact of the threat on the hospital based on assessment of lost productivity, brand damage, and system restoration costs (recovery cost). The third step, the ROI assessment of threat mitigation controls offers recipes of determining the most cost-effective threat mitigation strategies based on assessment of return on investment and effectiveness rank of a given strategy.

To facilitate the use of the approach, the ThreNet tool was implemented. The web-based tool facilitates coordination of activities among actors during the threat analysis process. The tool implements techniques of computing threat likelihood, threat impact and return on investments on threat mitigation controls.

In order to ascertain the extent to which the approach enhances threat analysis process of healthcare information management systems, completeness, usefulness and usability were selected as appropriate parameters. Accordingly, two case studies were conducted at Case Hospital Kampala and Mengo Hospital. The case studies were setup in such a way that experts (security experts and business analysts) use the approach to analyze threats to the ClinicMaster healthcare information system at the selected hospitals. After which participants were asked by use of a questionnaire to express their appreciation of the usefulness, usability and completeness of the approach. In order to establish the utility of the approach, the outcome of expert evaluation of the case study were analyzed to establish the sensitivity of results. Furthermore, responses of the survey questionnaire were analyzed to

establish the expert's appreciation of the usefulness, usability and completeness of the approach. The results of expert evaluation indicate that indeed, the approach provides complete, usable and useful recipes for assessment of threat likelihood, threat business impact and cost-effectiveness of threat mitigation controls. The results further reveal that the recipes provided for coordination management, do enhance coordination of activities among actors during the threat analysis process. Case study results reveal that the most potent threat to ClinicMaster system at both Case Hospital and Mengo is the unintended disclosure of patient information mainly due to the lack of sound information access policies and patient authentication services. The analysis of the recommended threat mitigation controls for unintended disclosure of patient data revealed that: there is need to train doctors, nurses and lab technologists to be more security conscious when handling patient data.



## Samenvatting

---

Met informatiesystemen zoals Remote Patient Monitoring Systems (RPMS) kunnen dienstverleners in de gezondheidszorg essentiële patiëntgegevens verzamelen, analyseren en verspreiden. Dankzij de tijdige beschikbaarheid van betrouwbare patiëntgegevens kunnen zij zorg bieden aan op afstand gelegen patiënten, wat leidt tot een verlaging in de kosten van de dienstverlening, een betere therapietrouw en een beter toezicht op herstellende patiënten. Het is duidelijk dat informatiesystemen voor de gezondheidszorg zoals RPMS potentie hebben om de groeiende vraag naar diensten in de gezondheidszorg door de toenemende en verouderende wereldbevolking aan te pakken. Het gebruik van RPMS in dergelijke situaties geeft echter ook aanleiding tot bezorgdheid: wat zijn de gevolgen voor de patiënt en het ziekenhuis als een dergelijk systeem faalt? Het identificeren van kwetsbaarheden in RPMS en de bijbehorende bedreigingen en het evalueren van de kans op en gevolgen van bedreigingen zijn dan ook cruciale zaken in het besluitvormingsproces. Ziekenhuisbesturen richten zich bovendien op het vinden van optimale investeringsmogelijkheden. In dit verband is de beoordeling van de kosteneffectiviteit van strategieën om bedreigingen te mitigeren erg belangrijk. Het is duidelijk dat de beoordeling van de bedreigingskans, de evaluatie van de bedrijfsmatige gevolgen van bedreigingen en de kosteneffectiviteit van strategieën een pragmatische benadering vereist bij het begeleiden van de uitvoering van de verschillende activiteiten.

Daarom werden de methodes van bedreigingsanalyse van huidige informatiesystemen geanalyseerd om lacunes te bepalen, de vereisten van een ideale analysemethode van bedreigingen vast te stellen en parameters te bepalen voor de evaluatie van de bruikbaarheid van een analysemethode. Er werd vastgesteld dat de bestaande methodes geen betrouwbare technieken bieden voor het gebruiken van kennis van systeemkenmerken in de beoordeling van de bedreigingskans. De bestaande methodes voorzien bovendien niet in een logische techniek voor het kwantificeren van bedrijfsmatige gevolgen van bedreigingen. Het ontbreken van logische technieken aan de hand waarvan systeemkenmerken en de vindbaarheid van kwetsbaarheden kunnen worden gekoppeld aan de waarschijnlijkheid van de bedreigingen en de berekening van de gevolgen van bedreigingen resulteert vaak in subjectieve conclusies over de kans op en gevolgen van bedreigingen, die niet bijdragen aan een beter risicobeheer.

De Threat Nets Approach is derhalve voorgesteld om de bedreigingsanalyse te verbeteren voor informatiesystemen zoals RPMS. De methode biedt systematische richtlijnen om op een logische manier bedreigingen te kunnen analyseren. De methode is georganiseerd in vier diensten: de bedreigingskans-evaluatiedienst (threat likelihood assessment service), de bedreigingsgevolg-evaluatiedienst (threat impact evaluation service), de ROI (return on

investment = rendement op investering) op de bedreigingsmitigatiecontroles-evaluatiedienst (threat mitigation controls assessment service) en het coördinatiemanagement. De bedreigingskans-evaluatiedienst biedt modellen ter integratie van systeemkwetsbaarheden en kennis van bedreigingsmiddelen bij de bepaling van de bedreigingskans. De methode biedt een techniek voor het berekenen van de bedrijfsmatige gevolgen van bedreigingen en voor de evaluatie van de kosteneffectiviteit van mitigatiecontroles. In tegenstelling tot bestaande methodes, waarbij bedreigingen alleen door beveiligingsspecialisten worden geanalyseerd, stelt deze methode voor dat de analyse van bedreigingen voor informatiesystemen uitgevoerd moet worden door zowel beveiligingsspecialisten als bedrijfsanalisten. In de verkennende studie werd vastgesteld dat de meeste analisten slecht zijn uitgerust om een gezaghebbend oordeel te vellen over de gevolgen van bedreigingen voor een organisatie.

In de Threat Nets Approach moeten twee of meer beveiligingsspecialisten de bedreigingskans beoordelen, waarna een aantal bedrijfsanalisten de bedreigingsgevolgen kunnen evalueren. Voor deze opzet is gekozen om de beperkingen die in verband staan met de natuurlijke vooringenomenheid van deskundigen te minimaliseren. De methode stelt dat een bedreigingsanalyse van informatiesystemen zoals RPMS uitgevoerd zouden moeten worden door drie opeenvolgende activiteiten: bedreigingskansevaluatie, evaluatie van de gevolgen van bedreigingen en ROI-beoordeling van voorgestelde mitigatiestrategieën. De eerste stap houdt zich bezig met de identificatie van systeemkwetsbaarheden, bedreigingsmiddelen en evaluatie van de bedreigingskans. Deze stap omvat de beoordeling van de waarschijnlijkheid dat een kwetsbaarheid door een bedreigingsmiddel wordt ontdekt en gebruikt. De bedreigingskans-evaluatiedienst biedt modellen ter integratie van specialistische kennis over systeemkwetsbaarheden in de berekening van de bedreigingskans. De stap van de analyse van de bedrijfsmatige gevolgen van bedreigingen richt zich op het evalueren van de gevolgen van de bedreiging voor de organisatie gebaseerd op de beoordeling van productiviteitsverlies, merkschade en systeemherstelkosten (recovery-kosten). De derde stap, de ROI-beoordeling van de mitigatiecontroles, biedt modellen voor het bepalen van de meest kosteneffectieve bedreigingsmitigatiestrategieën op basis van de beoordeling van het rendement op investering en de relatieve effectiviteit van een bepaalde strategie.

Om het gebruik van de methode te vereenvoudigen, werd het hulpprogramma ThreNet geïmplementeerd. Met dit webgebaseerde hulpprogramma kunnen de activiteiten tussen betrokkenen bij het bedreigingsanalyseproces worden gecoördineerd. Het hulpprogramma maakt gebruik van technieken om de kans op en de gevolgen van bedreigingen en het rendement op investeringen van bedreigingsmitigatiecontroles te berekenen.

Om na te gaan in hoeverre de methode de bedreigingsanalyse van de informatiesystemen in de gezondheidszorg verbetert, werden volledigheid, nut en bruikbaarheid als de parameters geselecteerd. Vervolgens werden twee casussen uitgevoerd in het Case Hospital Kampala en het Mengo Hospital, waarbij deskundigen (beveiligingsspecialisten en bedrijfsanalisten) aan de hand van de methode bedreigingen van het gezondheidszorginformatiesysteem ClinicMaster van de geselecteerde ziekenhuizen analyseerden. De deelnemers werd daarna gevraagd middels een vragenlijst hun waardering uit te drukken ten aanzien van nut, bruikbaarheid en volledigheid van de methode. Om de bruikbaarheid van de methode vast te stellen, werden de uitkomsten van de evaluatie van de casussen geanalyseerd om de sensitiviteit van de resultaten vast te stellen. Daarnaast werden de reacties op de enquête geanalyseerd om de waardering van nut, bruikbaarheid en volledigheid van de methode vast te stellen. De resultaten van de deskundigenevaluatie geven inderdaad aan dat de methode volledige, bruikbare en nuttige modellen biedt ter beoordeling van de bedreigingskans, de bedrijfsmatige gevolgen van bedreigingen en de kosteneffectiviteit van bedreigingsmitigatiecontroles. Uit de resultaten blijkt verder dat de verstrekte modellen voor het coördinatiemanagement de coördinatie verbeteren van de activiteiten tussen betrokkenen in het analyseproces. Uit de casusresultaten blijkt dat de grootste bedreiging voor het ClinicMaster-systeem zowel in het Case Hospital als in het Mengo Hospital de onbedoelde openbaarmaking van patiëntinformatie is, wat voornamelijk te wijten is aan het ontbreken van een goed beleid voor toegang tot informatie en voor patiëntauthenticatiediensten. De analyse van de aanbevolen bedreigingsmitigatiecontroles voor de onbedoelde openbaarmaking van patiëntgegevens toonde aan dat er een behoefte is om artsen, verpleegkundigen en laboratoriumtechnici te trainen om zich bij het omgaan met patiëntgegevens meer bewust te zijn van veiligheidskwesties.



## Curriculum Vitae

---

Drake Patrick Mirembe was born on the 28<sup>th</sup> June, 1978 in Rakai district, Uganda. He obtained a Bachelors in Computer Science with honors in 2003 from Makerere University and graduated on top of his class. In 2006 he obtained a Masters of Computer Science from Radboud University, Nijmegen (majoring in Security of Systems). While pursuing his Masters, he worked with the Nijmegen Health Initiative and the Security of Systems Department on the development of a secure framework for the implementation of telemedicine, e-health and wellness services. Drake holds a number of professional certifications including Cisco Certified Network Associate, Cisco Certified Academy Instructor, ICDL, Project Management, ITU Cyber Security, ITSO Satellite Communication, Wireless Networking, and Innovation Management among others.

Before pursuing his doctorate he worked both in industry and academia. In industry Drake has worked with a number of organizations both public and private, local and international including Microsoft and ITU as a software developer, network administrator, IT systems security analyst, Innovations Manager, and Senior ICT Consultant. In academia he works with Uganda Technology and Management University (UTAMU) and Makerere University as a lecturer. He conducted his PhD research in Prof. dr. Henk G. Sol's school of engaged scholars in Technology and Management at Groningen University in the area of security management in general and information system risk analysis in particular. His research interests include security of information systems, ICT4D, mobile computing, innovations, and entrepreneurship acceleration.



