World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:12, 2020

Improving Cyber Resilience in Mobile Field Hospitals: Towards an Assessment Model

Nasir Baba Ahmed, Nicolas Daclin, Marc Olivaux, Gilles Dusserre

***Abstract*—**The Mobile field hospital is critical in terms of managing emergencies in crisis. It is a sub-section of the main hospitals and the health sector, tasked with delivering responsive, immediate, and efficient medical services during a crisis. With the aim to prevent further crisis, the assessment of the cyber assets follows different methods, to distinguish its strengths and weaknesses, and in turn achieve cyber resiliency. The work focuses on assessments of cyber resilience in field hospitals with trends growing in both the field hospital and the health sector in general. This creates opportunities for the adverse attackers and the response improvement objectives for attaining cyber resilience, as the assessments allow users and stakeholders to know the level of risks with regards to its cyber assets. Thus, the purpose is to show the possible threat vectors which open up opportunities, with contrast to current trends in the assessment of the mobile field hospitals' cyber assets.

***Keywords*—**Assessment framework, cyber resilience, cyber security, Mobile Field Hospital.

I. Introduction

OFTEN in healthcare, there is mostly a lack of understanding in the information and security risks and implications, 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. 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 [21]. To guide and protect the health sector's cyber space and usage, the 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." [1]. 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, as it is a healthcare subsystem of the healthcare sector and traditional hospitals. These emergency situations where the MFH is deployed help render services in support of local medical facilities; this 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, cannot be compromised. In France, [20] this requires critical operators to reinforce the security of systems, but has been focused on Defense and National Security identifying cyber-attacks as one of the main threats to defense 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.

Nasir Baba Ahmed is with the IMT Mines Ales, France (e-mail: nasir4u07@yahoo.com).

II. State of the Art

A. MFH & Its Cyber Assets

MFH are described as mobile, self-contained, self-sufficient health care facility capable of rapid deployment and expansion or contraction to meet immediate emergency requirements for a defined period of time [2]. This category of hospitals is unique due to its ability to be mobile in terms of transferring medical supply and medical services swiftly but still preserve the quality of services.

Two of the major reasons for the application of MFH are: to provide emergency medical services to remotely located areas, war-torn areas, terrorist attack areas, virus out-breaks, natural disasters and to provide to the less privileged citizens that lack access to basic healthcare services. These are all handled by its users and stakeholders, which include the management (e.g. local authorities), administration (e.g. logisticians), medical practitioners and care givers.

Some MFHs may have digital capability of management, in terms of managing the Electronic Medical/Health Records. This involves the use of tools such as computers/tablets, routers, barcode printers, barcode readers, electrical and network cabling etc.

The stakeholders and users are supported by certain I.T facilities and cyber assets that help to carry out tasks faster and more efficiently especially in cases of emergencies (Table I).

TABLE I
Main Cyber Assets Deployed in MFH

Workstation Computers	Barcode Reader
Tablet Computers	Barcode Printer
Network Router (HUB)	Printer/Copier
Network Switch	Wireless Router
Medical Devices	LAN/WAN
Patient Tracking System	External HD/USB Drives

These assets are connected to a LAN (Local Area Network),

the internet or are stand-alone systems with transferable memory or connection options, and may vary depending on the type of MFH of a particular organization. Also, the I.T systems help introduce a formalized and organized method of utilizing scarce medical resources through gathering information to track and present it to stakeholders. These systems also help manage the supply/demand chain of medical treatment and facilities continuity of care, and for logistics purposes.

B. Threat Landscape

The healthcare sector in general is a constant rising target for cyber criminals. In 2015 alone, the healthcare industry was the most attacked by cyber criminals where over 100 million healthcare records were compromised from more than 8,000 devices in more than 100 countries. This trend strongly suggests that the healthcare industry is a prime target of cyber criminals [3].

Considering the cyber assets deployed in the MFH, though its ad-hoc cyber infrastructure may pose a lesser avenue for cybercriminals but with identical cyber assets and technological elements, certain threats are faced. According to [4], the interconnected systems and devices are exposed to:

- Malicious actions coming from different sources such as malware (virus, trojans, worms), Denial of Services (DoS) attacks, device tampering and data exfiltration/theft from the cyber assets.
- Human factors that are carried out due to involuntary actions that may result in harm or damage of any component of the cyber assets.
- System or application failure that may cause destruction or disruption of software applications such as firmware failures, overload, network failure, database errors, server access failure and hardware device failure.
- Third-party or external stakeholder failure that are usually based on third-party actors/stakeholder such as the host community, other NGOs, suppliers etc., which may not have followed the required procedure or previously compromised.
- Natural phenomena that are out of the human control such as wildfires, earthquakes, floods and other natural disasters that may cause disruption of normal services of the MFH.

C. Cyber Resilience

Even though the cyber security concept is now used extensively in the information security practitioners, politics, and businesses, cyber resilience as an academic research topic is at an infancy stage. The concept of resilience combined and implemented in cyberspace refers to the concept of Cyber Resilience. For [5], resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions". 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 [6].

While the aim of cyber security is to protect assets available in the cyberspace, cyber resilience focuses on higher levels of ensuring service-delivery and continuity. Consequently, a system is cyber-resilient when it is able to deliver effective service value, even in adversity. Thus, all efforts must take into consideration the process in which the Health sector delivers its services, as the main goal of achieving this.

III. Cybersecurity in Healthcare & MFH

Over the years, the main causes of breaches have evolved with a preponderance of loss/theft of healthcare records and electronic protected health information, even though better policies and procedures, and use of encryption reduce easily preventable breaches. The healthcare data breach statistics show that the main causes are now hacking/IT incidents, with unauthorized access/disclosures (Fig. 1). Furthermore, it shows that there has been an upward trend in data breaches in the past 9 years, with 2018 showing more breaches reported than the rest [7].

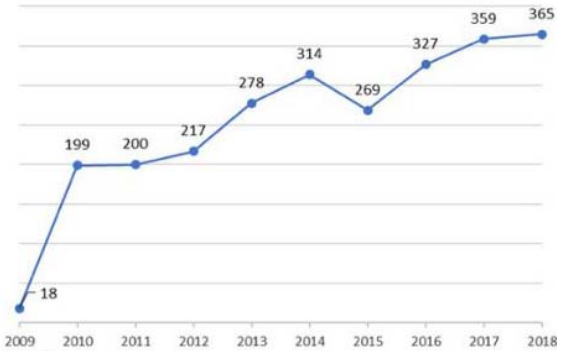

Fig. 1 Healthcare data breaches [7]

In the case of breaches and attacks on MFHs, there are no cases or reported breaches that have occurred directly from or on the MFHs, though most MFHs may be affected if the traditional hospitals are affected by such breaches, 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-maxim by cyber security experts goes "As long as you have the slightest relevance, you will be attacked, if not already, but just a matter of when". Accordingly, for MFHs especially those owned by Governments and well-known large corporate international NGOs, if they have not already been attacked without realization or detection, then it may just be a matter of 'when' it will happen. Moreover, the popular quote from the former director of the FBI Robert Meuller reads "There are only two types of Organizations, those that have been hacked, and those that those that will be" [22]. This statement stresses the need to achieve resiliency in delivery of its cyber assets' services and support, even though there are not as many as those cyber assets deployed in conventional hospitals.

IV. Cyber Resilience Assessment Trends

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.

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 allows the 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. [8]

According to [9], 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 ISO/IEC 27001/27002.

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.

A. Major Frameworks

The NIST Framework

The NIST Framework aims to enable organizations to manage cybersecurity risks, especially in critical national infrastructure [10], [11]. 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 one of 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 [12]. 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 [13].

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 [14].

B. Other 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 FFIEC CAT
ii. The CIIP framework
iii. The ENISA CSIRT Maturity self-assessment tool
iv. The SRA tool
v. The Colony tool
vi. The US-CERT CSET
vii. The RSA Cyber Security Maturity Assessment

The FFIEC CAT

The Federal Financial Institutions Examinations Council (FFIEC) of the U.S developed the Cybersecurity Assessment Tool (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 [15].

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.

The CIIP

The Critical Infrastructure Information Protection (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) [16].

The CIIP framework aims to establish a common minimum cybersecurity 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 [16].

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 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.

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) [17].

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.

The SRA Tool

The SRA (Security Risk Assessment) 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 [18]. This also concentrates on steps taken to secure patients' and users' electronically generated and stored data.

The tool's user-friendliness 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.

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 [19].

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.

V. Cyber Resilience Assessment Opportunities

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 procedures. 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 user-friendly and easy to implement security assessment framework that will be adopted and tailored to the requirement of an MFH is needed in order 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.

A. 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.

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.

B. 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 behaviors 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.

C. 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 centers. 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.

D. 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 requirement, 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.

VI. 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 paper, as recommended by ENISA and ANSSI [16], [17].

Out of the frameworks reviewed in this paper, 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.

TABLE II
PARAMETERS IN DIFFERENT SECURITY FRAMEWORK CHOICES

Requirements	Frameworks			
	NIST CSF	*ISO27001*	*FFIEC*	*CIIP*
Comprehensive general security	Yes	Yes	Yes	No
Prescriptive	Yes	Partial	No	No
Supported & Maintained	Yes	Yes	Yes	Yes
Practicable & Scalable	No	No	Yes	No
Assessment Guidelines	Yes	Yes	Yes	Yes
Open Standard	Yes	Yes	Yes	Yes
Assess once report many	Partial	Partial	No	Yes

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, as shown in Table II, 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.

VII. CONCLUSION

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, this affects the final assessment score. The model illustrated in Fig. 2 is proposed to be developed in the future work, with its inputs from the NIST and ISO sections, as well as other self-assessment frameworks serving as a foundational medium to provide a baseline and the as-is state.

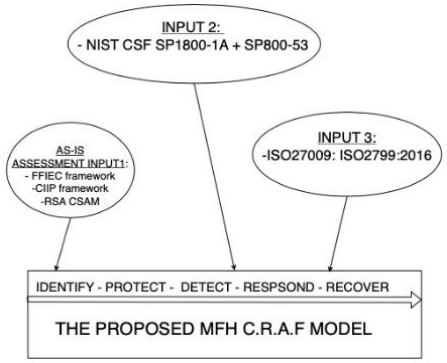

Fig. 2 Proposed CR assessment model for MFH

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) should be considered, especially regulations that apply to the host communities for the deployment of the MFH.

REFERENCES

[1] 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).

[2] PAHO, WHO, (2003). *WHO-PAHO Guidelines for the Use of Foreign Field Hospitals in the Aftermath of Sudden-Impact Disasters. In Hospitals in Disaster - Handle with Care*. San Salvador, El Salvador, 8-10 July 2003

[3] Infosec Resources. (2019). *Top Cyber Security Risks in Healthcare*. (online) Available at: https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare/#gref (Accessed 25 Nov. 2019).

[4] Cyber security and resilience for Smart Hospitals, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals (Accessed 20 Nov. 2019).

[5] Wold, G. (2017). *Cybersecurity resilience planning handbook*. Matthew Bender.

[6] Bodeau, Deborah, and Richard Graubart, "Cyber Resiliency Engineering Framework". MITRE Report. Pg. 37 (2011).

[7] HIPAA Journal. (2019). *Healthcare Data Breach Statistics*. (online) Available at: https://www.hipaajournal.com/healthcare-data-breach-statistics/ (Accessed 24 Nov. 2019).

[8] 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

[9] 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.
[10] 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.
[11] 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.
[12] 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).
[13] 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).
[14] Iso27001security.com. (2019). *ISO 27799 ISMS for healthcare*. (online) Available at: https://www.iso27001security.com/html/27799.html (Accessed 25 Nov. 2019).
[15] Ffiec.gov. (2019). *FFIEC Cybersecurity Awareness*. (online) Available at: https://www.ffiec.gov/cyberassessmenttool.htm (Accessed 25 Nov. 2019).
[16] 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).
[17] 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).
[18] 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).
[19] Us-cert.gov. (2019). *ICS-CERT Landing | CISA*. (online) Available at: https://www.us-cert.gov/ics (Accessed 20 Nov. 2019).
[20] Gurudutt, K. (2019). *Cyber Security Framework for Healthcare* (online) SogetiLabs. Available at: https://labs.sogeti.com/cyber-security-framework-healthcare/ (Accessed 20 Nov. 2019).
[21] 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).