IMT Mines Alès
École Mines-Télécom

N. BROTTIER
Y. MAHEU
G. PROT
PRISM 170

Rapport de mission R&D :

Cyber resilience in MFH (mobile field hospitals)

Tutor : Nasir Baba Ahmed

This report is exclusively in english, like the mission.

IMT Mines Alès
École Mines-Télécom

IMT Mines Alès
École Mines-Télécom

Summary :

1) Around Cybersecurity

Cyber security in hospitals has become a growing matter, indeed, we have entered a new era of digitalization. Therefore, the access to sensible data within hospitals has become easier and easier and in addition, these sensible data have a high value on the blackmarket, that's why there is a real proliferation of cyber-attacks on hospitals, moreover hospitals are a technology saturated environment, they are complex organizations really hard to protect, financials pressures complicate the task.. For example, in France, the number of cyber attacks on hospitals has been multiplied by 4. If big hospitals hardly manage to fight hackers and to protect their data, it's even more difficult for mobile field hospitals (MFH). The purpose of this R&D mission is to evaluate the cyber resilience of the MFH. First, we'll have a look at the general concept of cyber security and cyber resilience and how it is managed in the health sector, secondly on the MFHs and their cyber security, then the general concept of penetration test then how to apply it to MFHs.

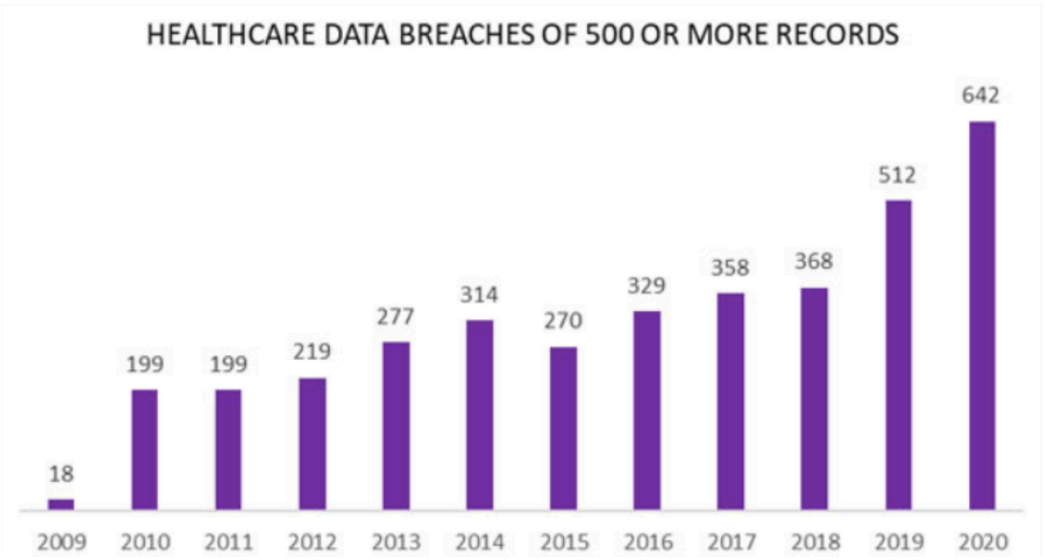


Figure 1: Number of data breaches in the Health sector

1.1. Technical concepts

The first thing we need to do is to explain the difference between cyber resilience and cyber security:

- **Cyber security:** Refers to an entity's ability to continuously deliver the intended outcome, despite adverse cyber events.
- **Cyber resilience:** Practice of defending/preparation/full cycle with steps computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Hackers can proceed by many different ways but the most common ones are :

- **DoS (Denial of Service) :** *flood of requests which cause an informatic bug*

- **Man-in-the-middle :** *hacker do the intermediary between the victim and the server*

- **Phishing :** *fake mails*

- **Drive by attack** : *set up an HTTP or a PHP script*

- **Password attack** : *test or steal password*

- **SQL injection attack :** *SQL request*

- **Cross-site scripting attack :** *inject Javascript in database*

- **Eavesdropping attack** : *intercept a message with information in it*

- **Birthday attack** : *find the MD of a message and replace it*

- **Malware attack :** *install malware without consent*

Thus, hackers can attack a system from many different ways,as shows the diagram below.

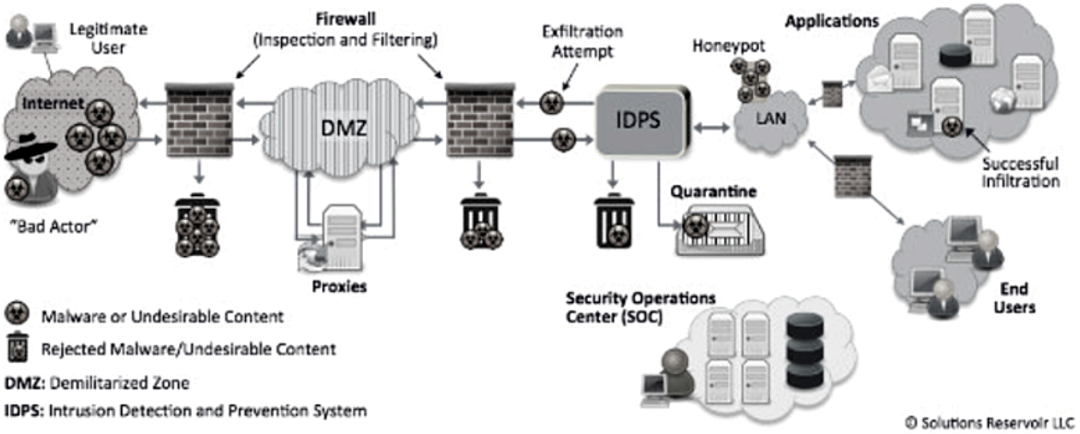


Figure 2: View of the Cybersecurity Landscape

1.2. Recent events

Cybersecurity is a field that is jeopardized by bad-intentioned people since it existed, but most lately many consequent attacks occurred during the last 4 months. Not as lucrative as the WannaCry operation (2017, ransomware that infected more than 300 000 computers through the world and generated 4+ billions of dollars of paid ransoms) nor as political as Stuxnet (2010, this american informatic worm was designed to take control of nuclear facilities in Iran), but attacks happen every day.

Lately, in France, two hospitals were targeted by cyber attacks : Dax and Villefranche. With the same operative process, those hospitals were temporarily put on stand by and delayed some cares that ought to be provided to patients. In February, one of Dax' hospitals was infected by a ransomware : its data were encrypted, so all the staff had to continue to work with pens and paper. The people needing urgent care that couldn't be provided here were transported to other hospitals. The Head of Regional Health Agency refused to pay, because there was no certainty that the data would have been recovered, and he also didn't want to fund crime and tempt other people to do the same. A few weeks after, Villefranche's hospital witnessed the same event.

Not in the health sector but also recently, the Afnor (french agency of standards and norms) was victim of a cyberattack (also ransomware, Ryuk) that blocked the agency's website. Students doing a PhD or a thesis, company researchers, all the people who needed to know an exact value of a standard to progress in their tasks were unable to access it via the website.

1.3. In health sector

As explained above, there are many ways to attack and destabilize a system, but in the health sector most of the attacks are related to data, it can be data stealing which the hackers sell after or a ransomware which is a virus that encrypt all your data and ask for money in exchange for the key to decrypt the data. There are different methods to do that for example: DoS, Man-in-the-middle, Phishing, Ransomware.

However, hospitals are not the only targets of hackers in the health sector, for example, attacks against laboratories which are seeking vaccine against the coronavirus, to do industrial spying/or confuse the research - The responsible are Strontium (Russia - password attack), Zinc and Cerium (North Corea - phishing).

There have been many attacks on the health sector in France lately, we can take the example of Dax and Villefranche which have been the targets of a ransomware attack (described above).

2) Mobile Field Hospitals

2.1. General information

Depending on the solutions it can operate as a stand-alone entity (as in the American solutions), or in conjunction with the whole hospital (but still autonomously, as in European solutions)

They are used in case of an epidemic, a natural disaster (notion of emergency) or when the access to a traditional, stationary health care facility is limited.

There are different types of field hospitals: PSM (1 or 2) and PMA depending on the number of patients and the reason for the MFH deployment.

2.2. Assets identification

We made an exhaustive list of the cyber assets of an MFH and we categorized them. Depending on the type of MFH and the context of its deployment some items might not be in all MFH.

Medical devices:

- Scope: Heart rate, pulse, oxygen level in blood, arterial tension, temperature…
- Defibrillator: Analyze heart rate and help resuscitate people after heart attack
- ECG machine: Measure the electrical activity of the heart
- Blood sample analysis machine: Performs analysis on blood sample
- Health sensors: Heartbeat sensor, pulse…
- Respiratory support: Helps people to have enough oxygen

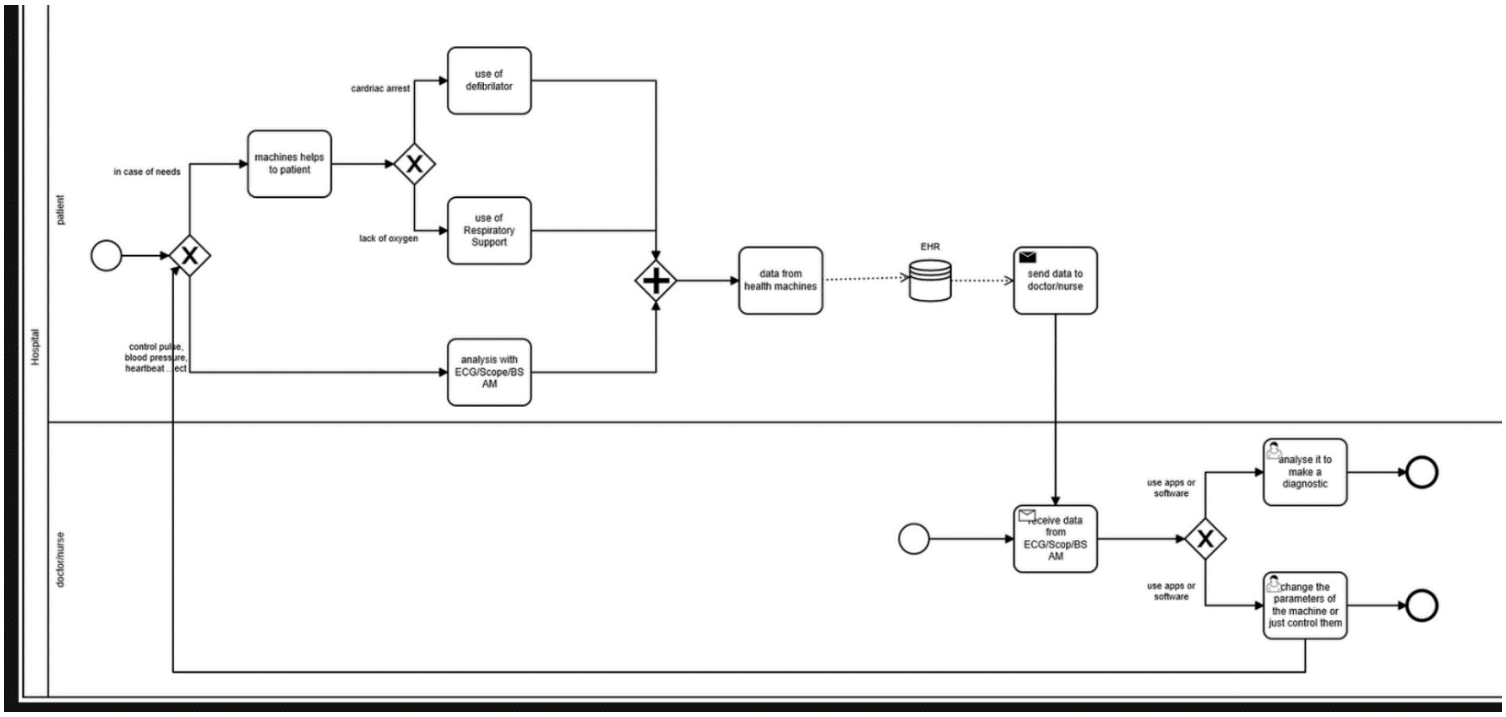


Figure 3: BPMN diagram on medical devices

Hospital operation :

- Cables: connect machines to aliment them or exchange information
- Power generator: generate electricity to aliment the machines of the hospital
- Hydraulic pumps: pumps distribute water in all services
- Antenna: Recover information from electromagnetic waves and transform it in a numerical signal

-

Extern assets:

- Mobile phone, tablet, computer, printer/reader, USB key: Machines use by members staff or patient, difficult to control they are often linked on hospital wifi and sometimes linked by USB or HDMI on hospital material
- Password/ID: choose by users they permit them to use hospital material

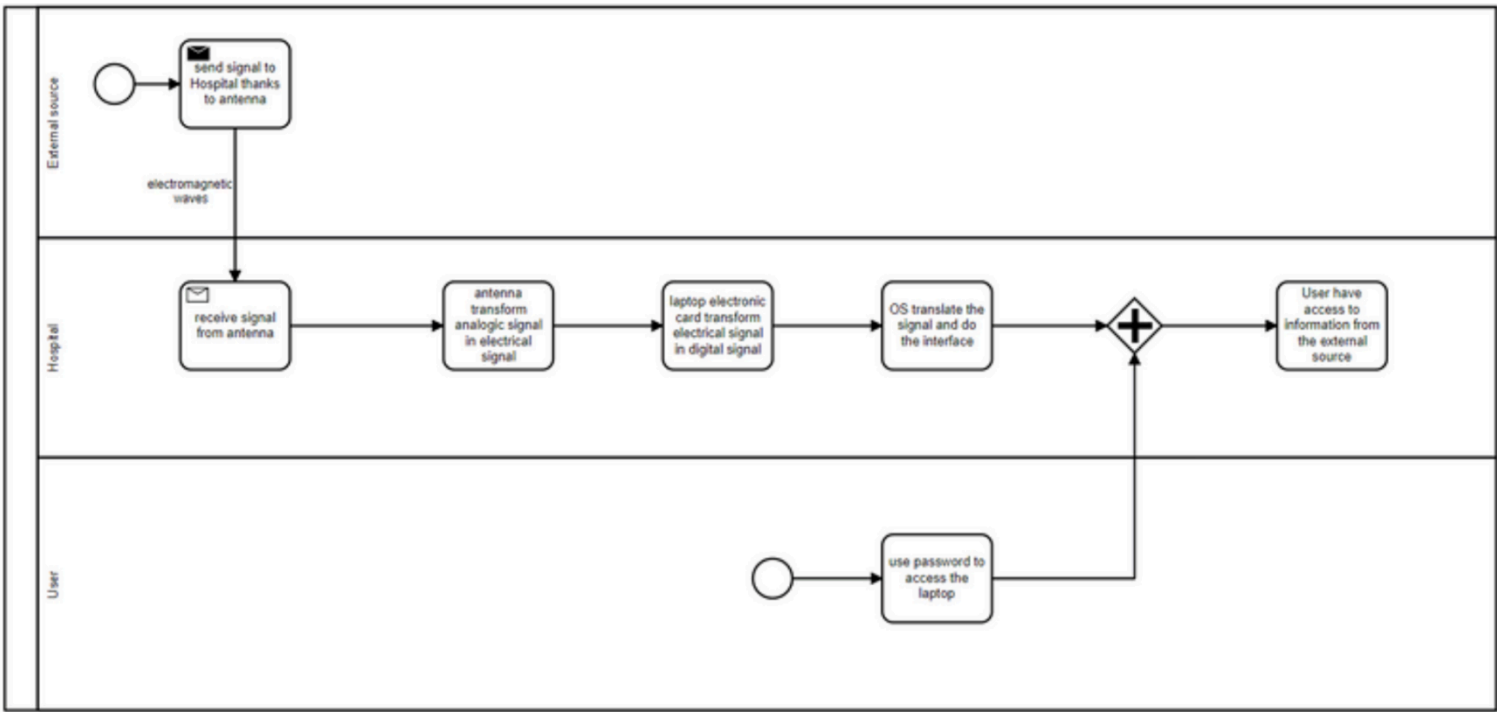
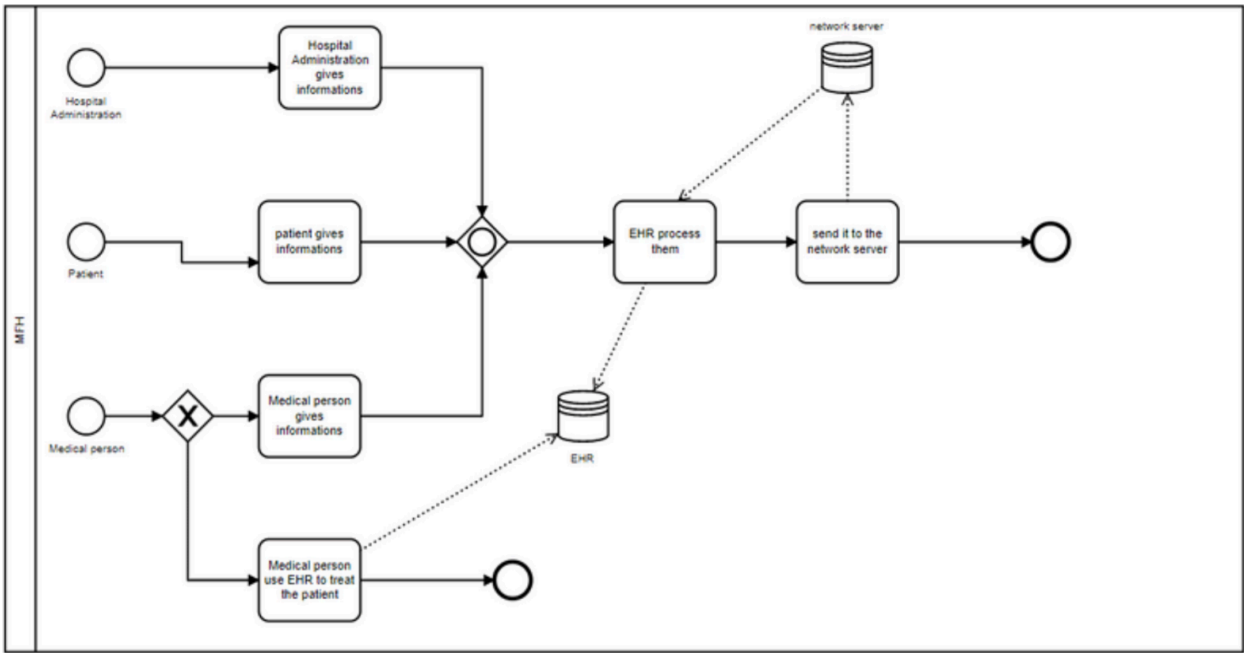


Figure 4: BPMN diagram of Extern assets in MFH

Data base:

- Electronic medical record (EMR): software that capture clinical data and allow it to be searched and managed
- Electronic health record (EHR): software that capture clinical data and allow it to be searched and managed, focused on communicating that data with other providers, making sure patient information flows unimpeded across the continuum of care

Figure 5: BPMN diagram on the database in MFH



Tools:

- Software like Excel/ Word etc…: Write/ edit files, spreadsheet…
- Website: Provide information on the MFH, access to MFH information
- Machine's software: The different software devices use
- Mobile apps: The apps mobiles use

Networks:

- LAN: local area network
- WIFI: A system for connecting electronic devices to the internet without wires
- Router: Router is a networking device, commonly specialized hardware, that forwards data packets between computer networks
- Network switch: Networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device
- Network server: A computer system, which is used as the central repository of data and various programs that are shared by users in a network
- Intranet: Network operating like the World Wide Web but having access restricted to a limited group of authorized users
- Network access control: A security tool that controls how computers connect to a network

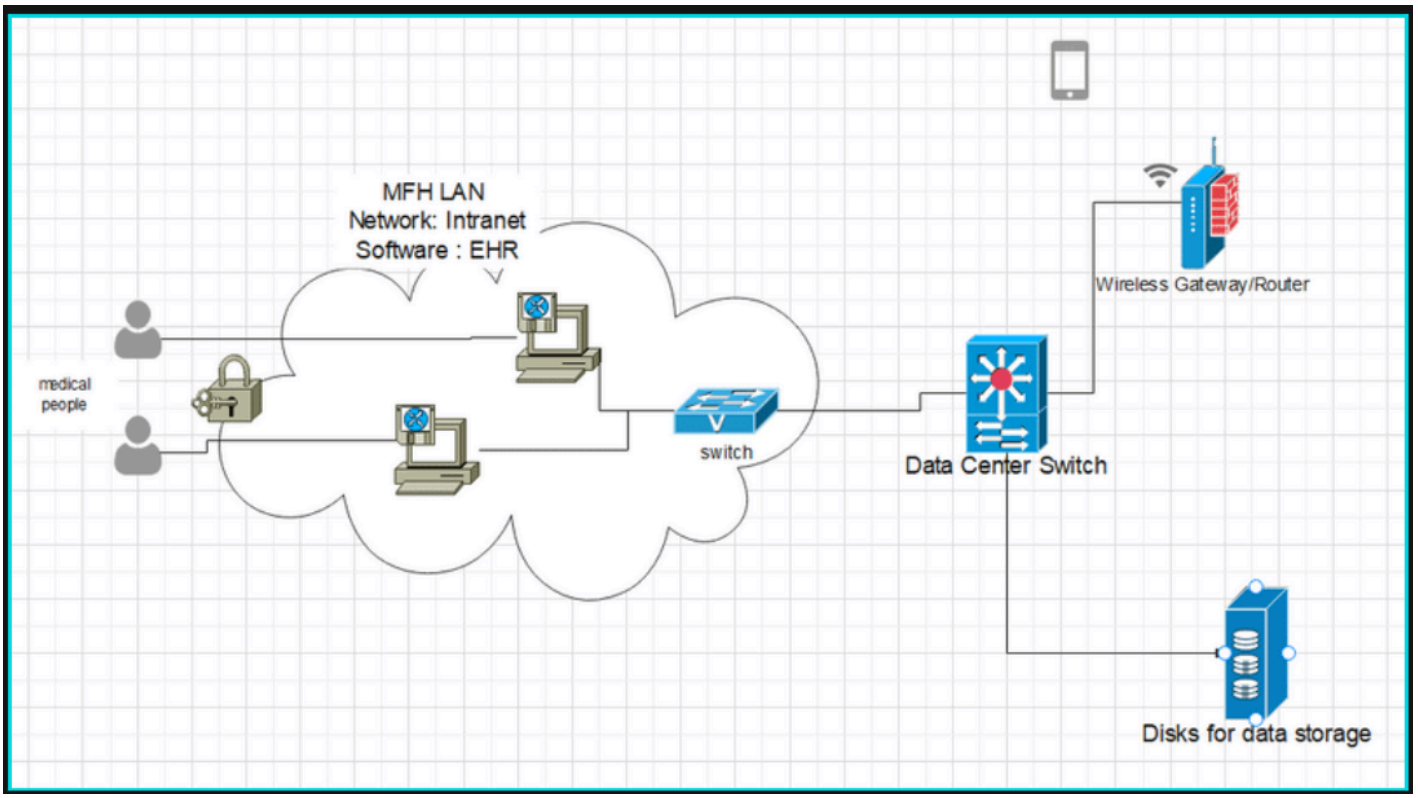


Figure 6: Diagram of the MDH network

Now that we established a list of the different cyber assets we can now prioritize them in term of cyber-attack:

1- **Extern assets:** *many items that come and go, often entry point of cyber attack*
2- **Database:** *source of all data, standby if endangered*
3- **Networks**: *because it is where all the data transits*
4- **Tools**: *may be consequences of an attack, paralysed because no data available*
5- **Medical devices**: *consequences too, but importance due to*
6- **Hospital operations :** *can function separately*

2.3. Stakeholders in MFH

Cybersecurity is the responsibility of everyone in a MFH, therefore, we need to identify all the different stakeholders in a MFH in order to be more prepared for social engineering.

Healthcare personnel :

- They are in charge of patients' health

- They have access to sensible data on patients

Paramedics :

- They can be in charge of patients' health

- They can have access to some data

Government :

- Authorize the deployment of the MFH

Patients :

- Give some information

- Many patients in an hospital

Outside personnel (upkeep, logistic personnel) :

- They have access to sensible infrastructure

- They are in charge of keeping up the infrastructure and differents devices of the MFH

Visitors :

- People that are with the patient (parents with a young child,...)

- Are external assets that are difficult to manage, but can have physical access to the MFH

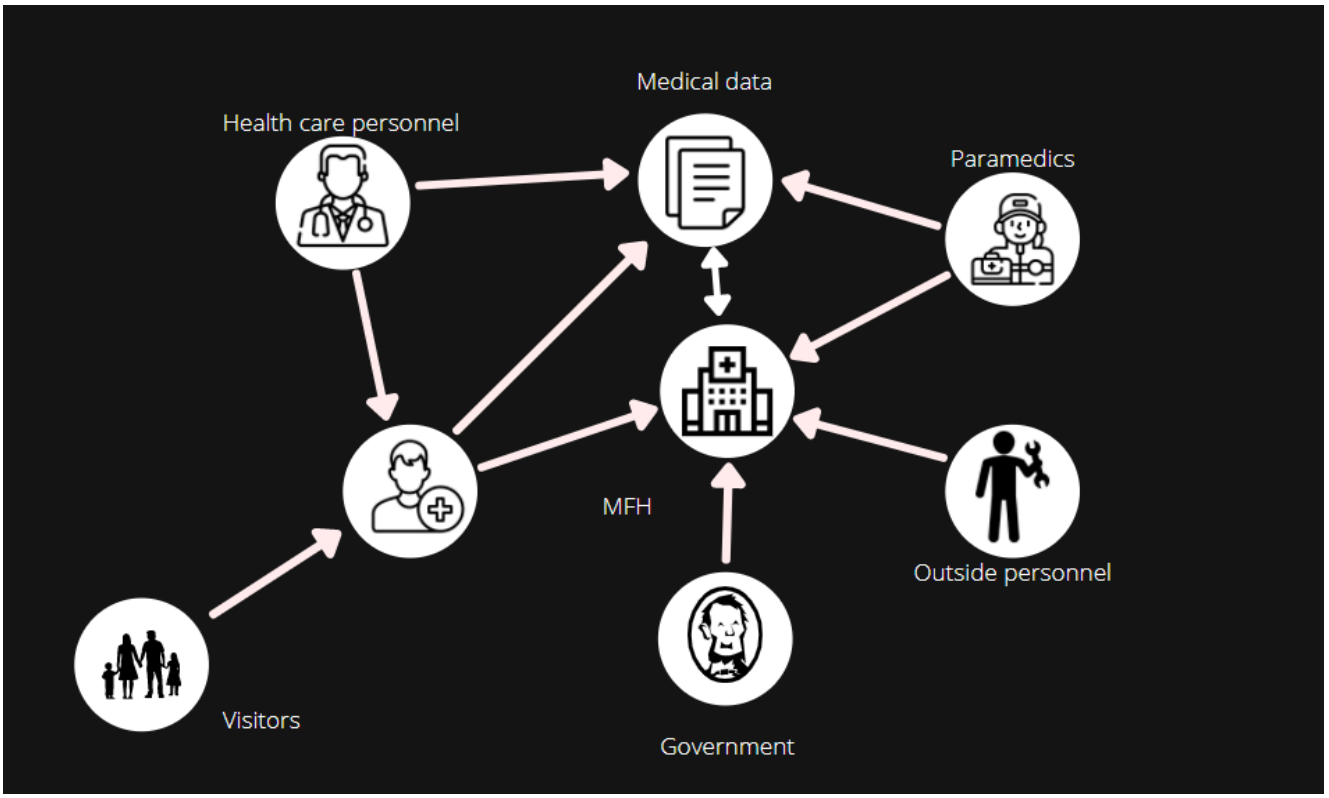


Figure 7: *Stakeholders mapping*

3) Penetration test

3.1. Comparison of Methodologies & Frameworks

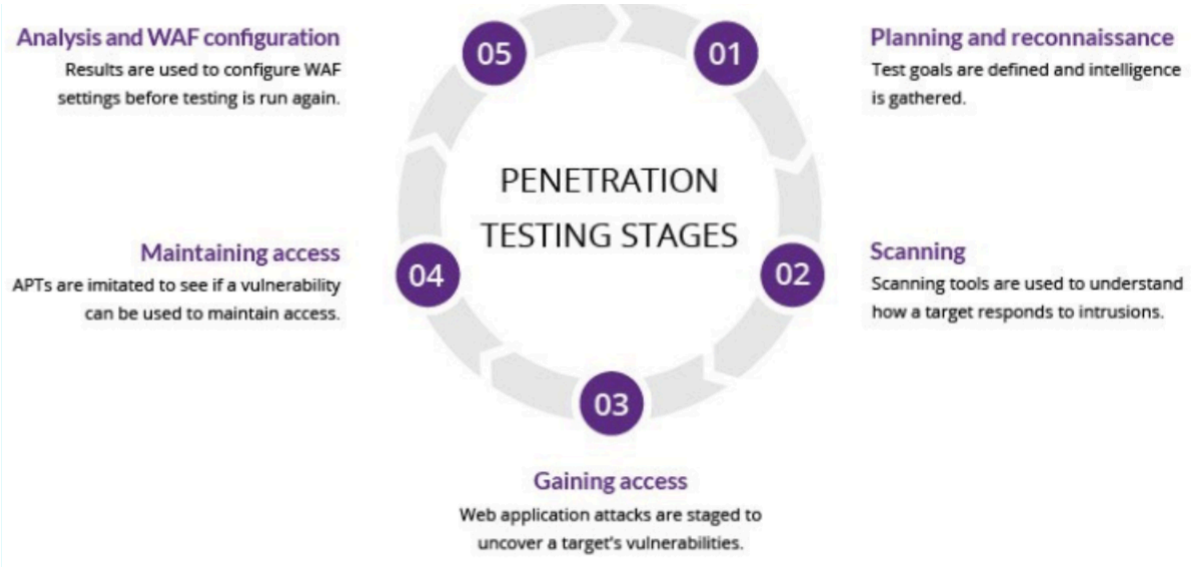


Figure 8: The 5 steps of penetration testing

There are many different penetration tests for every scenario of attack. First you have to determine the level of information that the hacker has on your system :

- **Blackbox:** The tester tries to find information on the system/company/person
- **Greybox:** The tester posses only User-Password (like an employee)
- **Whitebox:** The tester have access to multiple information on the targeted system
    - User-password (like employees)
    - Architecture diagrams
    - Source code

There are also many different types of methodology for these penetration tests (PTM).

Penetration Testing Frameworks and Methodologies	What is it ?
Open Source Security Testing Methodology Manual (OSSTMM)	-contains a comprehensive guide for testers to identify security vulnerabilities within a network -allows testers to customize their assessment -created to support network development teams -methodology relies on the tester's knowledge and IA
Open Web Application Security Project (OWASP)	- helped organizations to curb application vulnerabilities -the guide provides comprehensive guidelines for each penetration testing method
The National Institute of Standards and Technology (NIST)	-offers specific guidelines for penetration testers to follow -guarantee information security -tests on applications and networks
Penetration Testing Methodologies and Standards (PTES)	-highlights the most recommended approach to structure a penetration test -guidelines to perform post-exploitation testing -practical recommendations that management team can rely on to make decisions
Information System Security Assessment Framework (ISSAF)	-contains an even more structured and specialized approach to penetration testing -enable a tester to meticulously plan and document every step of the penetration testing procedure - complementary information, various vectors of attack, as well as possible results when a vulnerability is exploited

3.2. Most suitable solution

Considering the different assets of the MFH that we saw previously, the most suitable PTM are the following :

PTES :

- Good planification and structuration of the attack
- Goes from blackbox to whitebox

NIST :

- Test on the global system
- Test for network and applications
- Reliable test
- easy to use

4) Table-top exercise

Tabletop exercise (TTX) is a disaster preparedness activity that takes participants through the process of dealing with a simulated disaster scenario. The purpose of a tabletop exercise is to evaluate an organization's preparedness for a particular disaster and to inform required participants of their roles in the response. A tabletop exercise goes through every aspect of response and the follow up the organization will need to do.

We chose to perform a Table-top exercise for our study because we are working on cyber resilience, therefore we have to work on cyber security but also on social engineering, to see the response of every stakeholder/Role in a given scenario so that this scenario cover every step from reducing the risks to how to manage a cyber attack, to recover from it as quickly as possible. Also, a PT test would be too technical because we don’t have strong basics on this topic.

4.1. Preparation of our Table-top exercise

The objectives of this Table-top exercise (TTX) are to create a situation to test the reactions of the staff, to identify the different threats and weaknesses, to improve the response of the MFH in every step of the scenario and to talk about social engineering.

We first created 2 different scenarios, each composed of a primary scenario which explains why the government deployed a MFH and a secondary scenario which is the cyber attack.

4.2. Scenarii

First scenario : COVID-19 in Corsica + Ransomware

PLAN :

Primary :

- High contagion wave of COVID-19 in Corsica, few hospitals are full, difficulties due to the island geography
- Need to implement a MFH in Bastia

Secondary :

- Mail to a service staff
- The email asks the staff member to change their password due to a new staff password policy
- The attacker recovers the user + intranet password pair
- Physical implementation of ransomware (USB, accomplice) during a period of high activity in the MFH
- Data encryption
- Ransom is not paid

When the attack happens, the contagion has already reached a really high level with an incident rate of 800/100 000. Moreover the team has received a new convoy of patients from Ajaccio where there is no control anymore of the virus. There are patients everywhere, some of them are waiting outside to be healed. So no one remarks that an intruder has entered the MFH and when the first injection happens, it's chaos.

Second scenario : Tsunami in the Samoan + DoS

PLAN :

Primary :

- A tsunami caused big damage in Samoan Island, few hospitals are usable so countries offer their help
- France sends medical staff and equipments : MFH

Secondary :

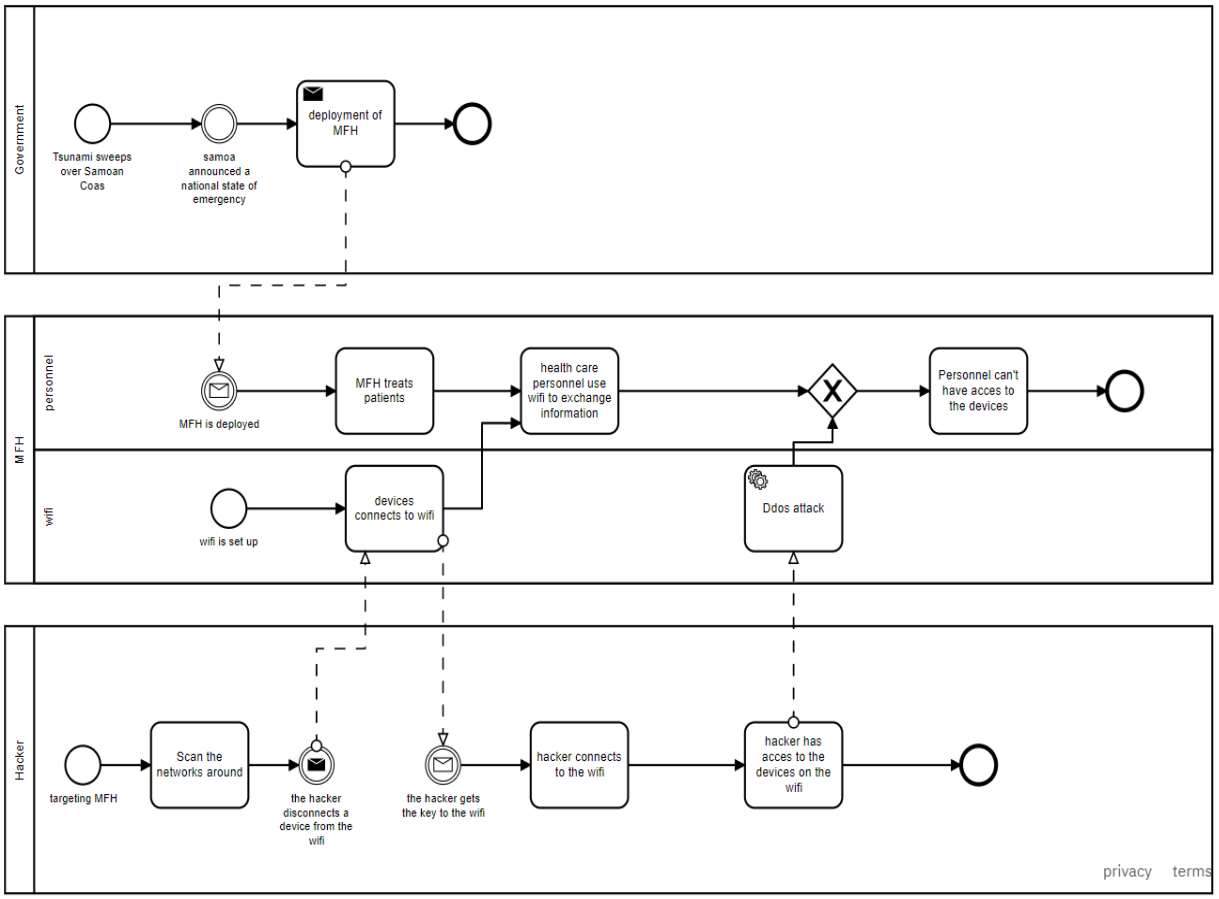
- A bad-intentioned person (Mr.H) comes near the MFH to be close to wifi
- Mr.H remotely disconnects 1 or 2 electronic equipments from the wifi
- While these are reconnecting to the network, Mr.H “listens” to the password
- Then he accesses the Wifi with the stolen password
- When connected to the wifi, he saturates the flow with a huge amount of useless data
- network crashes
- restoration of the network

Context :

MFH targeting : *The hacker pays a stakeholder to give him information about the MFH assets*

INTRUSION : *a fire happens near to the MFH, the hacker uses this event to go near the MFH without being recognized and hack the wifi in secret.*
INJECTION: *hacker uses the first injection to observe the MFH response*
hacker attacks at 1pm because it's really hot, so patients with respiratory help are in grave danger.

For more precise timeline and description of the scenarii, we refer you to the annexes.



4.3. Questions and roles

In order for the table-top exercise to be as precise as we can we designed a set of questions and we distributed all the different roles. Each person has a role and has to respond to the question accordingly to his predefined role. For this table-top exercise

to be the best possible and for us to have data to analyse, we decided to add a "time of response" (T.o.r) and also a scaling system for the question, which is the following :

- **1** : "I am prepared to this question, it is easy for me to answer because my formation learn me how to proceed in this situation"
- **2** : "First time I am seeing that but I know how to respond, I need my experience and my formation to answer but i'm think I will be ready in this case"
- **3** : "I am not is sure about the answer, I've used personal knowledge to answer"
- **4** : "Not sure at all about my answer, I am a novice in this domain but I tried something"
- **5** : "I have no idea at all"

The different roles of our exercise were : Medical staff, IT officer, Head of operation and Public relations officer.

This is an example of a question that we asked for the first scenario, you can see that each role has to answer it and scale it.

X) What do you know about Phishing and ransomware ? (2min max)

Roles	**Medical Personnel / Reception officer**	**Information Technology officer**	**Chief Medical officer / Head of mission**	**Public relations officer**	**Other**
Answers	Phishing? Ransomware is like a virus that blocks data in	use personal to have informations Hack a infrastructure	Phishing is a way to steal information, it can be ID/password for anything, ransomware is	From reports in the media, I am aware of the basic details and	

	exchange for a ransom?	then ask for money (more used in hospital hacking)	a virus that encrypts your data and then asks for a ransome to decrypt your data.	techniques used in this attack, and some victims too.	
T.o.r	1m53	1m42	1m27	42 s	
Question Scaling	2	1	1	3	

Data analysis

We analyzed data thanks to the 2 indicators we used in our questionnaire (T.o.r and Question scaling). We first did a summary of the different responses: we first looked at the scaling of the question to see if the question was easy or not for the different protagonists and we took this into account when we analyzed the answers. Then after reading the answers we made a list of what's good, what's bad, what's missing etc... And finally after that, we made recommendations about what they should do.

Test Analyze

With the method explained above, we have deduced some problems, areas of improvements for the two scenarios.

- First scenario :

  . There is an IT dependance

  . The personnel is not prepared to ransomware attack, they need a procedure to follow

  . The participants think that TTX scenario prepare the personnel

. As improvement areas we think that MFH personnel need some formations for ransomware attacks, phishing prevention and physical enter prevention .

- Second scenario :

  . There is an IT dependance

  . People are not aware of the danger of DDoS, they don't know what it is and don’t react accordingly.

  . They would need training on this topic. However, they have good ideas to continue to treat patients even without IoT

As a final conclusion we would say that this type of exercise is great to improve MFH cyber resilience, we noticed that there was not a simply procedure to follow. That’s why as an improvement ares we had done some SOPs to help the MFH personnel working safety. These SOPs can’t replace a serious cyber resilience formation, that is necessary for MFH safety.

BIBLIOGRAPHIE :

[1] Martin Untersinger "Attaques informatiques en série contre les laboratoires engagés dans la recherche d'un vaccin contre le Covid-19". Article paru le 17 novembre 2020.
https://www.lemonde.fr/pixels/article/2020/11/17/vaccin-contre-le-covid-19-des-laboratoires-dans-le-collimateur-de-pirates-informatiques_6060079_4408996.html

Source : Le Monde

[2] Dossier d'information du ministère des solidarités et de la santé, paru le 28 novembre 2019 pendant la campagne nationale d'information sur la cybersécurité en santé.
Source : Ministère des solidarités et de la santé

[3] Centre Médical des Armées de Courbevoie Brigade des Sapeurs de Pompiers de Paris "Plans d'Urgences Nombreuses Victimes" Présentation du 28 Août 2011.
Source : Centre Médical des Armées de Courbevoie

[4] Sécurité publique canada "Principes fondamentaux de cybersécurité" Dossier paru le 21 janvier 2019.
Source : Sécurité publique canada

[5] Rapport d'alerte de cyber vulnérabilité des instruments médicaux
https://cyberveille-sante.gouv.fr/cyberveille-sante/1210-une-vulnerabilite-decouverte-sur-un-instrument-ultrasons-illustre-les-cas-de
Source : Site du Ministère des Solidarités et de la Santé

[6] Conférence de presse du directeur de l'Agence régionale de la Santé de Nouvelle-Aquitaine
https://www.youtube.com/watch?v=05gRH05bJMQ&feature=emb_logo

Source : Vidéo capturée par le journal Sud-Ouest

[7] Site internet de l'ESCRIM
http://escrim.org/

[8] « Les hôpitaux plus que jamais en première ligne »
https://sd-magazine.com/securite-numerique-cybersecurite/cybersecurite-les-hopitaux-plus-que-jamais-en-premiere-ligne
Source : Article du journal Sécurité et Défense

Timeline for the first scenario

Date	Time	Event	Description	Expectation
05/08/2021	X	COVID pandemic contagion wave	First cases of Corsican Covid, more contagious and lethal variant	The variant is not to stay and patients are to be treated
21/08/2021	18h03	Corsica in quarantine	After 2 weeks the Covid impact factor is of 500 people, J. Castex annonces a confinement in Corsica	PEOPLE STAY AT HOME AND NO MORE VIRUS
24/08/2021	X	Need to implement a MFH	Too many patients with Corsican Covid, their number is still highly increasing	The MFH is correctly deployed and is to accept patients
26/08/2021	8h02	First patients arrive at the MFH	The MFH is set and operational, first patients incoming	Treatments are provided, patients are being taken care of, the virus is slow down
29/08/2021	-	Cyberattack	MFH assets targeting	-
29/08/2021	8h23	Inject 1	MFH Stakeholders receive an email to change their passwords.	Stakeholders inform their superior and don't do the request

			The email seems to be a gouv. asking to change id/password for security	
29/08/2021	9h02	Password stealing	A nurse clicks on the fake link in the email and enters his/her password	Stakeholders inform their superior and don't do the request
06/09/2021	9h47	Physical intrusion in the MFH	Someone disguised as an IT employee (BadGuy) comes in the MFH	Better access control of the MFH and numeric equipments
06/09/2021	9h49	Accessing the computer	The BadGuy goes to a computer during an emergency (so they not notice him)	Better access control of the MFH and numeric equipments
06/09/2021	9h50	Login	The BadGuy logins to the computer with the id+password he stole before (29/08)	Better access control of the MFH and numeric equipments
06/09/2021	9h51	Inject 2	The BadGuy connects an USB key to the unlocked computer and injects the virus in the networks	The computer detects the infected device and directly puts itself in standby to avoid jeopardizing the whole facility
07/09/2021	02h36	Asking for a ransom	After a day, data are encrypted, hacker asks for 50k€ within 24h in bitcoin (1.10 bitcoin) to have the decryption key	IT try to solve the problem
08/09/2021	02h36	MFH don't pay	The government don't want to fund cyberterrorism, crime and because there is no certainty that the data will	IT try to solve the problem

			be unlocked	
09/09/2021	02h36	Data are lost, critical patients are transferred to other Hospitals	The government prepare the evacuation of patients to the continent	Italia, Spain help France to redistribute patients in hospitals
09/09/2021	10h07	Arrival of media	Media professional ask questions about MFH choices, lack of cybersecurity ..ect	Senior executive must handle the situation, be confident
16/09/2021	14h58	MFH recover their data basa	MFH recovers some data and add others in order to continue to work	MFH add firewalls/cyber resilience to their informatic system to be more secure

IMT Mines Alès
École Mines-Télécom

Timeline for the second scenario

Date	Time	Event	Description	Expectation
07/03/2022	08h15	Tsunami sweeps over Samoan Coast	samoa is largely submerged and power grids cut	Fastest and most efficient recovery possible
07/03/2022	10h02	National state of emergency	Samoan government announces a national state of emergency, lot of public building are nonfunctional	Fastest and most efficient recovery possible, need some help
12/03/2022	14h31	Escrim MFH arrives from France	Samoan Island need MFH because their hospitals are nonfunctional and there are lot of wounded people	The MFH is correctly deployed and is to accept patients
14/03/2022	8h02	First patient admit in a escrim MFH	The MFH is set and operational, first patients incoming	Treatments are provided, patients are being taken care of, the virus is slow down
20/03/2022	-	Pre-attack	MFH assets targeting	-
29/03/2022	8h11	Intrusion	An intruder (Mr.H) comes near the MFH with a PC and a antenna, no one remarks him (in a little truck)	Stakeholders remark the intruder and inform the security team
29/03/2022	8h15	Disconnection of the devices	He disconnects 1 or 2 devices that are already connected to the wifi	The device automatically

				reconnects to the wifi
29/03/2022	8h16	Password stealing	When the device (removed of wifi) tries to reconnect itself to the network, Mr.H is “listening” and can access the wifi’s password	The password can be accessed by people like Mr.H
29/03/2022	8h17	Connection to the wifi	Now that he is the password, Mr.H can connects himself to the wifi	The network spots Mr.H and sends an alert signal
29/03/2022	8h20	Overflow of data	In order to DoS the MFH’s network, Mr.H sends a huge amount of data to the MFH devices to sature one or several electronic devices through wifi	The network spots Mr.H and sends an alert signal
29/03/2022	8h23	Inject 1	There is a system crash, website can’t be used	IT try to figure the problem, if patients are in danger they are sent to other hospitals
30/03/2022	11h56	Access Recovery	Website access is back	IT find the breach and adapt the wifi protection
30/03/2022	13h	Inject 2	There is a system crash, MFH computers can’t be used	IT try to figure the problem, if patients are in danger they are sent to other hospitals
30/03/2022	15h56	Access Recovery	Network access is back	IT find the breach and adapt the wifi protection

TTX's answers of scenario 1 :

	Medical Personnel/ Reception Officer	Information Technology Officer	Chief Medical Officer/ Head of mission	Public relations Officer
What do you know about Phishing and Ransomwares	Phishing? Ransomware is like a virus that blocks data in exchange for a ransom?	use personal to have informations Hack a infrastructure then ask for money (more used in hospital hacking)	Phishing is a way to steal information, it can be ID/password for anything, ransomware is a virus that encrypts your data and then asks for a ransome to decrypt your data.	From reports in the media, I am aware of the basic details and techniques used in this attack, and some victims too.
What assets are really sensitive to cyber attacks	electronic devices connected to the internet (computers?) but also some medical equipment that we use (scanners and that)	ventilator respiratory, ecg, pc, IoT, EHR/EMR	medical devices, the medical software (EHR), the alimentation (electricity, oxygen…)	the network and the people (medical personnel)
Receive a mail from a .gouv to change your id and password. Do you open it or/and report it to someone ?	maybe maybe not cannot say I think I would be a little suspicious but I think I wouldn't report it	depends of the form of the email, i'm not reporting it	I don't know but I would feel weird about it.	I will click on it and change the id and password. This is simply because it is from a ".gouv" website which I think is maybe genuine.

As an IT how can you check that is not a fake mail ?	finding the location with IP address or smth like that	Check the email source, try to focus on the pictures, the way the e-mail si written	Check the real address of the email because I know you can change it but only as a front	by checking the email sender, and the domain (for example the ".gouv" domain). Also by checking the content to see if there are mistakes and any malicious messages included.
What are you watching in the mail to check if the source is clean	I think I would look at the link more precisely to see if it's like a website address I know or I would trust	same that before	I would check the sender and then I would check if there is anything weird on the mail like an orthographe mistake	I can also check to see if the mail has attachments, and if I am not expecting any mails from the sender. Other reasons are the same as Q2 answers.
Evaluation of the situation	1	1	1	1
An unknown person enters in the MFH : How do you prevent someone from entering in the MFH ?	maybe some badges to access certain areas in the mfh	it needs some securities in the mfh, i don't know everyone so i can't know if he is a stranger	I think we should have security checking everyone's badge but it would be difficult and could lose time, more importantly in the case of an emergency	There should be a security at the entrance of the MFH that can identify the MFH personnel allowed access into the facility, by using a list or the ID cards checked before access. the unknown persons should be reported immediately when

				sighted.
The stranger connects to a PC : Do you ask questions to the stranger who logs in to the server ? Do you consider it a threat	depends on what this person look like (if it's a patient I would question it)	if i never seen him, i would think that is strange and i would ask the reception officier about him, i consider him as a threat	I know the medical staff but not all, if someone disguised as an IT person logs in to the computer I wouldn't consider it a threat	Yes, and Yes. You have to ask questions about why he is plugging a device (because he is a stranger). and Also it is considered a threat if it is carried out by a stranger.
Are they precious data that can be accessible from the PC ? What can be his motivations ?	Clearly money that's why it's called ransomware I think- I don't think that the blood type of Mrs Hendry is useful to anyone	record of patients, about the drugs they take, sensible information about them. It's for money or he hates someone	All the records of the patients, access to medical devices, all the medical data, the software used by machines, access to the system. Motivation: It could be money or other	Yes, there is sensitive data/information available on the PC such as EHR/EMR, medical related data, some personal data and network information data. His motivations I think is to steal some of this category of data out of the MFH PC in order to use it for malicious purposes.
The stranger connects a USB key at the server : Do you consider connecting a USB key to a computer a normal thing ? Even by strangers	USB keys are meant for computers, I'm not sure I would notice it because it's normal	yes it's serious, the one who does that can insert a malware in it. If I know the person I would thinks it's normal but I might ask him the question why hé	Connecting USB key is a totally normal thing, but it can be a real disaster in this type of scenario, if I saw someone I don't know connecting a USB key to a computer I would	This is not a normal thing especially for a stranger, but normal for MFH personnel. This can be prevented by either using extra login for USB connections, or

? As an IT person , how can you prevent that ?		is doing that	have ask him what he is doing	disabling USB ports on the PC.
As an IT person , how can you prevent someone from connecting a USB key easily to a MFH PC ?	If it's a total stranger maybe ask him his role there, check if it's true then react to the answer he gives	put a cadena or something like that to prevent that a stranger put a malware in the system	You'd need to put some kind of login when you connect a USB key	by either adding login requirements for USB connection, or disabling the USB ports on the PC.
Evaluate the situation	2	4	3	2
Data is not accessible anymore : Do you try to figure out how to solve the problem ? How much time do you try before calling someone else ?	I would try 2 or 3 times and if it's look still weird, I'll call the IT gum guy	as an it i try to figure the problem on my Own during 5min then I call my colleagues to have help, if we don't figure it, i inform the chief medical officer	I don't try to figure this out because some are more qualified than me. After 3 hours I would call someone else for help	I will call the IT Officer to try to resolve the problem. If not resolved in time and the MFH processes is affecting patients, we will escalate the issue to the Head of Mission to take a decision on payment or not.
Demanding Bitcoin to return the Personal Health Information (PHI). Do you decide to pay?	surely don't pay and find the best ways to recover while always providing care to the patients who need it	depending on the amount, but i will pay because if these data are in the nature it will be a disaster	I don't want to pay but we have to be able to work so I would pay I think	I will try to check with the effort of the IT officer, and also discourage the Head of mission not to pay, and find another solution, maybe getting more help from a third-party.

You don't have access to EHR anymore, what do you do with data that patients give you ?	pen and paper, and excellent communication within the team as always But I won't stand there doing nothing while looking for a more viable solution, our main goal is to take care of the patients !	pen and paper, try to organize them with classeurs	I will try to find the best way to continue to work with pen and paper and be faithful to the way we usually work so that it will be easy to report the data on the system when he's up	i will check advice the medical personnel to use the physical filing (pen and paper) manual method, while the issue is still pending
Evaluate the situation	4	4	4-5	4
According to the grade you gave to the situation, how do you plan to solve the problem?	I think medical staff would continue to provide the more urgent cares, but working old-fashioned I think the IT staff would look for a solution to get the data back without paying nor jeopardise anything else I think the head of operations would think of how to recover and transport the	I would ask the help of everyone in my service, it's the most important thing to do. I will work in coordination with the chief medical officer to inform him about the advancement of the IT. Ask help to others mfh which had the same problem	I would ask help from the government, other hospitals, other countries in order to dispatch as more as I can all the patients for them to be treated somewhere else so that we (medical staff) can manage less patient in the MFH with the working system that we chose	I plan to advise the IT officer to use any backup available to restore the systems. If this is not available, i will advise the Head of mission not to pay and use a manual method of records.

	patients that need care that can't be given here			

TTX's answers of scenario 2 :

	Medical Personnel/ Reception Officer	**Information Technology Officer**	**Chief Medical Officer/ Head of mission**	**Public relations Officer**
What do you know about wifi hacking and DDOS ?	???	needs an antenna, hacker need to be near the wifi, you can use the force for password or disconnect someone and listen Ddos send lot of informations so there is a crash in the system	with wifi attacks you can get the adresse from the wifi to be able to connect to it, DoS is when you send a lot of request to a website to crash it	very little, only from the report on tv and the media
Can you imagine three reasons for an attack on a MFH (from a hacker point of view) ?	- money - challenge - ideology	money, politic, personal reason (he hates the director, he doesn't like how they treat their patients)	to get medical information because they have a huge value on the balck market	- for selling the data on dark web (financial), -to damage the reputation of the MFH, -to disrupt the activities of the MFH
You see a stranger near the MFH with a laptop. Can he be a threat for the MFH ?	No	yeah might be, but i'm not sure about his intentions	No, I don't consider him a threat	maybe, depending on what he is doing, but normally he is not a threat.

Medical Personnel remark that a MFH printer is disconnected from the wifi. Do you reconnect it immediately ? Can you know if it's a hacker that has disconnected the asset ?	I'll wait maybe it will reconnect itself in a few seconds If not, rebooting it If still nothing let's call IT	yes i reconnect it Don't know I ask to my colleagues	Yes I would reconnect it immediately without asking question I cannot know if it's a hacker that has disconnected my device.	Yes, I will suggest reconnecting it. I can not know if it is a hack or not.
You want to reconnect the printer on the wifi. What would you do to not be listened to by the hacker ? Can you know if a hacker is listening to the wifi ?	???	don't know at all	I don't know anything	I don't know how to reconnect without listening or not.
Sometimes later you remark that the printer is connected to the wifi but you haven't done anything. How can you know that a stranger PC is connected to the Wifi ?	I can't know for sure	don't know	I think you can manage to see every devices connected to the wifi but I don't know how	I have to ask the IT officer for this
The Website is not accessible	a what?	it must be that	I would think it's a bug, not an attack	i have to ask the IT officer

anymore, how can you know it's a DDOS attack ?				
Some patients complain about it, what solution do you have to help them?	if there is no information available there is no data	i send them to the reception officer so they can have all the informations they need	Some brochure papers	i will refer the to the IT officer, and suggest to him to solve the problem
What possibilities have you to restore the website ?	ask the IT department ...	can reload the wifi, change the password	I would ask an IT person	maybe suggesting to restart the web server, or the web pages
The public opinion says your cybersecurity isn't efficient. How can you protect MFHs website from this type of attack ?	that's a question for an IT guy I don't have a clue	buy a better software against virus	You can improve your servers, there must be some firewalls to help prevent many people from sending data to your website. A system that detects when there is a suspicious amount of data at the same time.	I will try to convince the IT officer and the head of mission to upgrade the security such as login credentials encryption and using more modern firewalls. And also train the MFH personnel on how to detect basic cyberattacks.
Evaluate the situation	2	2	2	3
Computers are not accessible : How to react to a DDOS attack on computers ?	disconnect it from the wifi?	reboot everything (wifi and assets) change wifi password, need to inform the chief medical officer that it	I would reboot the system	i will report to the iT officer immediately

		will take time and we need solutions to take care of patients		
The chief officer blames the IT because there is a fault in the cybersecurity. How do you prevent this type of attack ?	Safier wifi?	it's hard to do, the best is to prepare the staff in this type of situation. The wifi needs the best security possible	I don't know	no idea
You have to continue to treat patients even if computers and IoT are unusable. What do you do to continue to collect patients data ?	use the available equipments and take notes with pen and paper	pen and paper	pen and paper	using the manual method, pen and paper
There are hundreds of patients in the MFH and you have to know fastly which are in danger. How do you detect them quickly?	normally the staff already know the situation of the people that are in a critical state Moreover, we need to identify within the others patients that are not taken in charge, quickly identify them and sort them by need/treatments	mfh needs a color code for each patient, it's necessary for them, see with chief medical officer	An emergency team to see patients early and to give an early diagnostic of patients before we really treat them, that way we can detect the most endangered ones	i have no idea, i will contact the chief medical officer and the medical personnel

How can you ensure patients safety without a PC/IoT ?	Providing care to the people in need, evaluate the possibility of fast transport if necessary	see with chief medical officer	Evaluate the situation of most of the patients and if necessary to transfer them to other hospitals to be treated	consult the medical personnel and the IT officer for this
Evaluate the situation	4	4	4	4
According to the grade you gave to the situation, what do you plan to solve the problem?	I think medical staff would continue to provide the more urgent cares, but working old-fashioned, by prioritising the different needs of patients I think the IT staff would look for a solution to get the wifi and assets back to normal I think the head of operations would think of how to recover and transport the patients that need care that can't be given here	I need to work in a team with the chief medical officer and the reception officer. The best thing first is to have the best wifi security and to be prepared for these types of attacks. Need to work with my colleagues to defend the mfh against ddos attack that can be a real threat for patients.	I would ask for help, the more I can find the better. It's a really difficult situation. The medical staff should continue to provide medical care to the patients. See with the IT person how to reboot the system, to see if the system will be down for a long time or not and adjust the response accordingly	i would advise the IT officer to consult with the medical personnel to come up with a good idea to solve the issue

Penetration Testing Frameworks and Methodologies	What is it ?
Open Source Security Testing Methodology Manual (OSSTMM)	-contains a comprehensive guide for testers to identify security vulnerabilities within a network -allows testers to customize their assessment -created to support network development teams -methodology relies on the tester's knowledge and IA
Open Web Application Security Project (OWASP)	- helped organizations to curb application vulnerabilities -the guide provides comprehensive guidelines for each penetration testing method
The National Institute of Standards and Technology (NIST)	-offers specific guidelines for penetration testers to follow -guarantee information security -tests on applications and networks
Penetration Testing Methodologies and Standards (PTES)	-highlights the most recommended approach to structure a penetration test -guidelines to perform post-exploitation testing -practical recommendations that management team can rely on to make decisions
Information System Security Assessment Framework (ISSAF)	-contains an even more structured and specialized approach to penetration testing -enable a tester to meticulously plan and document every step of the penetration testing procedure - complementary information, various vectors of attack, as well as possible results when a vulnerability is exploited

Frameworks Review	What is it ?
The National Institute of Standards and Technology (NIST)	-offers specific guidelines for penetration testers to follow -guarantee information security -tests on applications and networks
CIS Critical Security Controls	- a set of 20 actions designed to mitigate the threat of the majority of common cyber attacks
ISO 27001	-international standard that describes best practice for implementing an ISMS (information security management system) -demonstrates that your company is following information security best practice, and delivers an independent, expert assessment of whether your data is adequately protected
PCI DSS	-governs the way credit and debit card information is handled -applies to any organization