THREATS

Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

How to protect a hospital against cyber attacks

A. Guinet

Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union

THREATS
Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

Context

- A study published by the Institute for Critical Infrastructure Technology in 2016, specifies that 72% of the US health care societies have been targeted by cyber attacks during 2012. 47% of the US people which accessed to the health care system have been victims of corrupted medical data, due to hackers.

- On May 2017, at least 16 hospitals in the United Kingdom are being forced to divert emergency patients after their computer systems were infected with the ransomware “Wannacry”, a type of malicious software that encrypts the victim’s documents, images, music and other files unless the victim pays for a key to unlock them.

- In 2009, the Carrell Clinic in Dallas (Texas) suffered a computer intrusion, the hacker installed malicious software all over the Carrell Clinic, including the systems that contained confidential information, and others systems which controlled the buildings' air-conditioning.

THREATS
Terrorist attacks on Hospitals:
Risk & Emergency Assessment, Tools & Systems

Outline

- The cyber attack sources,
- The cyber attack approach,
- The Information system mapping as a tool,
- The critical assets,
- The critical asset attractiveness,
- The threat scenarios,
- The scenario assessment from the information system mapping.

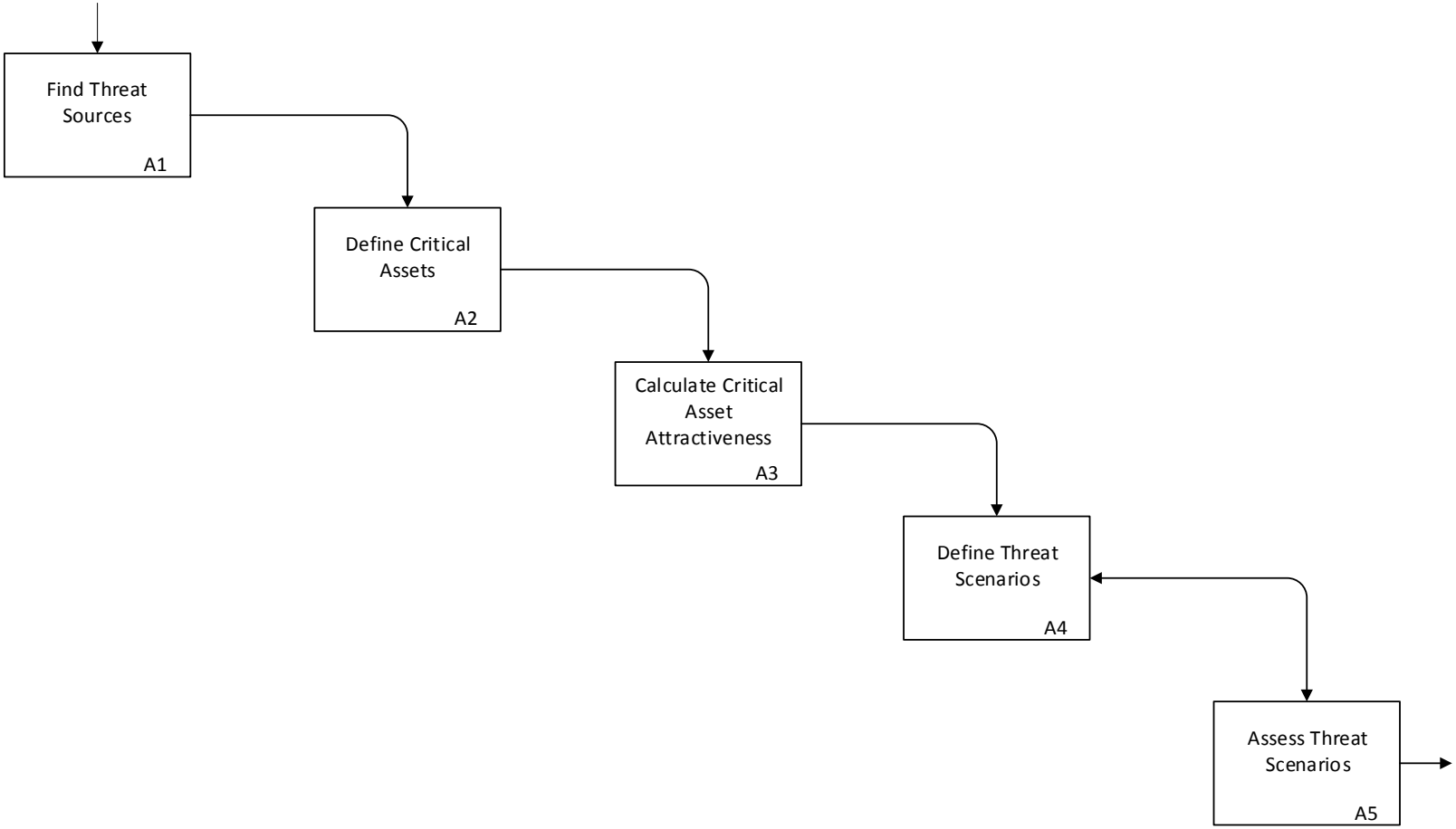
The Cyber Attack Sources

- Hacktivists try to make propaganda by obtaining media attention in order to promote their values. These hackers can also act for enjoyable reasons. Cyber attacks from hacktivits are disruptive. The most common hacktivist attack is a denial of service (DDoS) attack.

- The main terrorist objectives are to spread terror and to kill people. Terrorists try to cause violence and damage, in order to destabilize the hospital and the patients. Cyber attacks from terrorists are destructive. The different forms of cyber attacks are: espionage, theft, sabotage and personal abuse.

- Cyber criminals try to generate profit through the exploitation or through the racketeering of hospital data or patients' data. Cyber attacks from criminals can be disruptive or destructive. The most common criminal attack is the ransom-ware attack, which encrypts files in an information system.

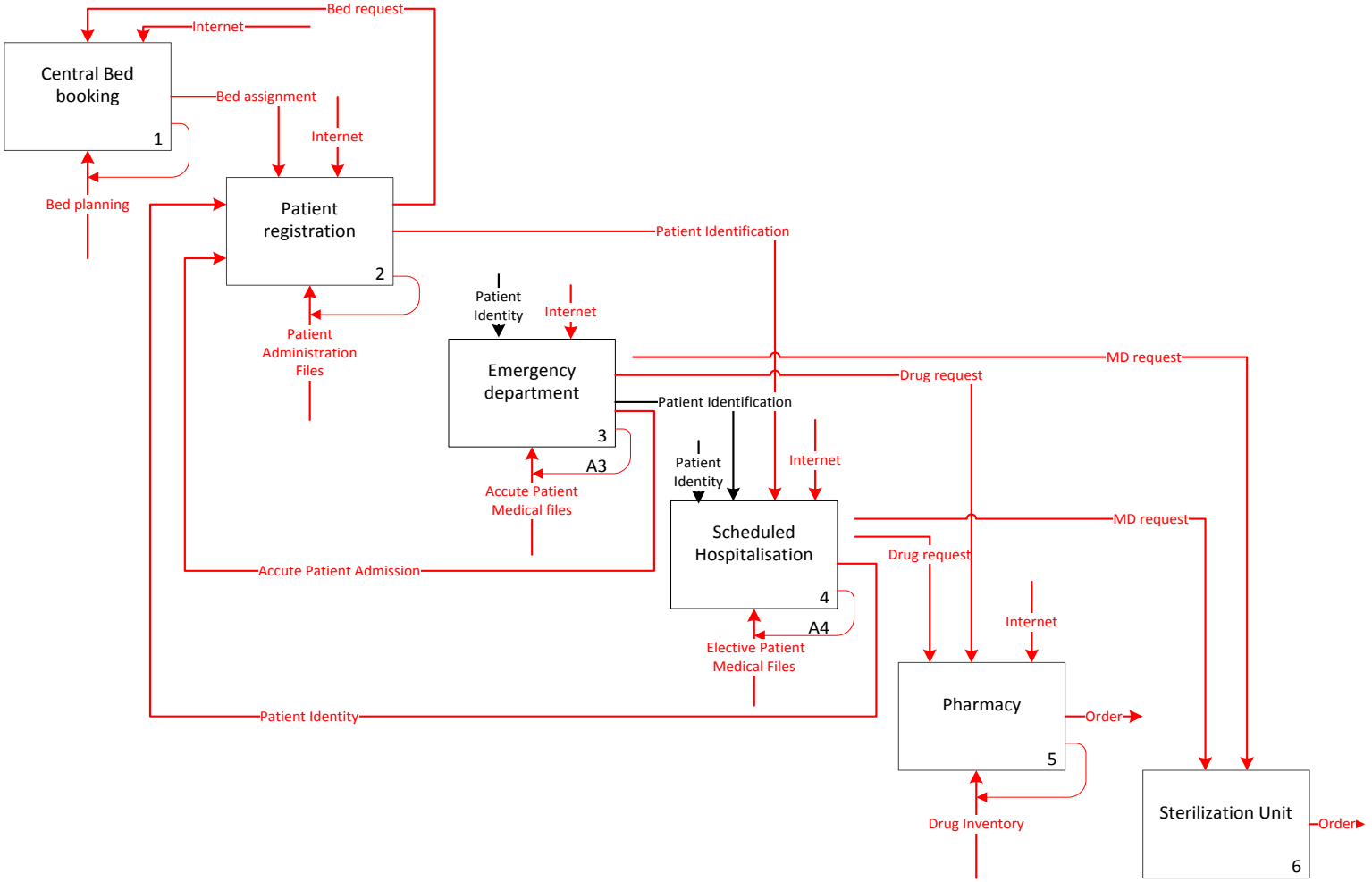
The Cyber attack approach (1/2)



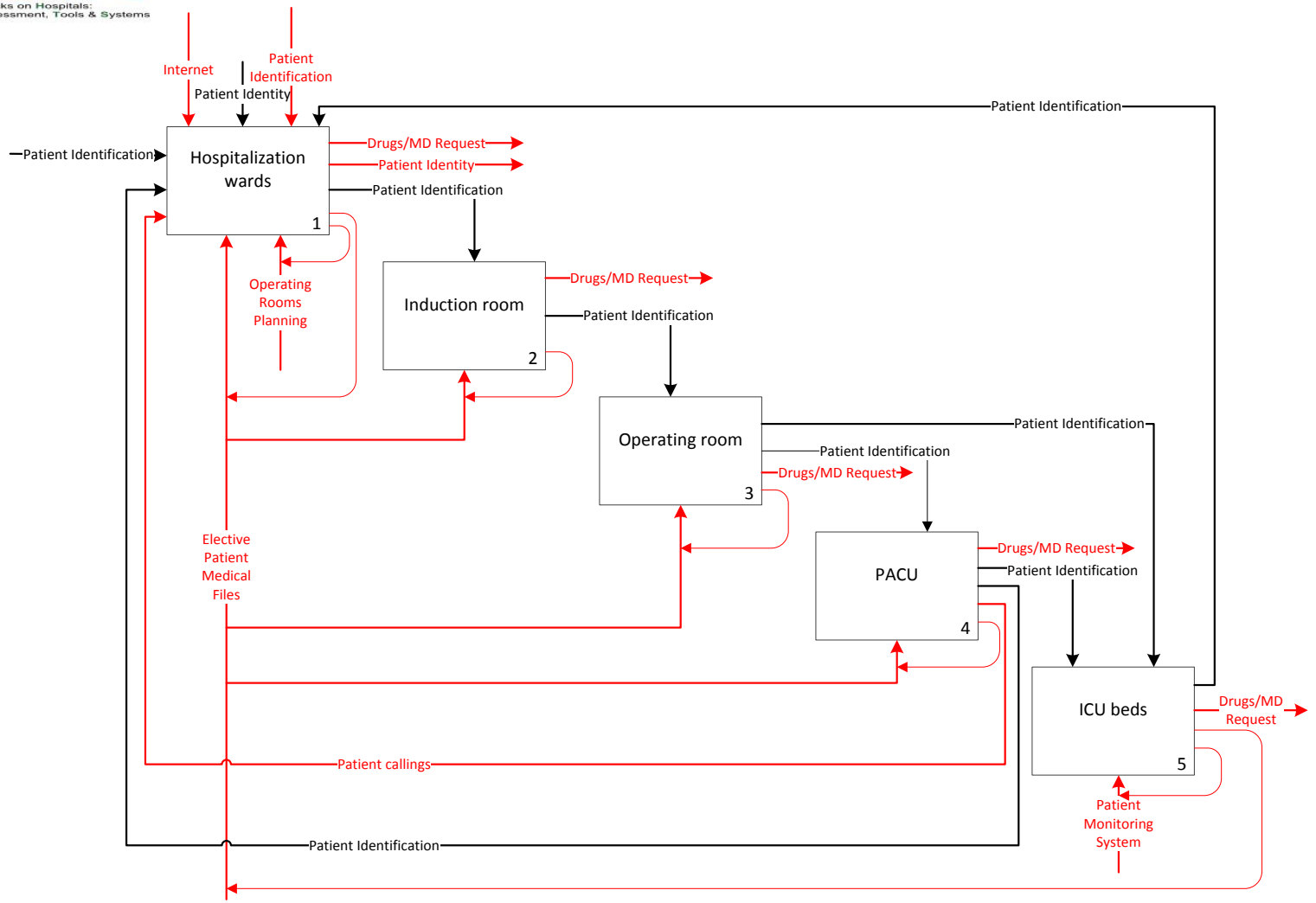
The Cyber attack approach (2/2)

- Find the threat sources: Reviewing historical data on cyber attacks, we specify the adversary profile, their potential actions, their capabilities, and their motivation.
- Define critical assets: Identifying the care units which use digital information, we locate the critical assets regarding to their contribution to the information system. An IDEFØ model enables us to map the critical assets.
- Calculate critical asset attractiveness: Realize an analysis based on pairing of each critical asset and of each threat source, in order to identify potential vulnerabilities per adversary.
- Define Threat Scenarios: Based on the attractiveness of the critical assets per adversary, the most likely scenarios with the worst consequences are constructed.
- Assess Threat Scenarios: scenarios are studied to evaluate their consequences, to propose possible counter-measures implementation in order to reduce the risk to an acceptable level. A transitive closure of the information system map with a mixed integer linear program is proposed to help the decision maker.

The Information system mapping



The Information system mapping



The Information system mapping

	A1	A2	A31	A32	A33	A34	A35	A36	A41	A42	A43	A44	A45	A5	A6
A1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0
A31	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0
A32	0	0	1	1	1	0	1	1	0	0	0	0	0	1	1
A33	0	0	1	1	1	0	1	1	0	0	0	0	0	1	1
A34	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
A35	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0
A36	0	0	1	1	1	0	1	1	0	0	0	0	0	1	1
A41	0	1	0	0	0	0	0	0	1	1	1	1	1	1	1
A42	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A43	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A44	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A45	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
A5	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
A6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

The Critical Assets

- Emergency department and scheduled hospitalization: The patient medical files from emergency and hospitalization wards are collections of personal data about patient diagnosis, patient treatments, patient laboratory tests, medical reports, etc.

- Patient registration: The patient administrative files managed by the patient registration unit contain information about personal data (names, addresses, phone number, bank details, etc), insurance identification, relatives' information...

- Intensive care unit: The patient monitoring system of ICU supervises the oxygen/drug supply to patient requiring intensive cares. The blood pressure, the heart rate, the ECG signal, etc., are vital parameters which are monitored and can trigger nursing/physician alerts.

The critical asset attractiveness

Critical assets	Hacktivists	Criminals	Terrorists
Scheduled hospitalisation (Elective patient medical files) and Emergency department (Acute patient medical files)	The identification of patients requiring an abortion or of the surgeons practicing abortion, and the diffusion of such information on social networks could be a goal of hacktivists.	The patient medical files contain confidential information about patient test results and patients' treatments. Such information can be sold to malicious financial companies.	Patients suffering from AIDS, could be identified by terrorists, and could be individually targeted by further criminal actions. Patient's blood types can be changed to mass casualties.
ICU beds (patient monitoring system)	The hacktivists could inform people about the lack of security for patients in a given hospital, such as unprotected equipment i.e. without password or encrypted data.	The patient monitoring system could be hacked to kill a VIP in an ICU bed, by a false drug dosage or inadequate ventilation, the VIP being in the most vulnerable state.	The patients monitoring system could be hacked to kill the patients in their ICU bed. Such cyber attack could bring media attention and terrorize people.

The threat scenarios

- An employee has been recently fired. He/she approaches a hacker and he convinces him to destroy the hospital network by encrypting the servers. The hacker inserts a worm to get the network node plan, then she/he remotely jeopardizes the network introducing crypto-lockers.

- An important politician is in a surgery unit. He/she has just favored in Parliament the approval of a law in favor of the abortion/euthanasia. A criminal paid by domestic terrorists, infiltrates the hospital information system, and next jeopardizes the patient monitoring system of ICU beds. After the surgery the Politician requires an ICU bed. The politician is killed by disruption of ICU monitoring system that has been compromised (drug dosage and/or ventilation).

The scenario assessment from the information system mapping (the transitive closure)

	A1	A2	A41	A42	A43	A44	A45	A31	A32	A33	A35	A36	A34	A5	A6
A1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	0	0
A2	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	0	0
A41	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	1	1
A42	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	1	1
A43	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	1	1
A44	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	1	1
A45	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0	0	0	0	1	1
A31	0	1	0	0	0	0	0	**1**	**1**	**1**	**1**	**1**	0	0	0
A32	0	0	0	0	0	0	0	**1**	**1**	**1**	**1**	**1**	0	1	1
A33	0	0	0	0	0	0	0	**1**	**1**	**1**	**1**	**1**	1	1	1
A35	0	0	0	0	0	0	0	**1**	**1**	**1**	**1**	**1**	1	0	0
A36	0	0	1	0	0	0	0	**1**	**1**	**1**	**1**	**1**	0	1	1
A34	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0
A5	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0
A6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**

The scenario assessment from the information system mapping (MILP: The data)

- N: number of system components,
- K: the minimum number of partitions,
- c (i,j): it is equal to 1 if system component i is linked as input with system component j (the IDEFØ matrix after its transitive closure),
- d (i): potential damage of critical asset i when corrupted (disruption of activity, data restoration) in euros,
- w (i,j): data traffic from the system component i to the system component j, expressed in working hours to evaluate the potential loss of digital traffic over a given horizon, in euros.

The scenario assessment from the information system mapping (MILP: The variables)

- X (i,k): this binary variable is equal to 1 if i is assigned to partition k and 0 otherwise,
- Y (k): this binary variable is equal to 1 if at least one node has been assigned to partition k,
- Loss (i,j): real variable, the link from i to j is deleted and it results a loss of w (i,j) traffic,
- Dmax: real variable, maximum damage of a partition when corrupted.

The scenario assessment from the information system mapping (MILP: The partitioning)

$$Minimize\ (Z) = \sum_{i=1}^{N} \sum_{j=1}^{N} Loss\ (i,j) \quad + \quad Dmax \quad (1)$$

We minimize the losses of traffic knowing that partitions are not linked, and the maximum damages to a partition. We hypothesize one attack over the studied horizon to only one partition instead of the entire information system.

Constraints:

$$\sum_{k=1}^{N} X\ (i,k) \ = \quad 1 \quad \forall\, i = 1, \dots, N \quad (2)$$

A system component i must belong to one and only one partition.

$$X\ (i,k) + \ X\ (j,k) - \ 1 \ \leq \quad c\ (i,j) \ \forall\, i,j,k = 1, \dots, N \quad (3)$$

A pair of system components i and j belonging to the same partition, must exchange traffic.

The scenario assessment from the information system mapping (MILP: The number of partitions)

$$\sum_{i=1}^{N} X(i,k) \leq N * Y(k) \quad \forall k = 1, \ldots, N \quad (4)$$

$$\sum_{i=1}^{N} X(i,k) \geq Y(k) \quad \forall k = 1, \ldots, N \quad (5)$$

$$\sum_{k=1}^{N} Y(k) \geq K \quad (6)$$

A partition must contain at least 1 system component. We count the number of partitions which must be greater than K.

The scenario assessment from the information system mapping (MILP: The criteria calculation)

$$Loss\,(i,j) \;\geq\; w\,(i,j) * X\,(i,k) - w\,(i,j) * X\,(j,k) \;\; \forall\, i,j,k = 1,\dots,N \quad (7)$$

$$Loss\,(i,j) \;\geq\; w\,(i,j) * X\,(j,k) - w\,(i,j) * X\,(i,k) \;\; \forall\, i,j,k = 1,\dots,N \quad (8)$$

The calculation of loss of traffic is done taking into account the links between system components belonging to different partitions.

$$\sum_{i=1}^{N} d\,(i) * X\,(i,k) \;\leq\; Dmax \;\; \forall\, k = 1,\dots,N \quad (9)$$

The calculation of the potential damages is done. The maximum damage is sought.

The scenario assessment from the information system mapping (MILP: The results)

Partition	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Total
A1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A31	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
A32	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
A33	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
A34	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
A35	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
A36	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
A41	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A42	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A43	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A44	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A45	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
A5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
A6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1
Total	**0**	**5**	**0**	**0**	**1**	**1**	**0**	**7**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**15**

The scenario assessment from the information system mapping (after partitioning)

- Regarding the revenge scenario, the hacker has to steal the authentication and the identification of five employees who have an authorized access to the five sub-systems, in order to corrupt the whole system. If the fired employee has still an access to one of these sub-systems, the ransom-ware attack is limited.

- Regarding the murdering scenario, the patient monitoring system of ICU belongs to a critical asset (scheduled hospitalization) which includes two kinds of data: SCADA data and elective patient medical files. Both data could be corrupted to kill the VIP, the medical prescription or the SCADA parameters. If we can isolate the patient monitoring system of ICU to an independent sub-system, then the SCADA data is no more connected to elective patient medical files and transmitted infections disappeared.

Conclusion

- We have proposed an approach to assess the vulnerability of hospitals against cyber attacks, It is supported with tools.
- We suggest defining the critical assets of information system in terms of units/services.
- The attractiveness of critical assets is specified per adversaries. The modelling support to find the weaknesses is a map resulting from an IDEFØ analysis.
- Some scenarios are studied, and the consequences of cyber attacks are analysed thanks to the information system map.
- By calculating the partitioning of the information system, we can propose mitigation countermeasures (rules 21 and 22 of the 40 essential measures for a healthy network, ANSSI).
- A mixed integer linear program has been modelled to find the best set of sub-systems for the hospital information system, by minimizing losses of digital traffic between the independent sub-systems and contamination damages by belonging to the same sub-system.

Discussion

Thanks for your attention