

# Information Risk Management: An Example of healthcare Domain

Salimeh Dashti, Paolo Giorgini and Elda Paja  
University of Trento, Italy,  
salimeh.dashti@studenti.unitn.it,{elda.paja,paolo.giorgini}@unitn.it

## Contents

Introduction	4
Textual Description of the Scenario	4
Modeling with STS – tool	4
Social view	4
Social View Diagram	5
Asset View	6
Asset View Diagram	7
Asset Evaluation Tables	8
Social View After Asset Classification	17
Authorization View	19
Authorization View Diagram	20
Authorization Property	21
Threat View	23
Threat View Diagram	23
Likelihood tables	25
Threat View Diagram Together with the Scales	32
Risk Evaluation- Using Risk Evaluation Matrix	34
Analysis.	38
Risk Assessment	38
Security and Threat Analysis Result	40

## Table of Figures

FIGURE 1- SOCIAL VIEW FOR THE HEALTHCARE EXAMPLE.....	5
FIGURE 2- THE ASSET VIEW OF THE HEALTHCARE EXAMPLE. ....	7
FIGURE 3. ASSET EVALUATION TABLE OF INFORMATION PERSONAL DATA .....	8
FIGURE 4. ASSET EVALUATION TABLE OF INFORMATION PRESENT ILLNESS .....	8
FIGURE 5. ASSET EVALUATION TABLE OF INFORMATION ALLERGY .....	9
FIGURE 6. ASSET EVALUATION TABLE OF INFORMATION MEDICAL HISTORY.....	9
FIGURE 7. ASSET EVALUATION TABLE OF DOCUMENT MEDICAL RECORD .....	10
FIGURE 8.ASSET EVALUATION TABLE OF DOCUMENT REGISTRATION RECORD .....	10
FIGURE 9.ASSET EVALUATION TABLE OF INFORMATION BLOOD NEEDS.....	11
FIGURE 10.ASSET EVALUATION TABLE OF DOCUMENT BLOOD USAGE LISTING .....	11
FIGURE 11.ASSET EVALUATION TABLE OF INFORMATION BLOOD TYPE .....	12
FIGURE 12. ASSET EVALUATION TABLE OF INFORMATION BLOOD INFO .....	12

FIGURE 13.ASSET EVALUATION TABLE OF DOCUMENT BLOOD BANK .....	13
FIGURE 14.ASSET EVALUATION TABLE OF DOCUMENT REPORT .....	13
FIGURE 15.ASSET EVALUATION TABLE OF INFORMATION HEALTH RECORD .....	14
FIGURE 16.ASSET EVALUATION TABLE OF INFORMATION PERSONAL INFORMATION.....	14
FIGURE 17.ASSET EVALUATION TABLE OF INFORMATION MEDICAL HISTORY INFO.....	15
FIGURE 18.ASSET EVALUATION TABLE OF DOCUMENT HEALTH RECORD .....	15
FIGURE 19.ASSET EVALUATION MATRIX OF DOCUMENT DONOR CERTIFICATE.....	16
FIGURE 20.ASSET EVALUATION MATRIX OF DOCUMENT TEST RESULT .....	16
FIGURE 21- SECURITY REQUIREMENTS ACCORDING TO VALUES HAS ASSIGNED .....	18
FIGURE 22-FIGURE 2- THE AUTHORIZATION VIEW OF THE HEALTHCARE EXAMPLE.....	20
FIGURE 23. HOSPITAL-PATIENT AUTHORIZATION PROPERTY.....	21
FIGURE 24-EMMA-MODERN LAB AUTHORIZATION PROPERTY .....	21
FIGURE 25-EMMA-RED CROSS BTC AUTHORIZATION PROPERTY .....	21
FIGURE 26-PHYSICIAN-RED CROSS BTC AUTHORIZATION PROPERTY.....	21
FIGURE 27-HOSPITAL- PHYSICIAN AUTHORIZATION PROPERTY.....	21
FIGURE 28- EMMA-PHYSICIAN AUTHORIZATION PROPERTY .....	21
FIGURE 29-ALICE-PHYSICIAN AUTHORIZATION PROPERTY .....	22
FIGURE 30-ALICE-HOSPITAL AUTHORIZATION PROPERTY .....	22
FIGURE 31-THREAT VIEW (I) .....	23
FIGURE 32-THREAT VIEW (II).....	24
FIGURE 33-ALICE LIKELIHOOD TABLE.....	25
FIGURE 34- MODERN LAB LIKELIHOOD TABLE .....	25
FIGURE 35-RED CROSS BTC LIKELIHOOD TABLE .....	26
FIGURE 36- PATIENT LIKELIHOOD TABLE.....	26
FIGURE 37- HOSPITAL LIKELIHOOD TABLE .....	27
FIGURE 38- PHYSICIAN LIKELIHOOD TABLE .....	27
FIGURE 39. BLOOD BANK-REGISTRATION RECORD .....	28
FIGURE 40.TEST RESULT - HEALTH RECORD .....	29
FIGURE 41.TEST RESULT .....	29
FIGURE 42. MEDICAL RECORD .....	30
FIGURE 43.TEST RESULT .....	30
FIGURE 44. BLOOD BANK.....	31
FIGURE 45-THREAT VIEW(I)- SCALES ASSIGNED.....	32
FIGURE 46-THREAT VIEW(II)- SCALES ASSIGNED .....	33
<i>FIGURE 47. HOSPITAL – DOCUMENT REGISTRATION RECORD.....</i>	34
FIGURE 48- HOSPITAL BANK RISK EVALUATION MATRIX .....	34
FIGURE 49HOSPITAL- DOCUMENT BLOOD BANK.....	34
FIGURE 50- PHYSICIAN RISK EVALUATION MATRIX.....	35
FIGURE 51 MODERN LAB RISK EVALUATION MATRIX .....	35
FIGURE 52- PATIENT RISK EVALUATION MATRIX .....	36
FIGURE 53- RED CROSS RISK EVALUATION MATRIX .....	36
FIGURE 54-RISK EVALUATION MATRIX.....	37
FIGURE 55- IMPROVEMENT /ADDED SECURITY REQUIREMENTS TO THE SOCIAL VIEW AS TREATMENT .	39
FIGURE 56.PROPAGATION OF VIA TRANSMISSION AND THEIR IMPACT ON ACHIEVING GOALS .....	40
FIGURE 57, PROPAGATION VIA DOCUMENT/INFORMATION STRUCTURE.....	41
FIGURE 58.A. NUMBER OF COPY VIOLATED                      FIGURE 59.B. NUMBER OF USER VIOLATION.....	41

## Introduction

This document describes the security requirements for the Healthcare project. It provides a detailed description of the socio-technical security requirements models from different views (Social, Asset, Authorization and threat). The *Social view* represents stakeholders as intentional and social entities, representing their goals and important asset in terms of documents, software, hardware and system, together with their interactions with other actors to achieve these goals and to exchange information. Stakeholders express constraints over their interactions in terms of security needs. It also represents the captured threat against assets. The *Asset view* represents the content of stakeholders' asset, showing how asset are interconnected, as well as how they are composed respectively. The *Authorization view* represents which stakeholders own what information, and captures the flow of permissions or prohibitions from one stakeholder to another. The modelling of authorizations expresses other security needs related to the way information is to be manipulated. The *Threat view* represents how captured threats were able to an exploit system by expressing the vulnerabilities that allowed threats to start one or chain of events (threat scenario) which lead to incidents (unwanted incident) that harm the system.

## Textual Description of the Scenario

A healthcare system is a socio-technical system which involved different roles (abstract actors) and actors (concrete participants). The system allows hospitals and healthcare centers allow physicians or general practitioners to perform medical tests and give advice to registered patients for medical services. The scenario involves the Red Cross RBT for blood donation and distribution. People who would like to donate (e.g., Alice) can make a test a in the ModernLab and send the result to the Red Cross RBT and have a certificate back. There are laboratories involved for specialized tests as well as research centers that conduct data analysis to make forecasts on the need for blood banks. This is complex socio-technical system in participants (actors) need to rely on each other to achieve their objectives, by interacting and exchanging information.

## Modeling with STS – tool

### Social view

The social view shows the involved stakeholders, which are represented as roles and agents. Agents refer to actual participants (stakeholders) known when modelling the Healthcare example, whereas roles are a generalization (abstraction) of agents. To capture the connection between roles and agents, the play relation is used to express the fact that certain agents play certain roles. Stakeholders have goals to achieve and they make use of different information to achieve these goals.

They interact with one another mainly by delegating goals and exchanging assets. Assets may be manipulated by actors, to achieve their goals.

# Social View Diagram

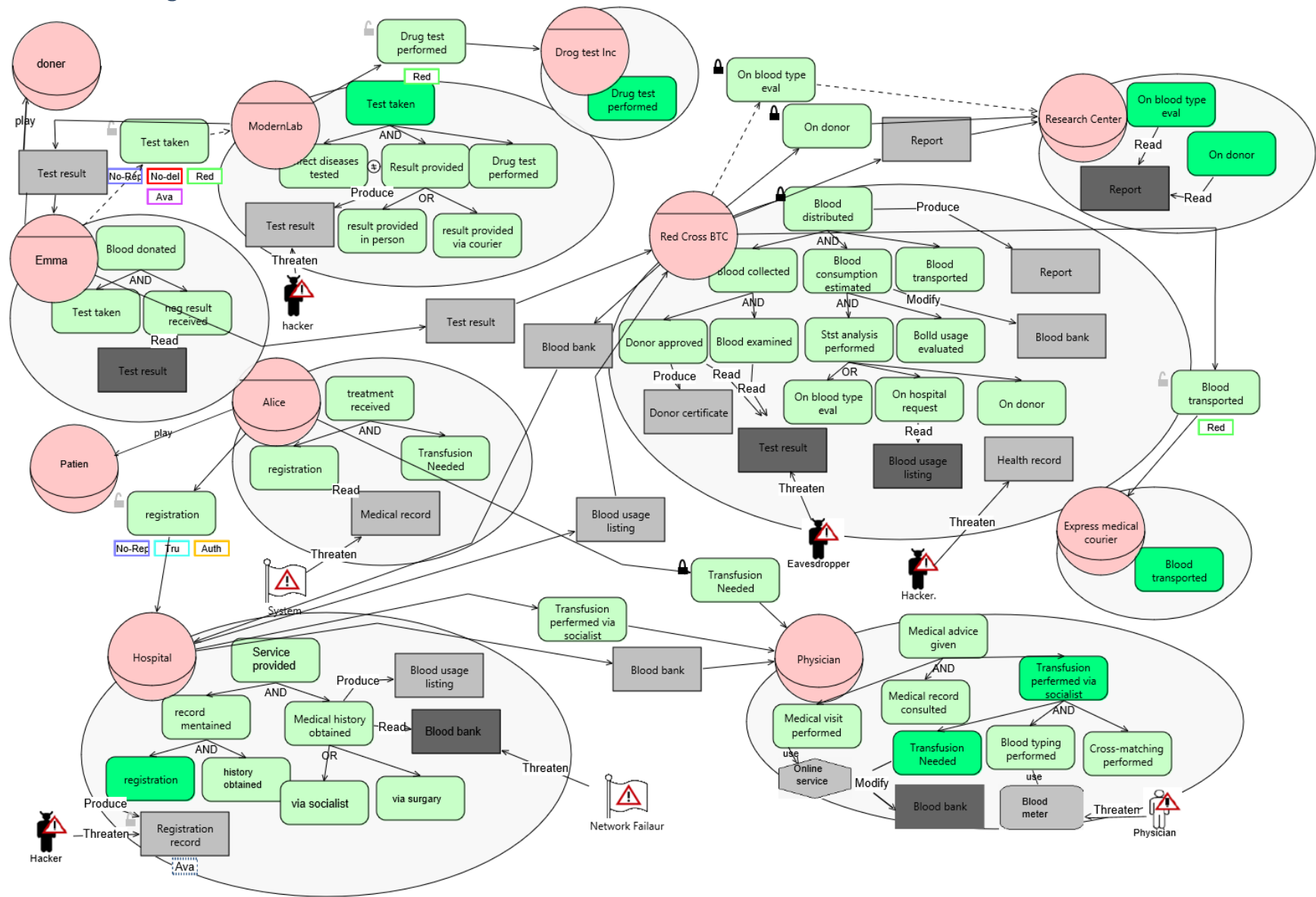


Figure 1- Social View for the Healthcare Example

## Asset View

The Asset view gives a structured representation of the assets in the Healthcare example. It shows what is the content of the assets represented in the social view. Information asset is represented by one or more documents via *tangible by* relation. Moreover, the Asset view considers composite asset, capturing these by means of *part of* relations. After modeling asset structure, the assets will be valued using *Asset valuation* table. Once they are valued, their classification, and security requirements will be assigned, according to their value.

# Asset View Diagram

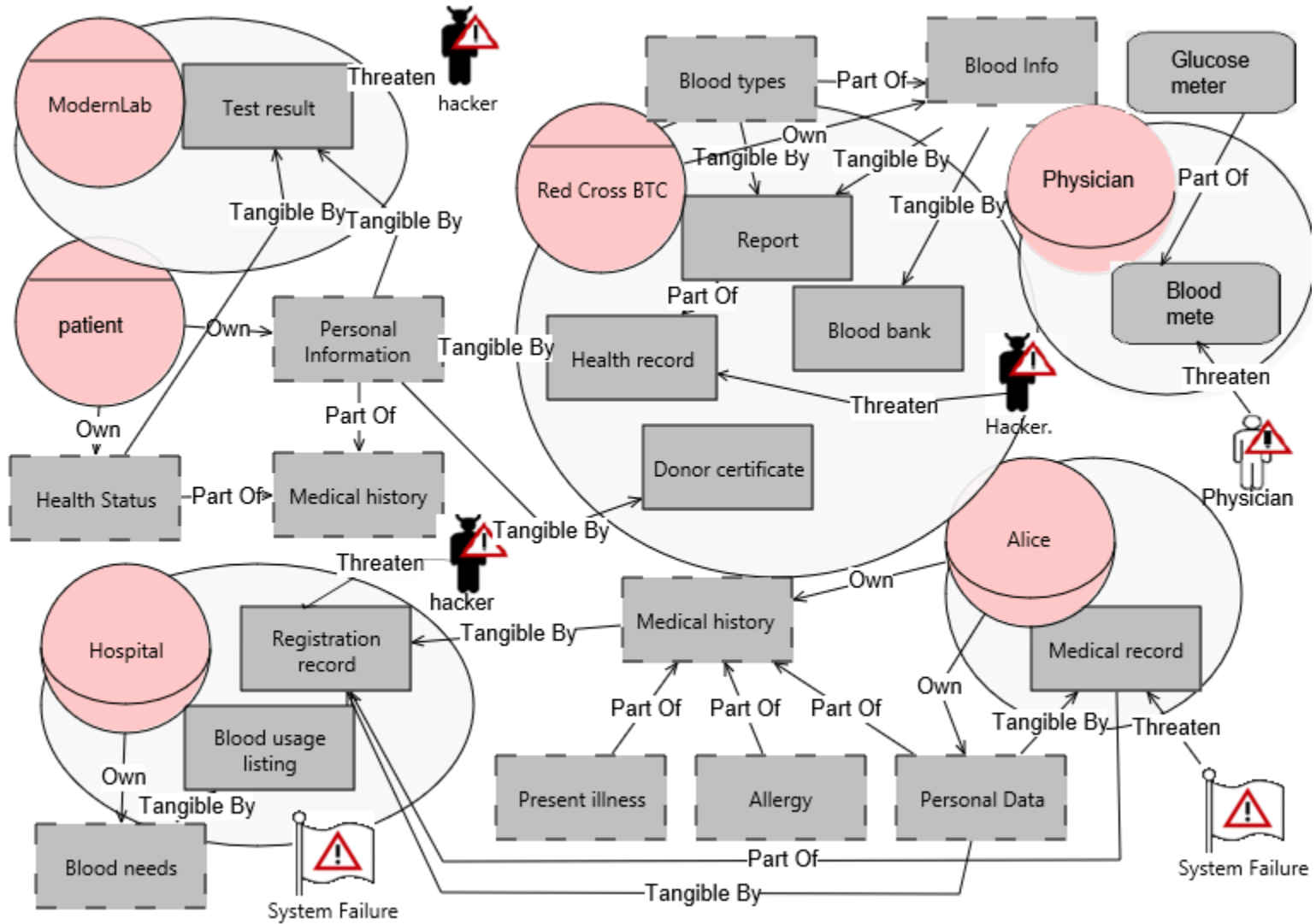


Figure 2- The Asset View of the Healthcare Example.

### Asset Evaluation Tables

After modeling structure of asset, using *Asset Evaluation Table* asset are evaluated. Once the value has been assigned, the class and final value will be set, automatically.

Name	Personal Data			Owner	Patent	Label	Top Secret
Value	C	I	A	Final value	3	Number of Copy	2
	3	3	2			Number of User	1
Direct Asset							Indirect asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 3. Asset Evaluation Table of Information Personal Data

Name	Present illness		Owner		label	Secret	
Value	C	I	A	Final Value	2	Number of Copy	3
	2	2	2			Number of User	3
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 4. Asset Evaluation Table of Information Present Illness



Name	Allergy			Owner	Patent	Label	Secret
Value	C	I	A	Final value	2	Number of User	3
	2	2	2			Number of Copy	2
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 5. Asset Evaluation Table of Information Allergy

Name	Medical history		Owner		Label	Top Secret	
Value	C	I	A	Final Value	3	Number of Copy	2
	3	3	2			Number of User	1
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Present illness		2	2	2	3	3	
Allergy		2	2	2	3	2	
Personal data	Patient	3	3	2	2	1	

Figure 6. Asset Evaluation Table of Information Medical History

Name	Medical record			Owner	Patient	Label	Top Secret
Value	C	I	A	Final value	3	Number of Copy	2
	3	3	2			Number of User	1
Direct Asset							Indirect Asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Personal Data	Patient	3	3	2	2	1	

Figure 7. Asset Evaluation Table of Document Medical Record

Name	Registration record	Owner	Patient	Label	Top Secret		
Value	C	I	A	Final value	3	Number of Copy	2
	3	2	2			Number of User	1
Direct Asset							Indirect Asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Personal Data	Patient	3	3	2	2	1	
Medical history	Patient	3	3	2	2	1	
Medical record		3	3	2	3	1	

Figure 8. Asset Evaluation Table of Document Registration Record

Name	Blood needs			Owner	Hospital	Label	Top Secret
Value	C	I	A	Final Value	3	Number of User	4
	2	3	2			Number of Copy	4
Direct Asset							Indirect Asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 9. Asset Evaluation Table of Information Blood Needs

Name	Blood usage listing			Own		Label	Top Secret
Value	C	I	A	Final Value	3	Number of User	4
	2	3	2			Number of Copy	4
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Blood needs	Hospital	2	3	2	4	4	

Figure 10. Asset Evaluation Table of Document Blood Usage Listing

Name	Blood types			Owner		label	Secret
Value	C	I	A	Final Value	2	Number of User	4
	2	2	2			Number of Copy	4
Direct Asset							
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 11. Asset Evaluation Table of Information Blood Type

Name	Blood info			Owner	Red Cross BTC	Label	Secret
Value	C	I	A	Final Value	2	Number of User	1
	2	2	2			Number of Copy	4
Direct Asset							Indirect Asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Blood types		2	2	2	1	4	

Figure 12. Asset Evaluation Table of Information Blood Info

Name	Blood bank		Owner		label	Secret	
Value	C	I	A	Final Value	2	Number of User	1
	2	2	2			Number of Copy	4
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Blood Info	Red Cross BTC	2	2	2	1	4	
Blood types		2	2	2	1	4	

Figure 13.Asset Evaluation Table of Document Blood Bank

Name	Report		Owner		label	Secret	
Value	C	I	A	Final Value	2	Number of User	1
	2	2	2			Number of Copy	4
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Blood Info	Red Cross BTC	2	2	2	1	4	

Figure 14.Asset Evaluation Table of Document Report

Name	Health status		Owner		Alice	label	Secret
Value	C	I	A	Final Value	2	Number of User	1
	2	2	2			Number of Copy	4
Direct Asset							Indirect Asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 15.Asset Evaluation Table of Information Health Record

Name	Personal information		Owner		Alice	label	Top Secret
Value	C	I	A	Final Value	3	Number of User	2
	3	2	1			Number of Copy	2
Direct Asset							Indirect Asset
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			

Figure 16.Asset Evaluation Table of Information Personal Information

Name	Medical history info		Owner			label	Top Secret		
Value	C	I	A	Final value	3	Number of User	2		
	3	2	2				Number of Copy	2	
Direct Asset								Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy			
		C	I	A					
Personal Info	Alice	3	3	1	2	2			
Health status	Alice	2	2	2	3	3			

Figure 17.Asset Evaluation Table of Information Medical History Info

Name	Health record		Owner			label	Top Secret		
Value	C	I	A	Final Value	3	Number of User	2		
	3	2	2				Number of Copy	2	
Direct Asset						Indirect Asset			
Name	Owner	Value			Number of User	Number of Copy			
		C	I	A					
Personal Info	Alice	3	2	1	2	2			
Report		2	2	2	3	3			

Figure 18.Asset Evaluation Table of Document Health Record

Name	Donor certificate		Owner		label	Top Secret	
Value	C	I	A	Final Value	3	Number of User	2
	3	2	1			Number of Copy	2
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Personal info	Alice	3	2	1	2	2	

Figure 19.Asset Evaluation Matrix of Document Donor Certificate

Name	Test result	Owner		label	Top Secret		
Value	C	I	A	Final Value	3	Number of Copy	1
	3	2	2			Number of User	2
Direct Asset						Indirect Asset	
Name	Owner	Value			Number of User	Number of Copy	
		C	I	A			
Personal Info	Alice	3	2	1	2	2	
Health status	Alice	2	2	2	1	4	

Figure 20.Asset Evaluation Matrix of Document Test Result



## Social View After Asset Classification

To ensure a level of protection for all asset, security requirements are assigned after classification.

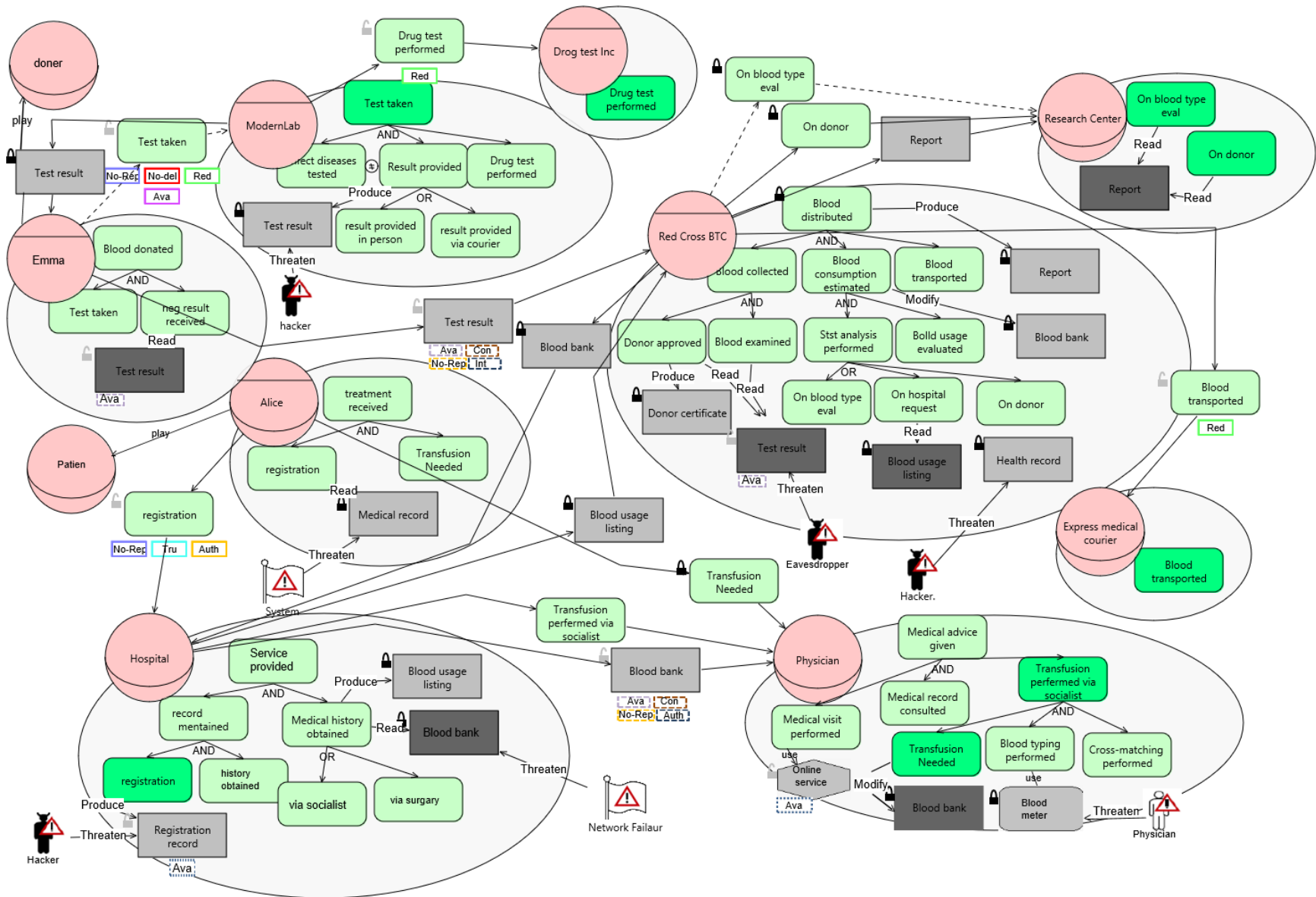


Figure 21- Security Requirements According to Values Has Assigned

## Authorization View

The authorization view shows the permissions or prohibitions flow from a stakeholder to another, that is, the authorizations stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorizing other actors (i.e. authorization transferability). Authorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

# Authorization View Diagram

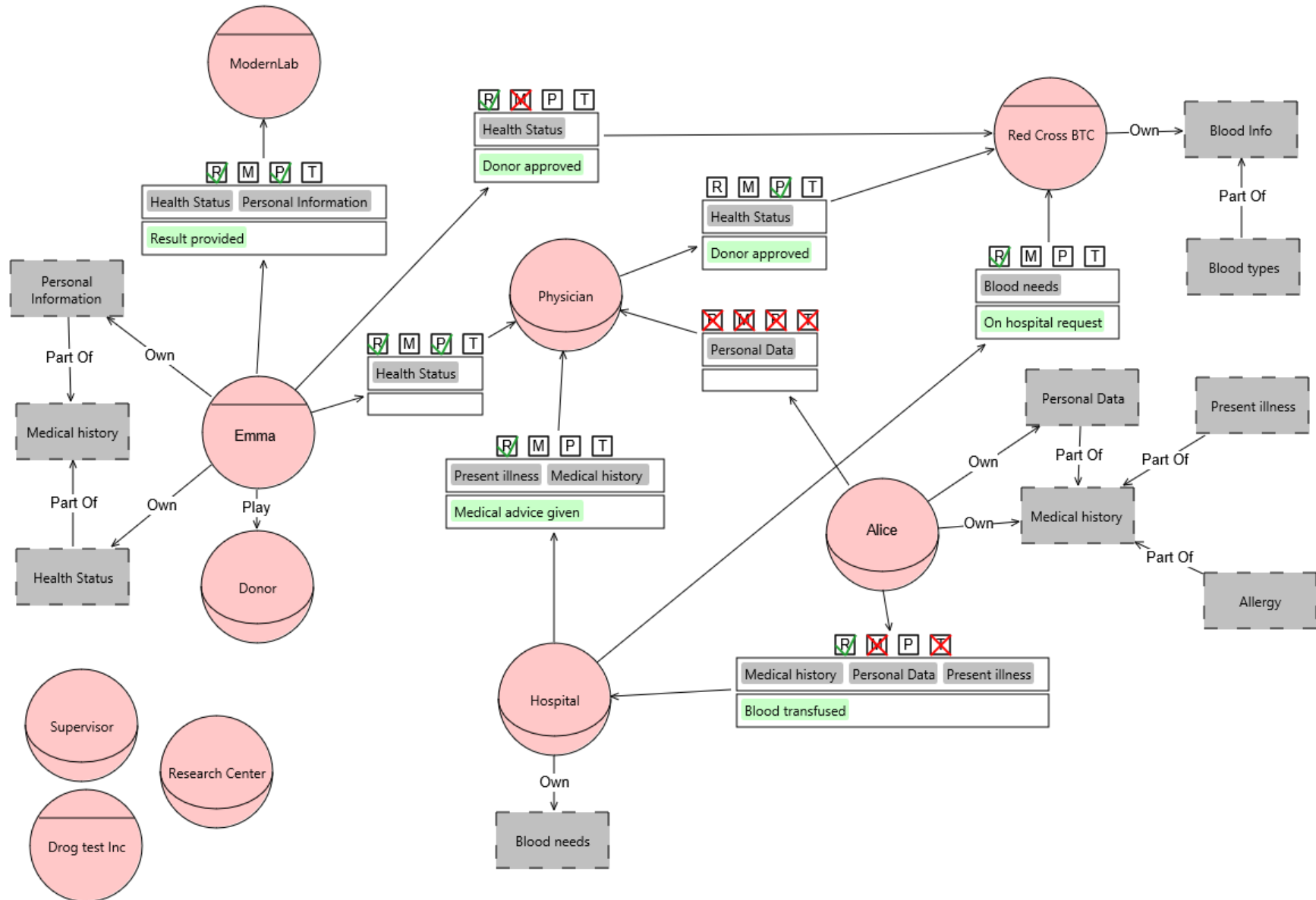


Figure 22-Figure 2- The Authorization View of the Healthcare Example.

## Authorization Property

Property	Value
Name	Hospital- Red Cross BTC
Duration of authorization	<b>During Contract</b>
Act on Termination	<b>Distroy</b>

Figure 23. Hospital-Patient Authorization Property

Property	Value
Name	Emm-Moden lab
Duration of authorization	<b>During treatment</b>
Act on Termination	<b>Distroy</b>

Figure 24-Emma-Modern Lab Authorization Property

Property	Value
Name	Emm-Red Cross BTC
Duration of authorization	<b>During treatment</b>
Act on Termination	<b>Return</b>

Figure 25-Emma-Red Cross BTC Authorization Property

Property	Value
Name	Physician-Red Cross BTC
Duration of authorization	<b>3 month</b>
Act on Termination	<b>Return</b>

Figure 26-Physician-Red Cross BTC Authorization Property

Property	Value
Name	Emm-Physician
Duration of authorization	<b>During treatment</b>
Act on Termination	<b>Return</b>

Figure 28- Emma-Physician Authorization Property

Property	Value
Name	Hospital- Physician
Duration of authorization	<b>During contract</b>
Act on Termination	<b>Return</b>

Figure 27-Hospital- Physician Authorization Property

Property	Value
Name	Alice-Hospital
Duration of authorization	<b>During treatment</b>
Act on Termination	<b>Return</b>

*Figure 30-Alice-Hospital Authorization Property*

Property	Value
Name	Alice-Physician
Duration of authorization	<b>During treatment</b>
Act on Termination	<b>Return</b>

*Figure 29-Alice-Physician Authorization Property*

## Threat View

The model captures the vulnerabilities that exist in the system which allows threats threat scenario(s), by which incident(s) raise to harm asset. We specify which security objective(s) of asset is compromised due to the incidents.

### Threat View Diagram

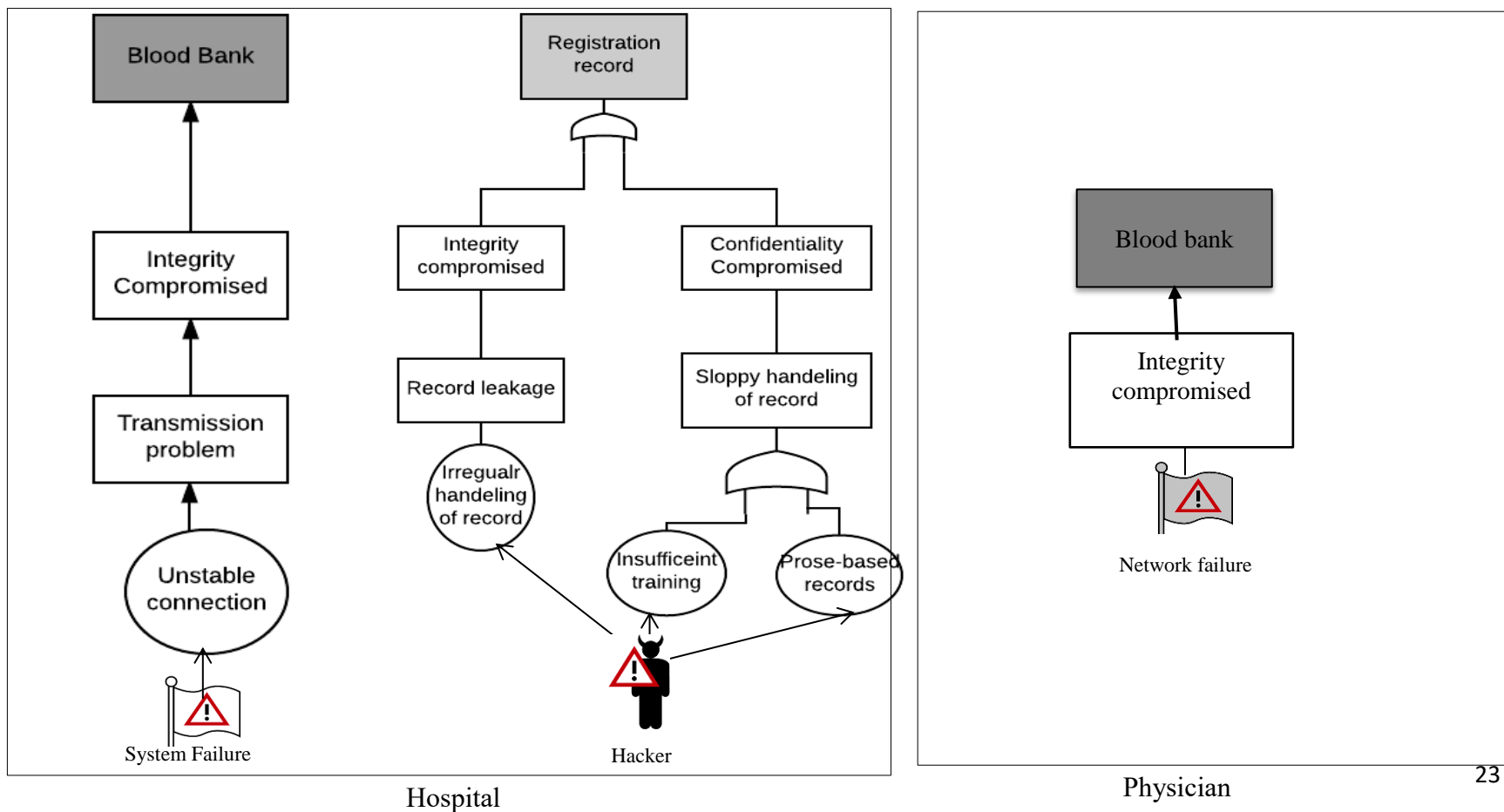


Figure 31-Threat View (I)

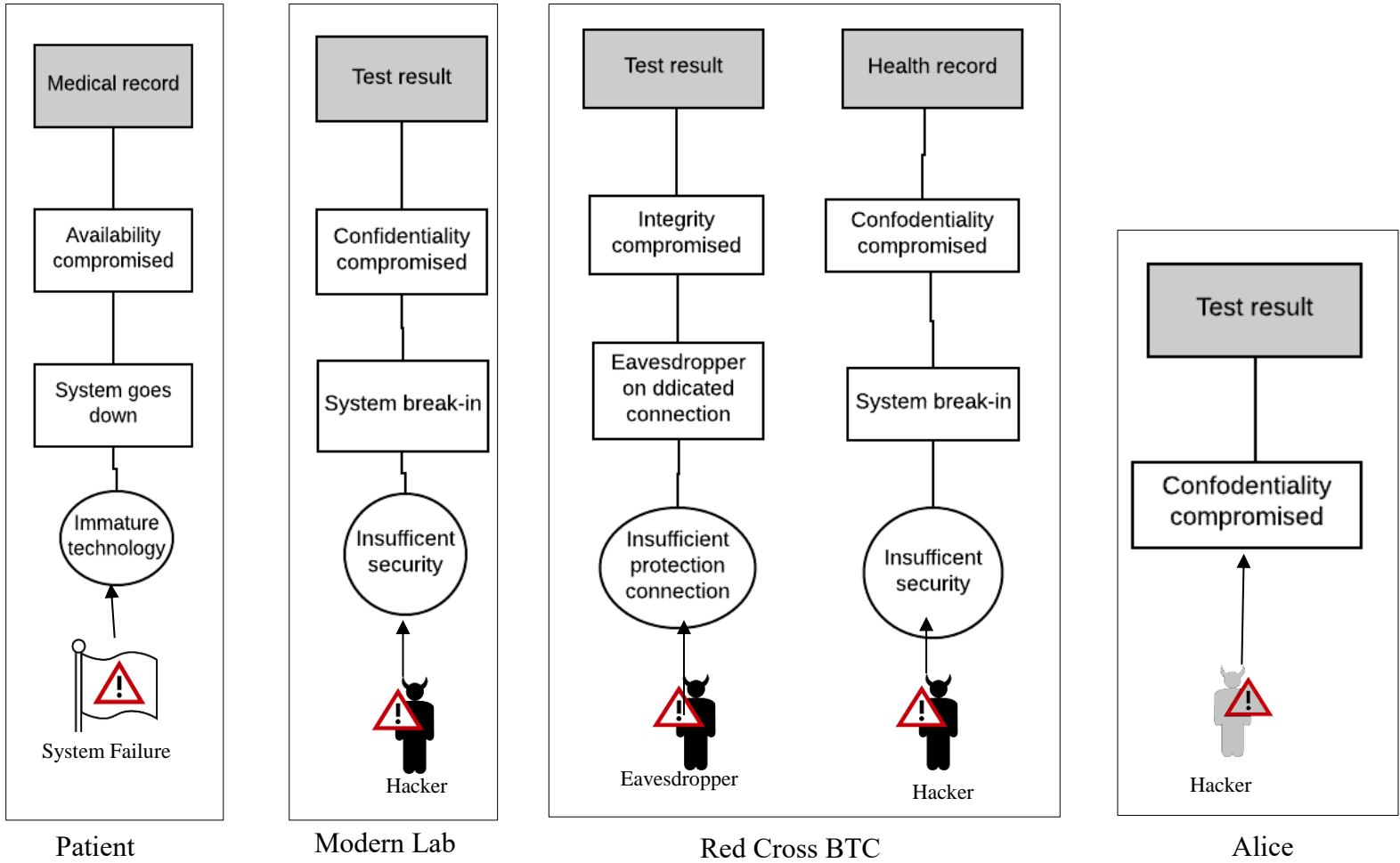


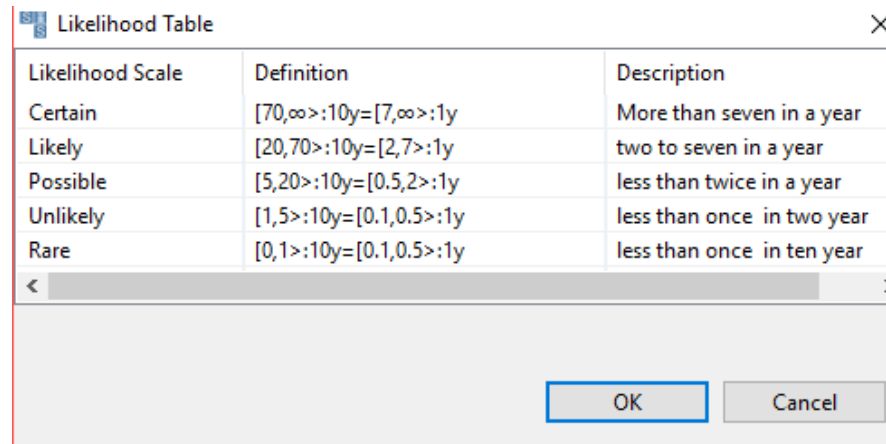
Figure 32-Threat View (II)



## Likelihood tables

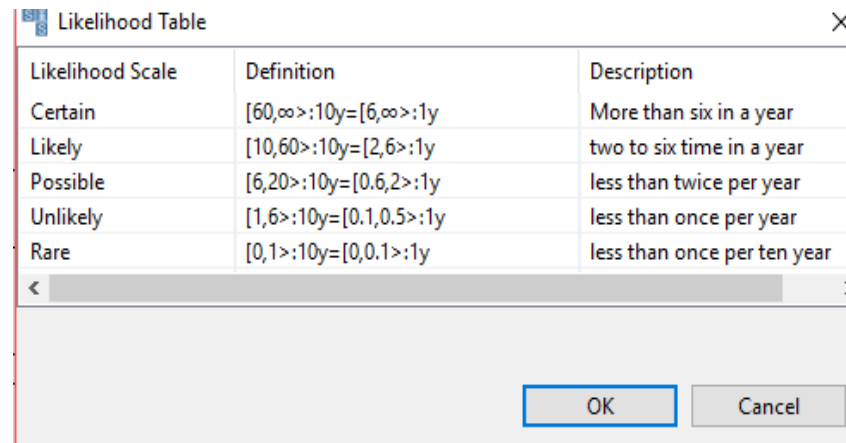
When the threat diagram is model, it is time to estimate likelihood and consequence scales, in order to compute the risk values which are used to decide whether threats are acceptable or not.

Likelihood Scale estimates for each victim actor with help pf analyst based on their judgment respect how they may be determined from their historical data that there are aware of. While, consequence is estimated for each asset based on their importance.



Likelihood Scale	Definition	Description
Certain	$[70, \infty > : 10y = [7, \infty > : 1y]$	More than seven in a year
Likely	$[20, 70 > : 10y = [2, 7 > : 1y]$	two to seven in a year
Possible	$[5, 20 > : 10y = [0.5, 2 > : 1y]$	less than twice in a year
Unlikely	$[1, 5 > : 10y = [0.1, 0.5 > : 1y]$	less than once in two year
Rare	$[0, 1 > : 10y = [0.1, 0.5 > : 1y]$	less than once in ten year

Figure 33-Alice Likelihood Table



Likelihood Scale	Definition	Description
Certain	$[60, \infty > : 10y = [6, \infty > : 1y]$	More than six in a year
Likely	$[10, 60 > : 10y = [2, 6 > : 1y]$	two to six time in a year
Possible	$[6, 20 > : 10y = [0.6, 2 > : 1y]$	less than twice per year
Unlikely	$[1, 6 > : 10y = [0.1, 0.5 > : 1y]$	less than once per year
Rare	$[0, 1 > : 10y = [0, 0.1 > : 1y]$	less than once per ten year

Figure 34- Modern lab Likelihood Table

Likelihood Table

Likelihood Scale	Definition	Description
Certain	$[70, \infty > : 10y = [7, \infty > : 1y]$	More than seven in a year
Likely	$[20, 70 > : 10y = [2, 7 > : 1y]$	two to seven in a year
Possible	$[5, 20 > : 10y = [0.5, 2 > : 1y]$	less than twice in a year
Unlikely	$[1, 5 > : 10y = [0.1, 0.5 > : 1y]$	less than once in two year
Rare	$[0, 1 > : 10y = [0.1, 0.5 > : 1y]$	less than once in ten year

OK Cancel

Figure 35-Red Cross BTC Likelihood Table

Likelihood Table

Likelihood Scale	Definition	Description
Certain	$[40, \infty > : 10y = [4, \infty > : 1y]$	More than four in a year
Likely	$[10, 40 > : 10y = [1, 4 > : 1y]$	one to four in a year
Possible	$[5, 10 > : 10y = [0.5, 1 > : 1y]$	less than once per year
Unlikely	$[1, 5 > : 10y = [0.1, 0.5 > : 1y]$	less than once per ten year
Rare	0	not happen at all

OK Cancel

Figure 36- Patient Likelihood Table

Likelihood Table

Likelihood Scale	Definition	Description
Certain	$[40, \infty > : 10y = [4, \infty > : 1y]$	More than four in a year
Likely	$[10, 40 > : 10y = [1, 4 > : 1y]$	one to four in a year
Possible	$[5, 10 > : 10y = [0.5, 1 > : 1y]$	less than once per year
Unlikely	$[1, 5 > : 10y = [0.1, 0.5 > : 1y]$	less than once per ten year
Rare	0	not happen at all

< >

OK Cancel

Figure 37- Hospital Likelihood Table

Likelihood Table

Likelihood Scale	Definition	Description
Certain	$[70, \infty > : 10y = [7, \infty > : 1y]$	More than seven in a year
Likely	$[20, 70 > : 10y = [2, 7 > : 1y]$	two to seven in a year
Possible	$[5, 20 > : 10y = [0.5, 2 > : 1y]$	less than twice in a year
Unlikely	$[1, 5 > : 10y = [0.1, 0.5 > : 1y]$	less than once in two year
Rare	$[0, 1 > : 10y = [0.1, 0.5 > : 1y]$	less than once in ten year

< >

OK Cancel

Figure 38- Physician Likelihood Table

Consequence Tables

Hospital Documents Affected Documents)

Consequence Table

Consequence Scale	Description
Catastrophic	1000+ file are affected
Major	500 - 1000 file are affected
Moderate	200-500 file are affected
Minor	100- 200 file are affected
Insignificant	less than  file are affected

OK Cancel

Consequence Table

Consequence Scale	Description
Catastrophic	up to 1000 file are affected
Major	400-1000 file are affected
Moderate	200 - 400file are affected
Minor	100 - 200 file are affected
Insignificant	up to 100 file are affected

OK Cancel

Figure 39. Blood Bank-Registration Record

Red Cross BTC Affected Documents

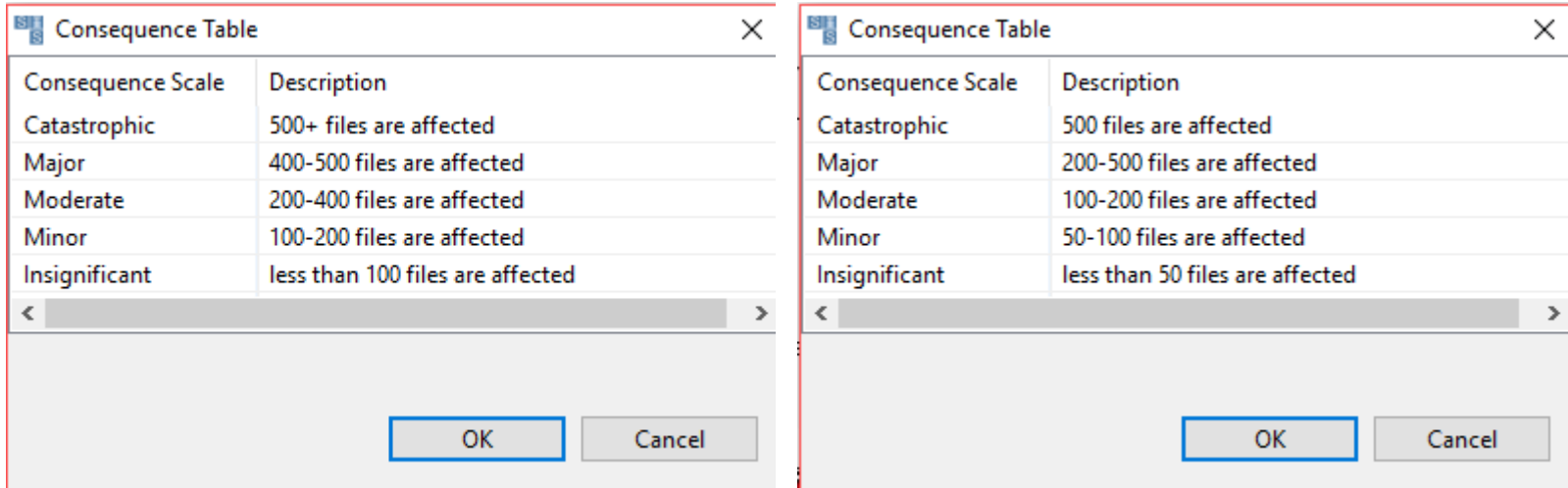


Figure 40. Test Result - Health Record

Modern Lab Affected Document

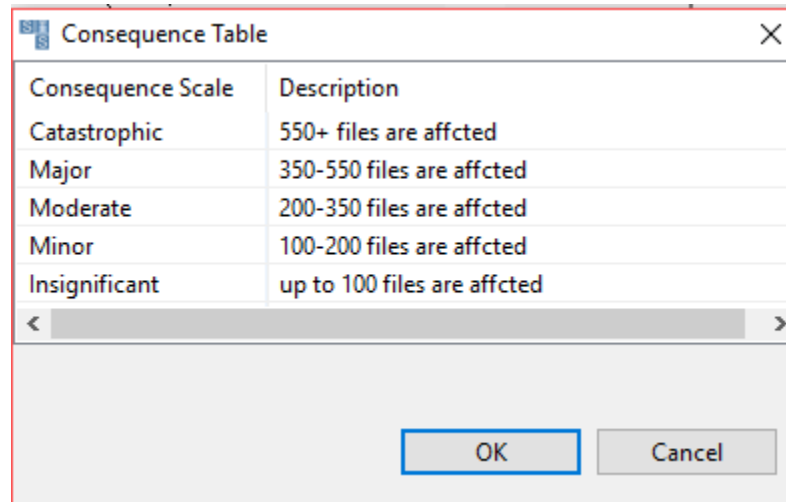
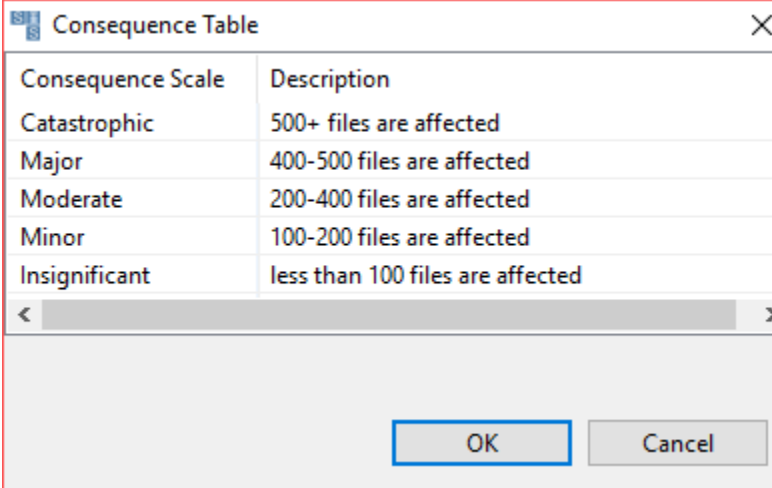


Figure 41. Test Result

Patient Affected Document

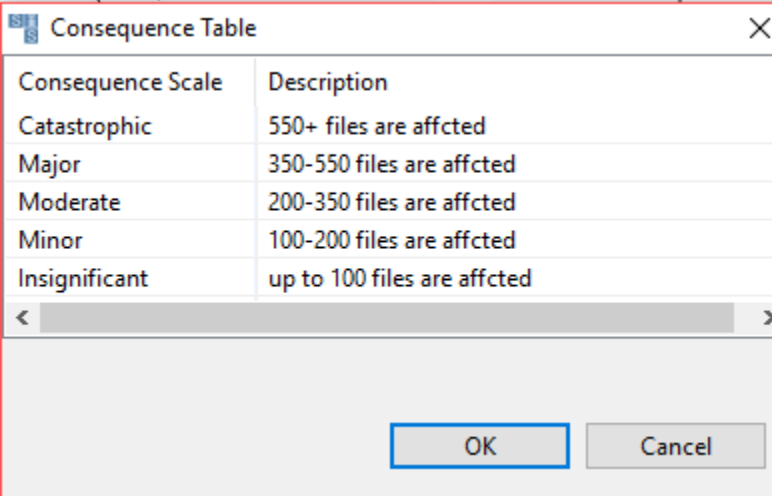


A dialog box titled "Consequence Table" with a close button (X) in the top right corner. It contains a table with two columns: "Consequence Scale" and "Description". Below the table is a horizontal scrollbar and two buttons: "OK" and "Cancel".

Consequence Scale	Description
Catastrophic	500+ files are affected
Major	400-500 files are affected
Moderate	200-400 files are affected
Minor	100-200 files are affected
Insignificant	less than 100 files are affected

Figure 42. Medical Record

Alice Affected Document

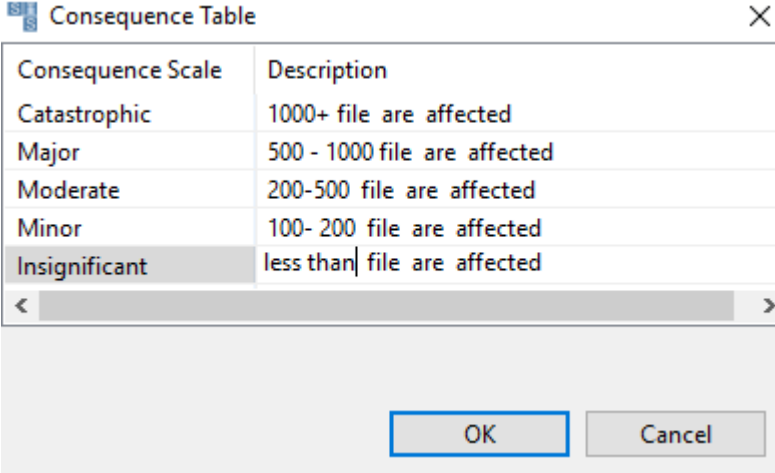


A dialog box titled "Consequence Table" with a close button (X) in the top right corner. It contains a table with two columns: "Consequence Scale" and "Description". Below the table is a horizontal scrollbar and two buttons: "OK" and "Cancel".

Consequence Scale	Description
Catastrophic	550+ files are affected
Major	350-550 files are affected
Moderate	200-350 files are affected
Minor	100-200 files are affected
Insignificant	up to 100 files are affected

Figure 43. Test Result

Physician Affected Document



A dialog box titled "Consequence Table" with a close button (X) in the top right corner. It contains a table with two columns: "Consequence Scale" and "Description". The table lists five levels of consequences: Catastrophic, Major, Moderate, Minor, and Insignificant. The "Insignificant" row is highlighted. Below the table is a horizontal scrollbar and two buttons: "OK" and "Cancel".

Consequence Scale	Description
Catastrophic	1000+ file are affected
Major	500 - 1000 file are affected
Moderate	200-500 file are affected
Minor	100- 200 file are affected
Insignificant	less than file are affected

Figure 44. Blood Bank

## Threat View Diagram Together with the Scales

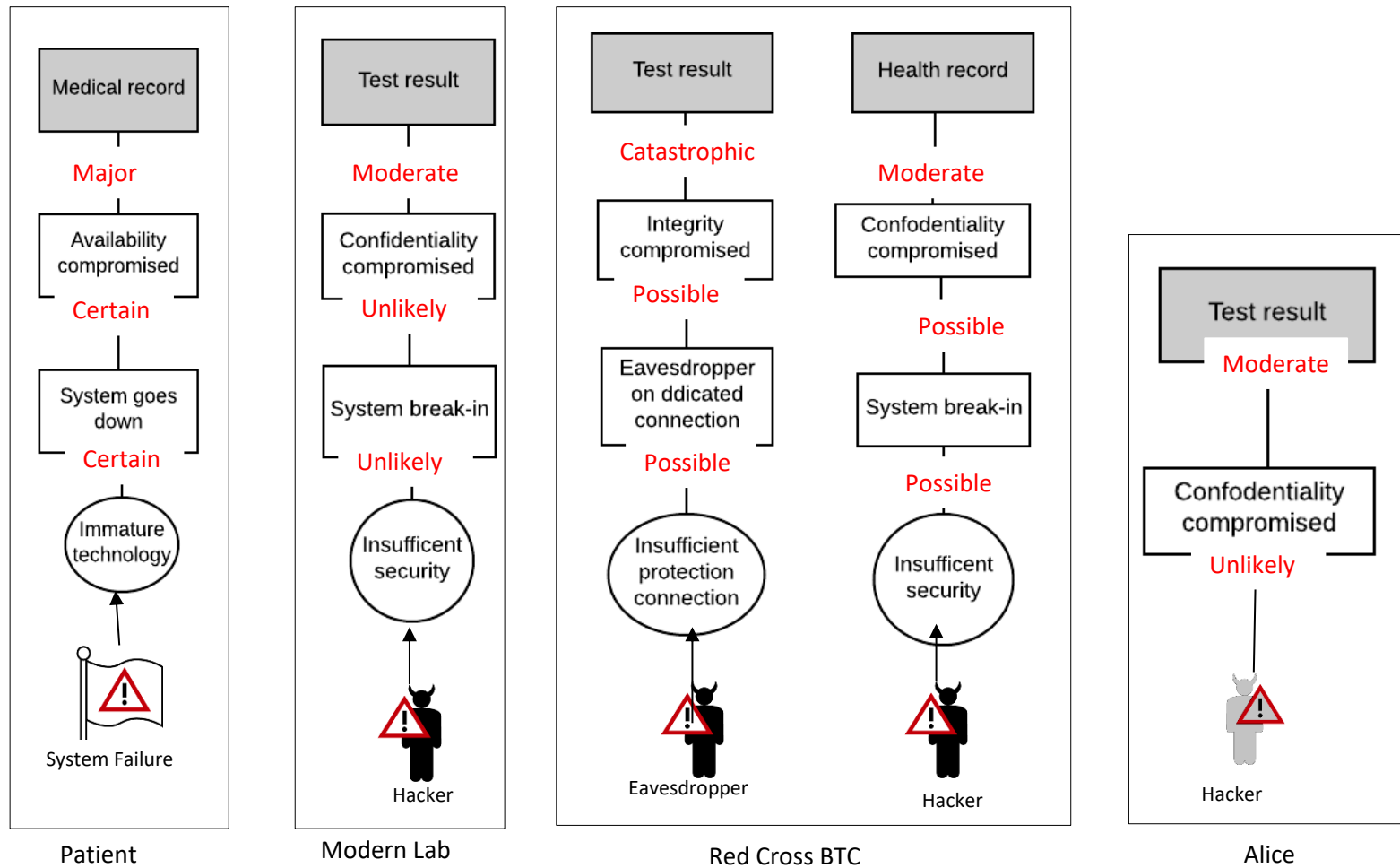


Figure 45-Threat View(I)- Scales Assigned



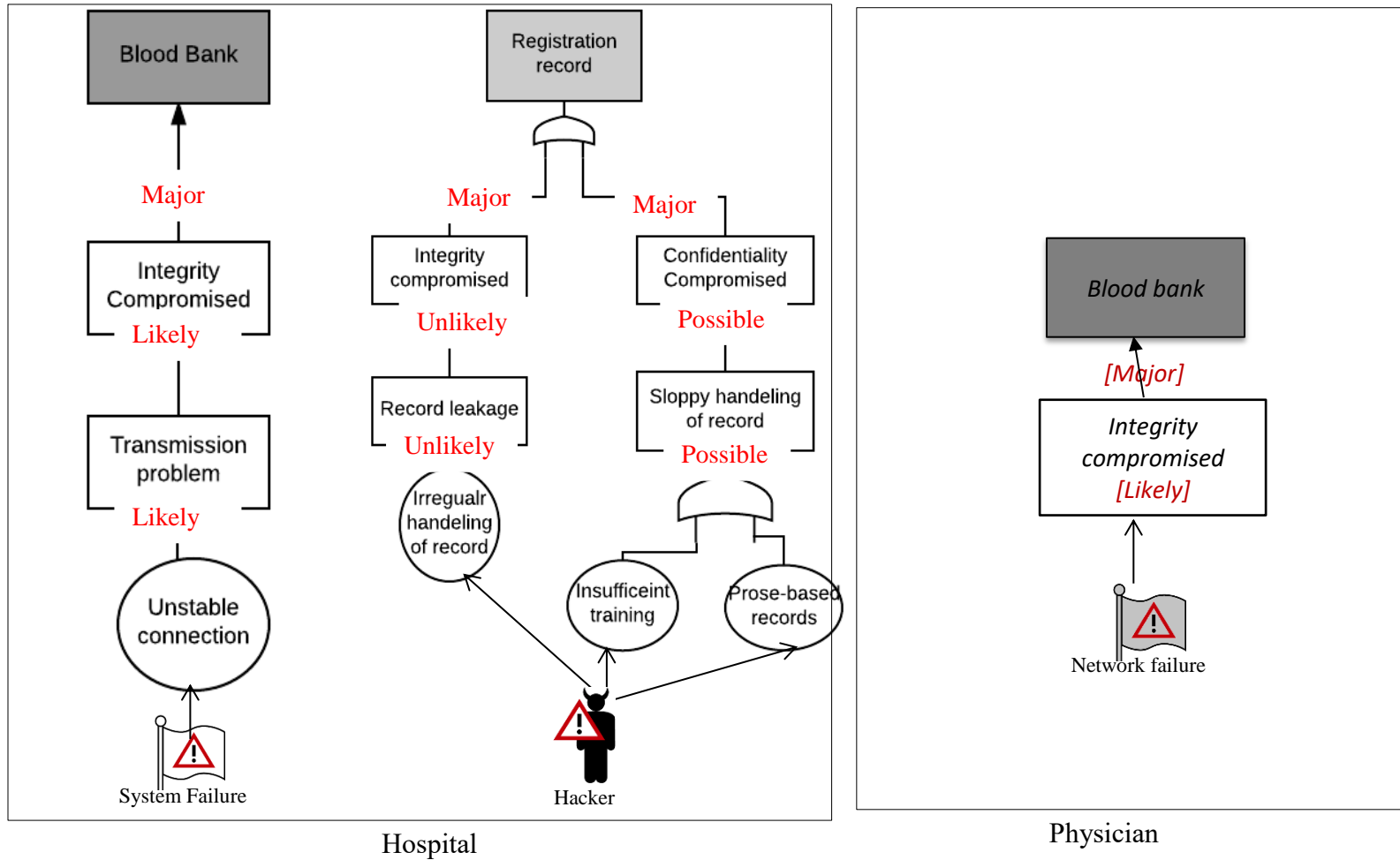


Figure 46-Threat View(II)- Scales Assigned

## Risk Evaluation- Using Risk Evaluation Matrix

Risk Evaluation Matrix is to realize whether the threat is out of stakeholder tolerance (unacceptable) or not respect to the two scales. The one falls in the red cells needs to be treated.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Registration ...	Insignificant	Minor	Moderate	Major	Catastrophic
	Rare	Green	Green	Green	Yellow	Red
	Unlikely	Green	Yellow	Orange	Hospital-Integrity ...	Red
	Possible	Green	Yellow	Orange	Hospital-confident...	Red
	Likely	Yellow	Orange	Orange	Red	Red
Certain	Orange	Red	Red	Red	Red	

Frequency: Rare, Unlikely, Possible, Likely, Certain

Consequence: Insignificant, Minor, Moderate, Major, Catastrophic

Dropdown menu options: VERYHIGH, HIGH, LOW, VERYLOW

Buttons: OK, Cancel

Figure 47. Hospital – Document Registration Record

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Blood bank	Insignificant	Minor	Moderate	Major	Catastrophic
	Rare	Green	Green	Green	Yellow	Red
	Unlikely	Green	Green	Yellow	Orange	Red
	Possible	Green	Yellow	Orange	Orange	Red
	Likely	Yellow	Orange	Orange	Hospital-integrity compromised	Red
Certain	Orange	Red	Red	Red	Red	

Frequency: Rare, Unlikely, Possible, Likely, Certain

Consequence: Insignificant, Minor, Moderate, Major, Catastrophic

Buttons: OK, Cancel

Figure 48- Hospital Bank Risk Evaluation matrix

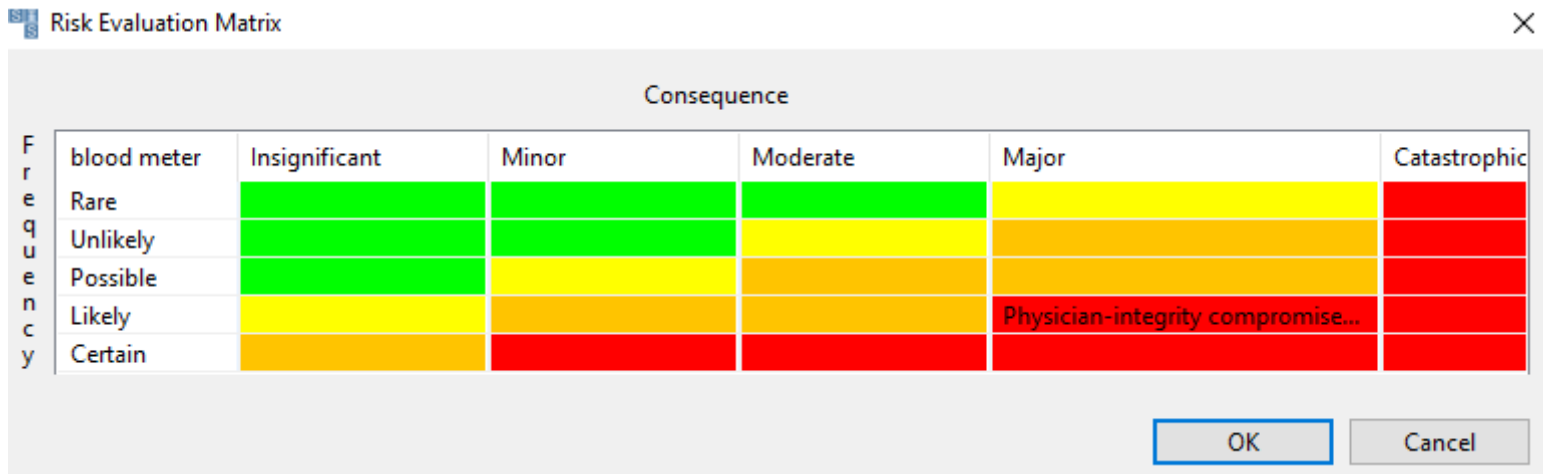


Figure 50- Physician Risk Evaluation matrix

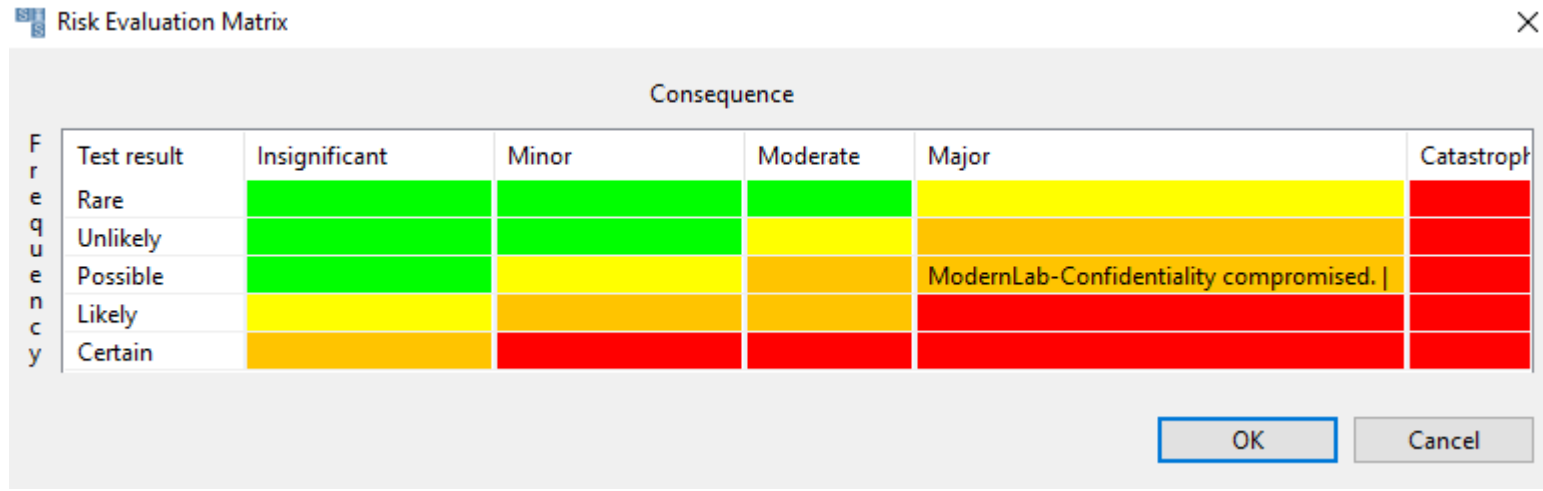


Figure 51 Modern Lab Risk Evaluation matrix

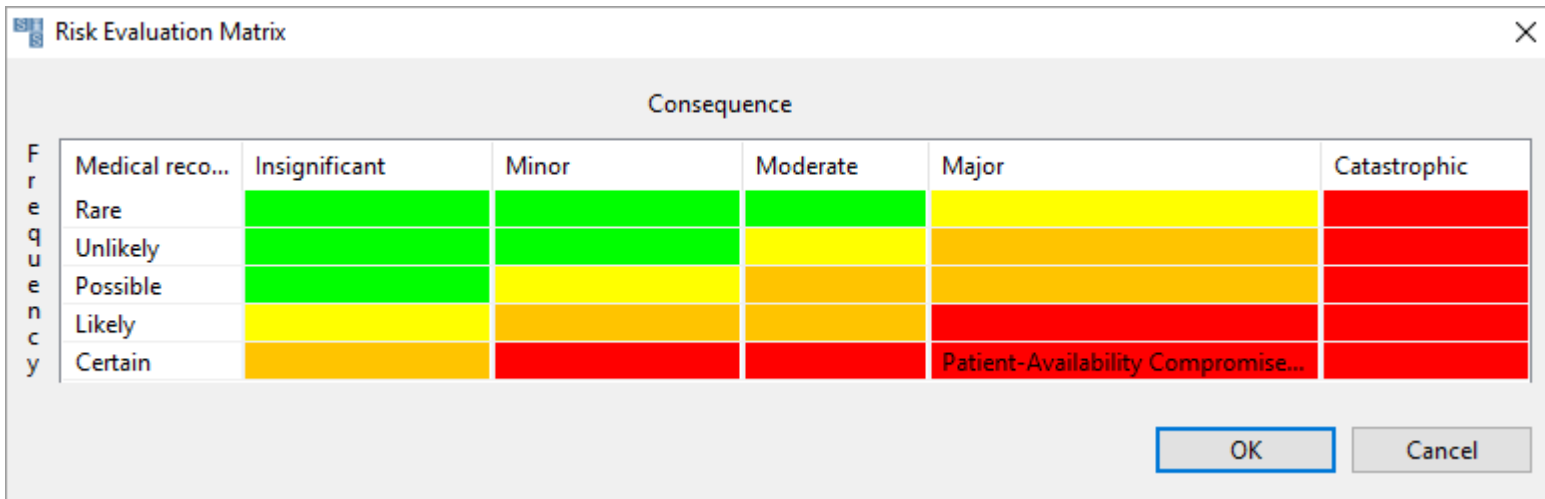


Figure 52- Patient Risk Evaluation matrix

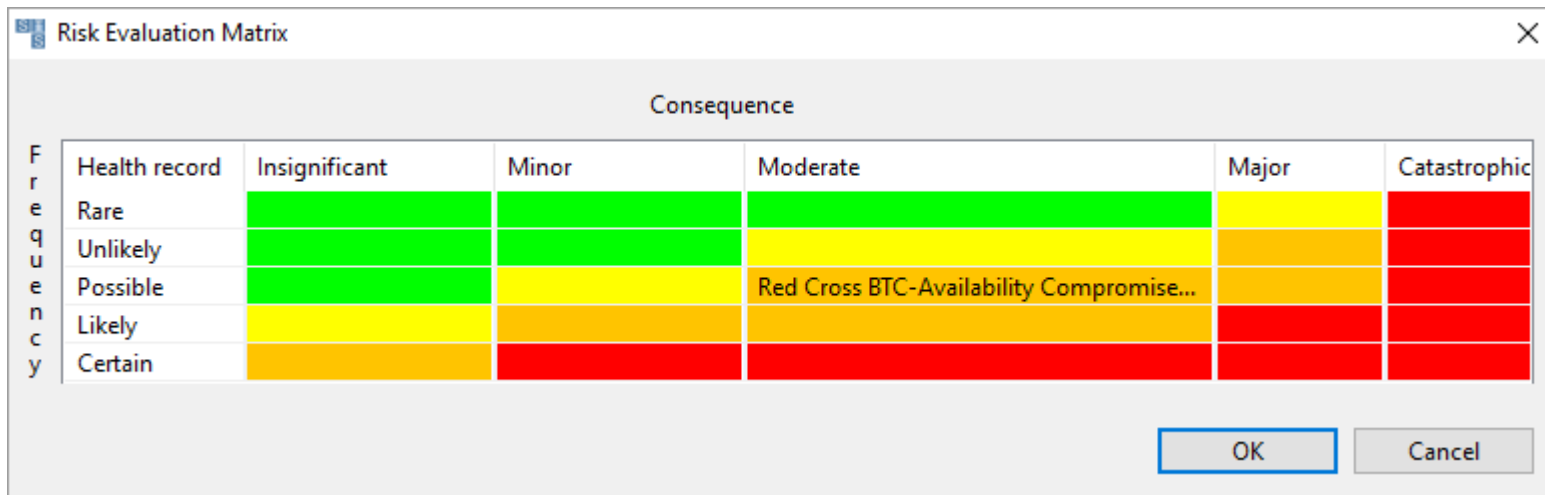


Figure 53- Red Cross Risk Evaluation matrix

		Consequence				
F r e q u e n c y	Test result	Insignificant	Minor	Mode...	Major	Catastrophic
	Rare					
	Unlikely					
	Possible					Red Cross BTC-Confidentiality compromised, ,
	Likely					
	Certain					Red Cross BTC-.Integrity Compromised ,

Figure 54-Risk Evaluation matrix

## Analysis.

### Risk Assessment

Evaluating threats by the *Risk Evaluation Matrix* Classified what are the unacceptable threats which need to be further assessment. The secret-class asset security requirements can be improved.

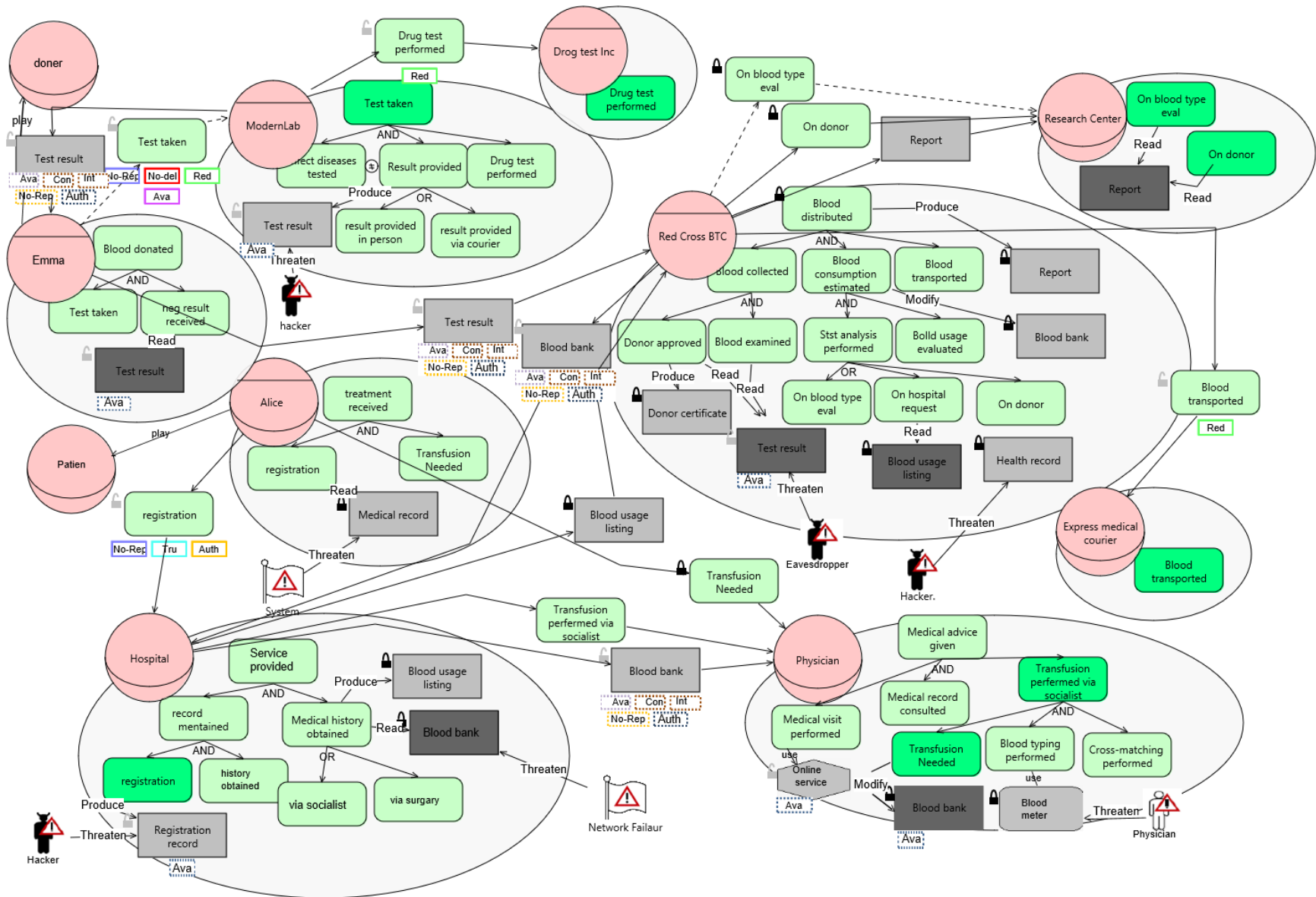


Figure 55- Improvement /added Security Requirements to the Social View as Treatment

## Security and Threat Analysis Result

Since the models created in modeling phase are tightly connected, there may be included some inconsistency and conflict between requirements and threats that endanger stakeholders' assets. To discover these issues, security and risk

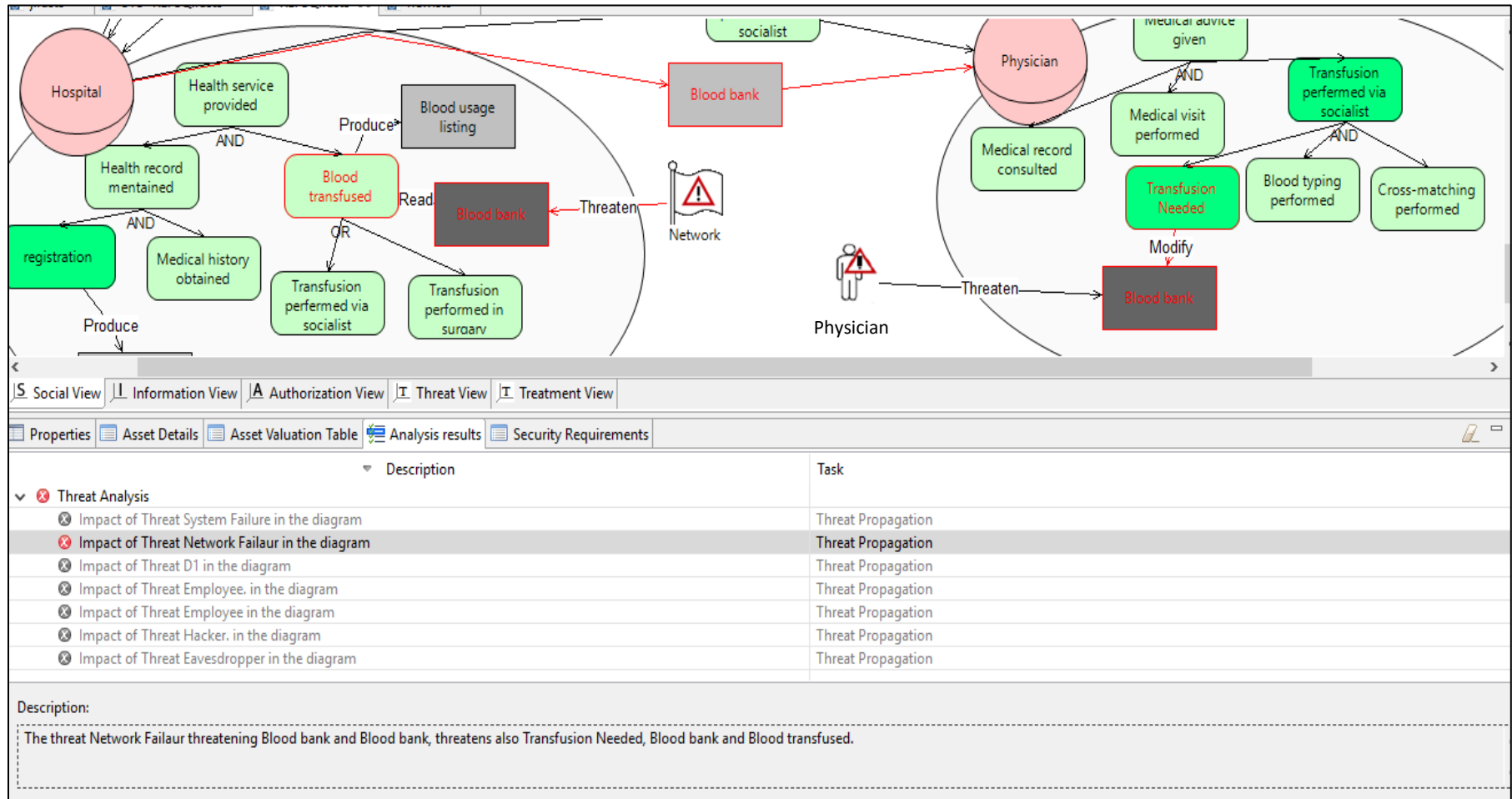


Figure 56. Propagation of via transmission and their impact on achieving goals



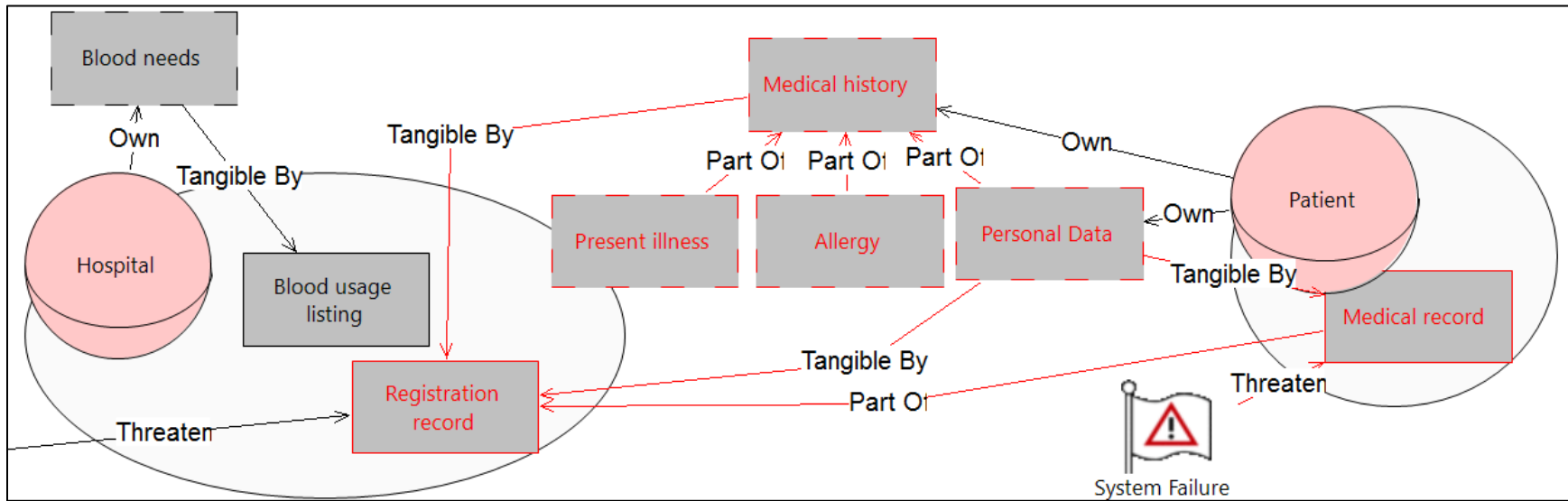


Figure 57, Propagation via Document/information structure

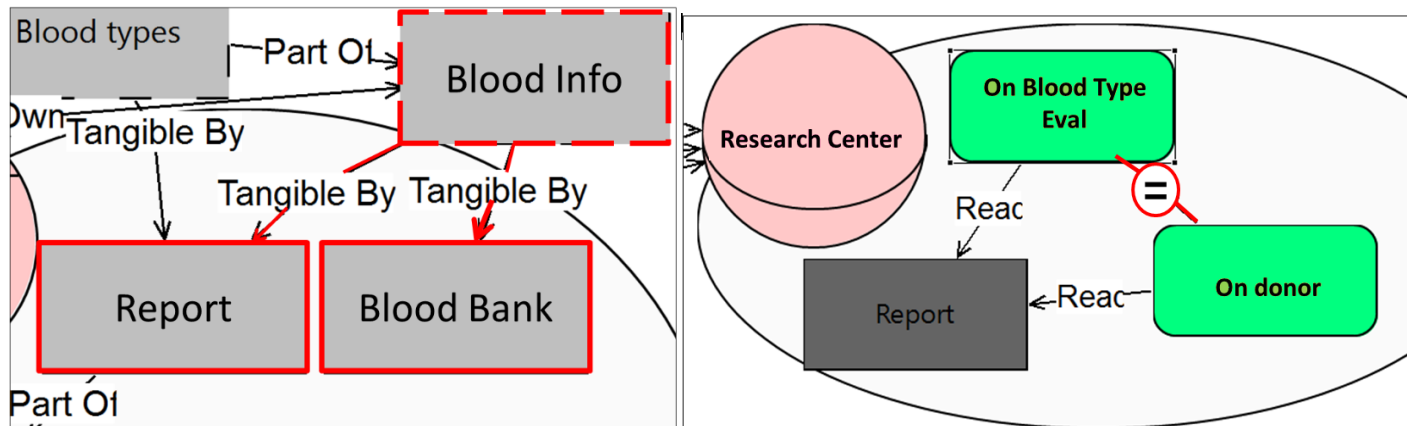


Figure 58.a. Number of Copy Violated

Figure 59.b. Number of User Violation