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

Table of Figures

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

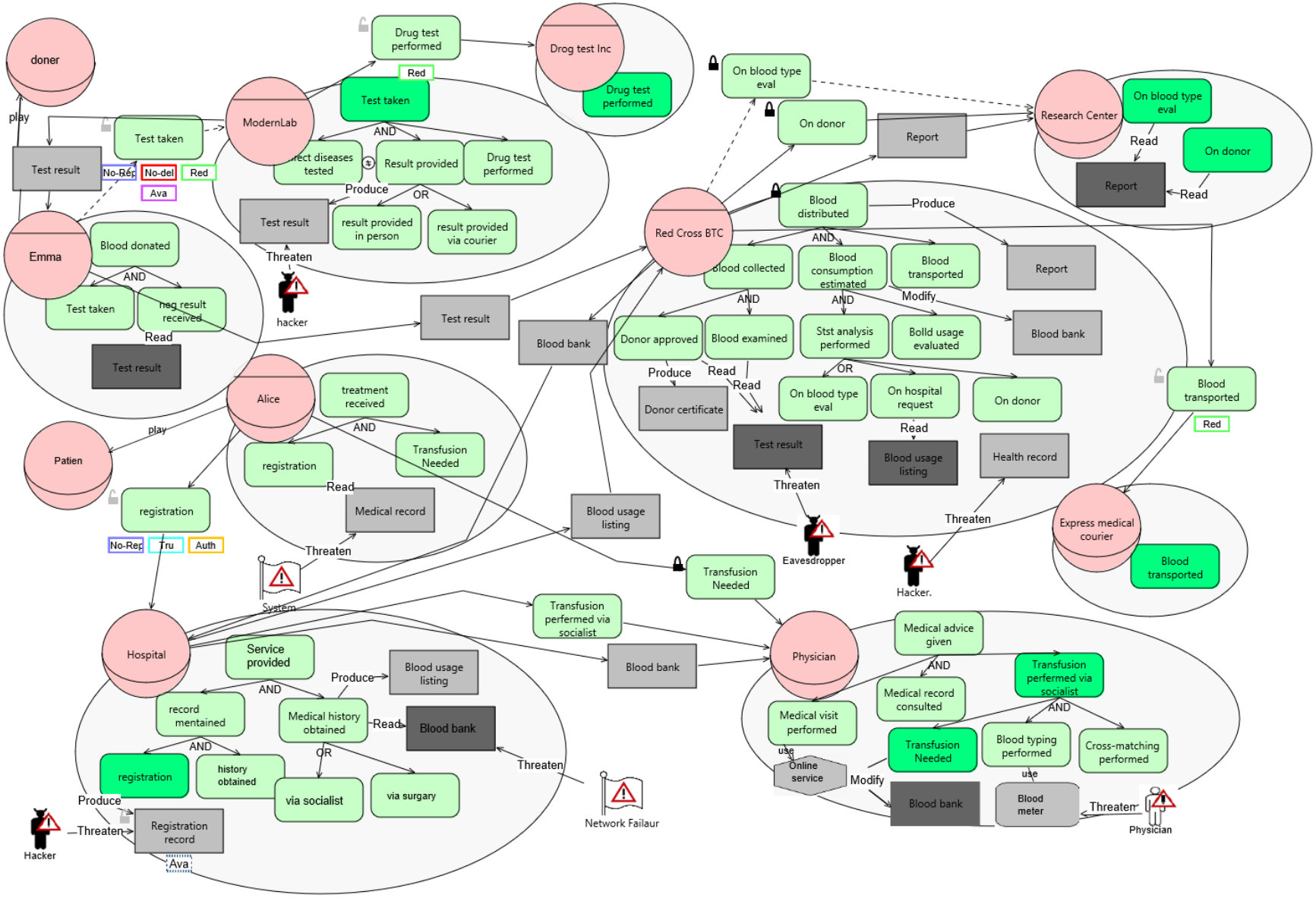

Figure 1- Social View for the Healthcare Example

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

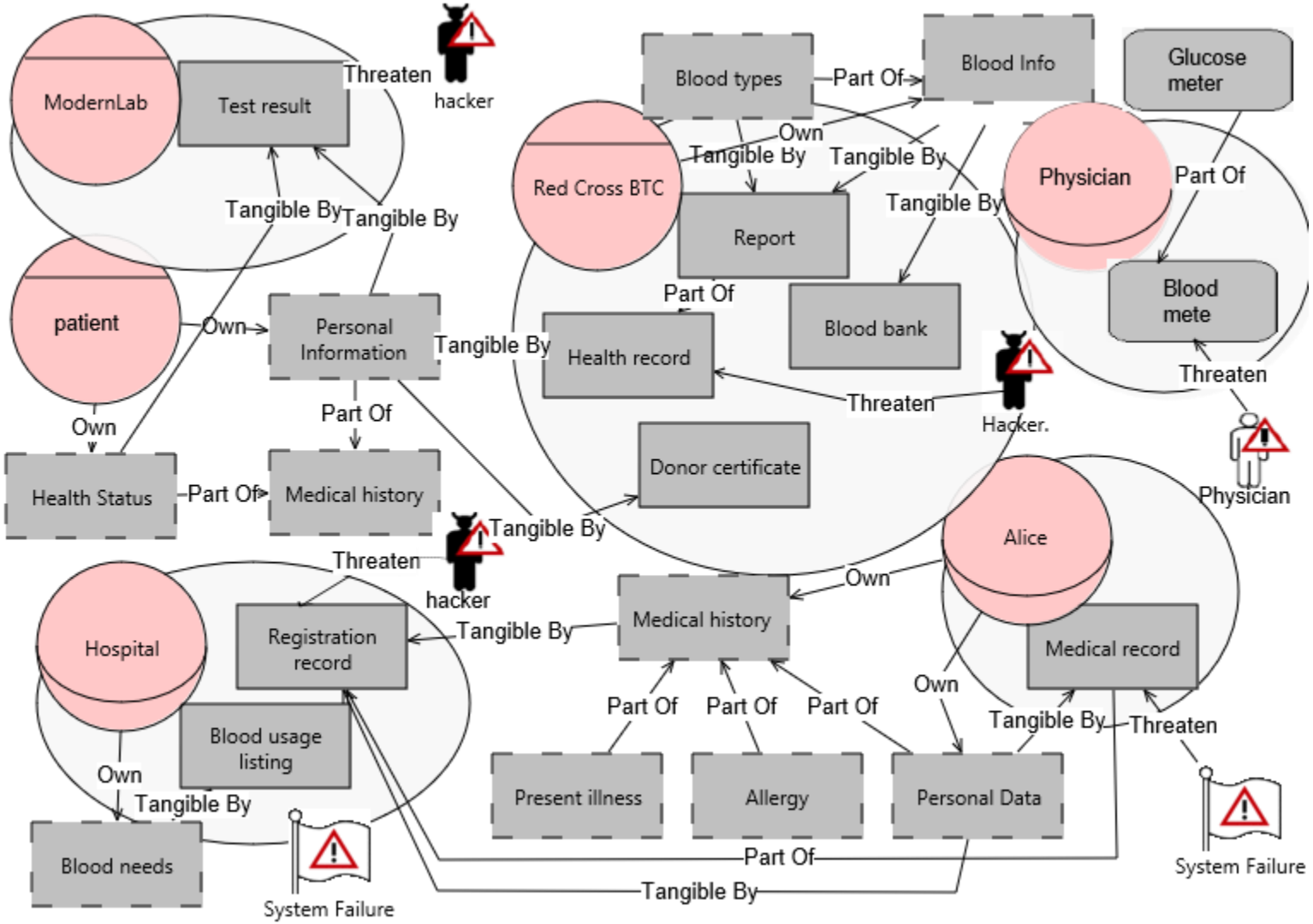

Figure 2- The Asset View of the Healthcare Example.

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					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					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.

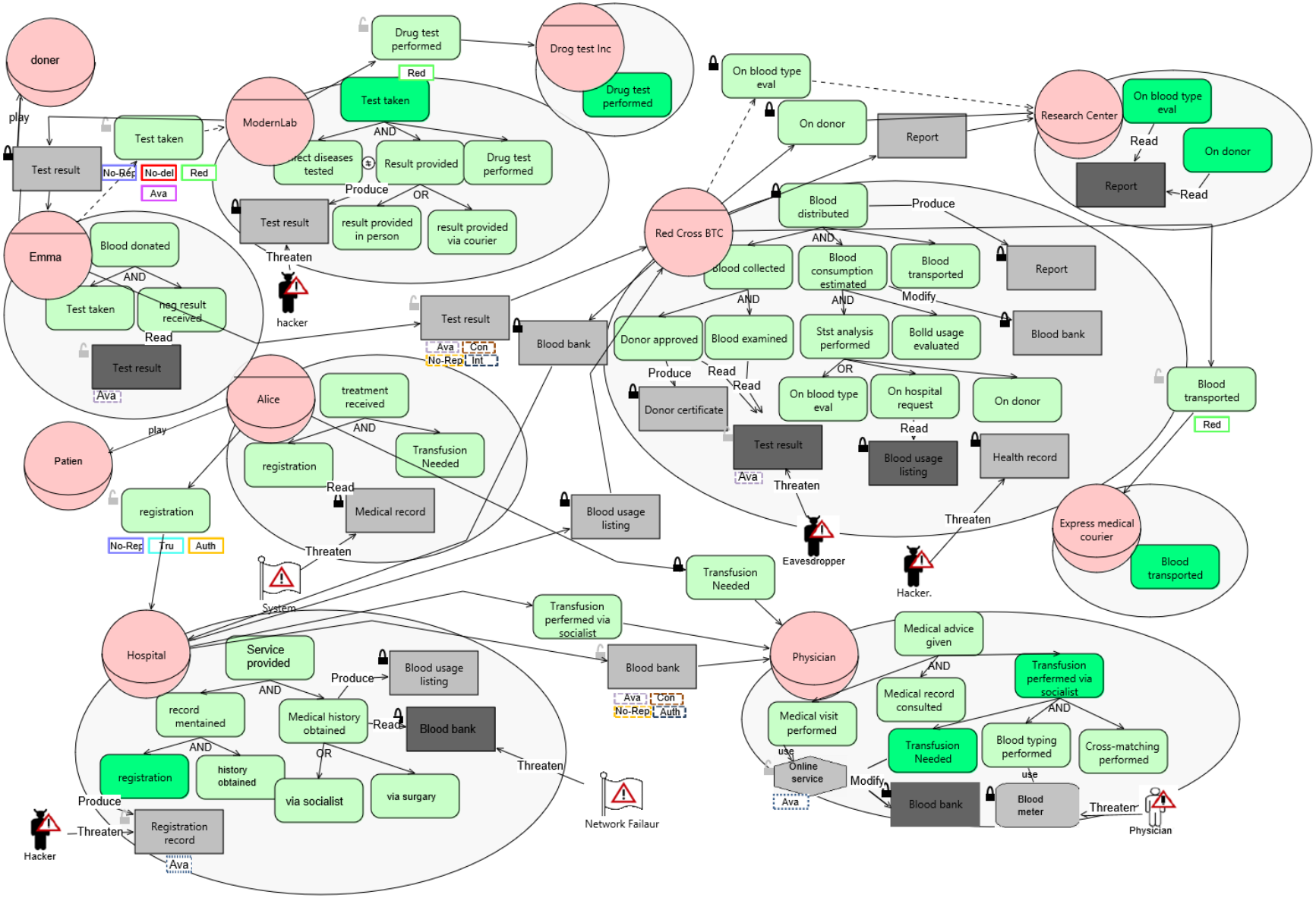

Figure 21- Security Requirements According to Values Has Assigned

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

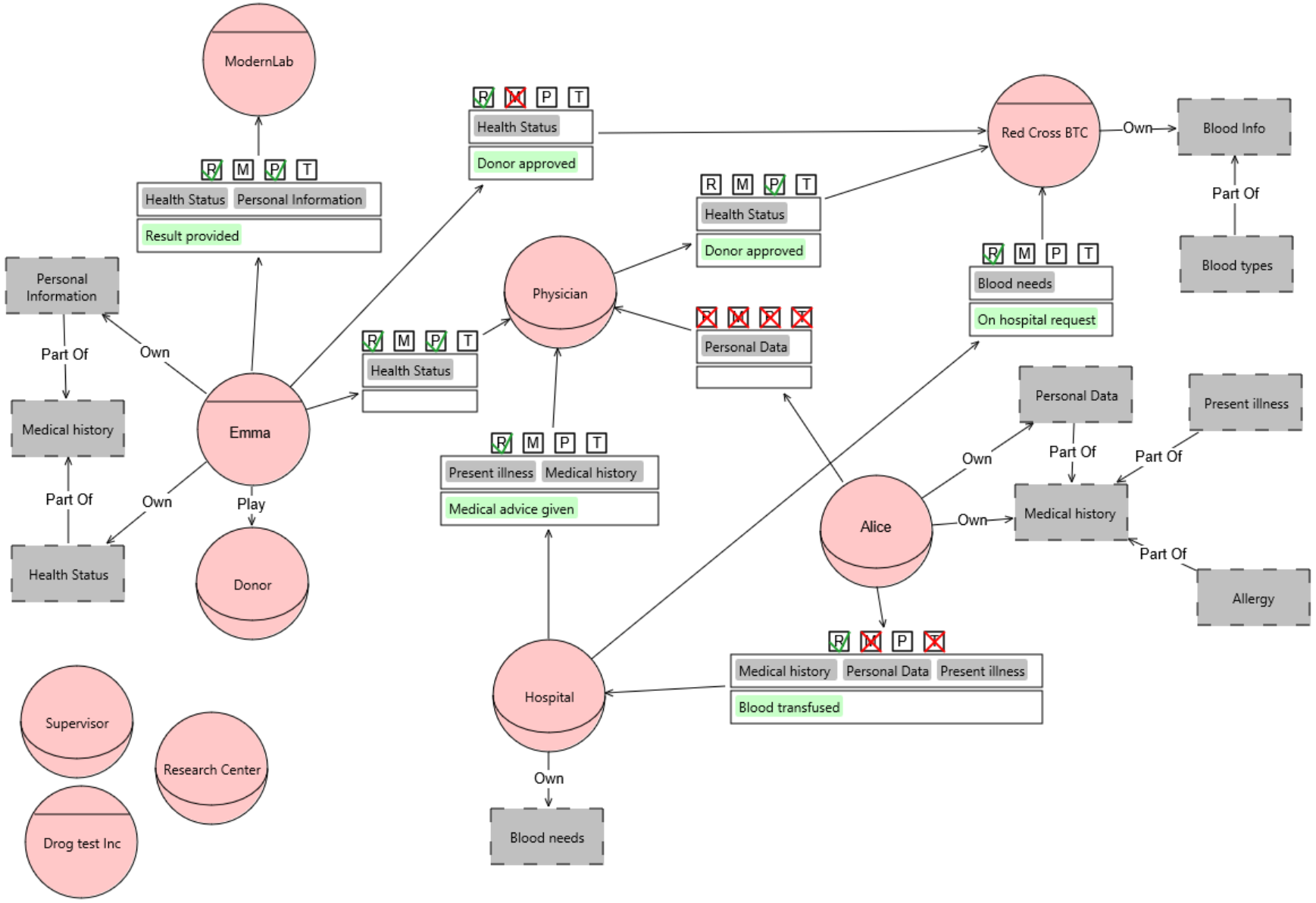

Figure 22-Figure 2- The Authorization View of the Healthcare Example.

Authorization Property

Property	Value
Name	Hospital- Red Cross BTC
Duration of authorization	**During Contract**
Act on Termination	**Distroy**

Figure 23. Hospital-Patient Authorization Property

Property	Value
Name	Emm-Moden lab
Duration of authorization	**During treatment**
Act on Termination	**Distroy**

Figure 24-Emma-Modern Lab Authorization Property

Property	Value
Name	Emm-Red Cross BTC
Duration of authorization	**During treatment**
Act on Termination	**Return**

Figure 25-Emma-Red Cross BTC Authorization Property

Property	Value
Name	Physician-Red Cross BTC
Duration of authorization	**3 month**
Act on Termination	**Return**

Figure 26-Physician-Red Cross BTC Authorization Property

Property	Value
Name	Emm-Physician
Duration of authorization	**During treatment**
Act on Termination	**Return**

Figure 28- Emma-Physician Authorization Property

Property	Value
Name	Hospital- Physician
Duration of authorization	**During contract**
Act on Termination	**Return**

Figure 27-Hospital- Physician Authorization Property

Property	Value
Name	Alice-Physician
Duration of authorization	**During treatment**
Act on Termination	**Return**

Figure 29-Alice-Physician Authorization Property

Property	Value
Name	Alice-Hospital
Duration of authorization	**During treatment**
Act on Termination	**Return**

Figure 30-Alice-Hospital 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

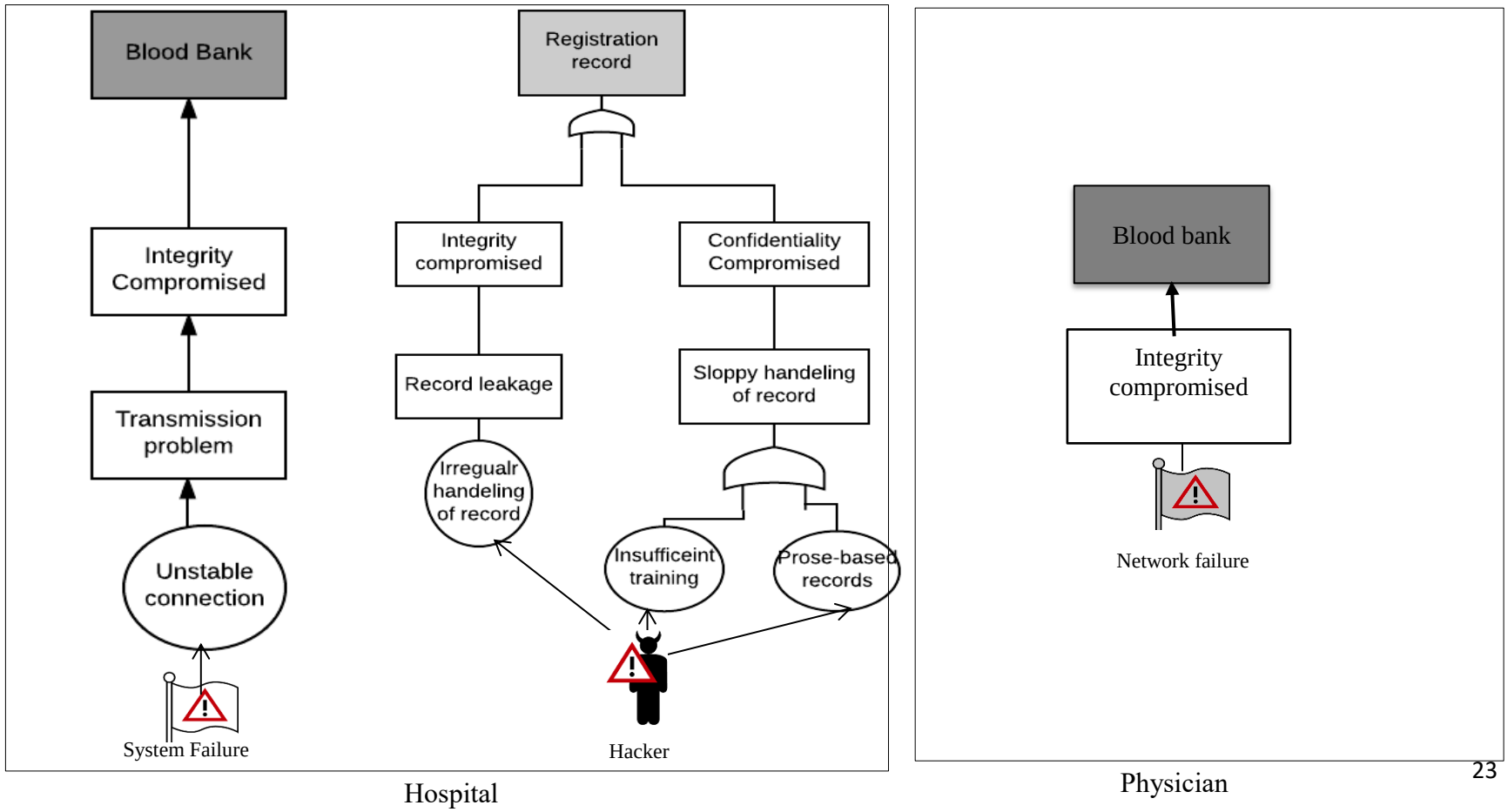

Figure 31-Threat View (I)

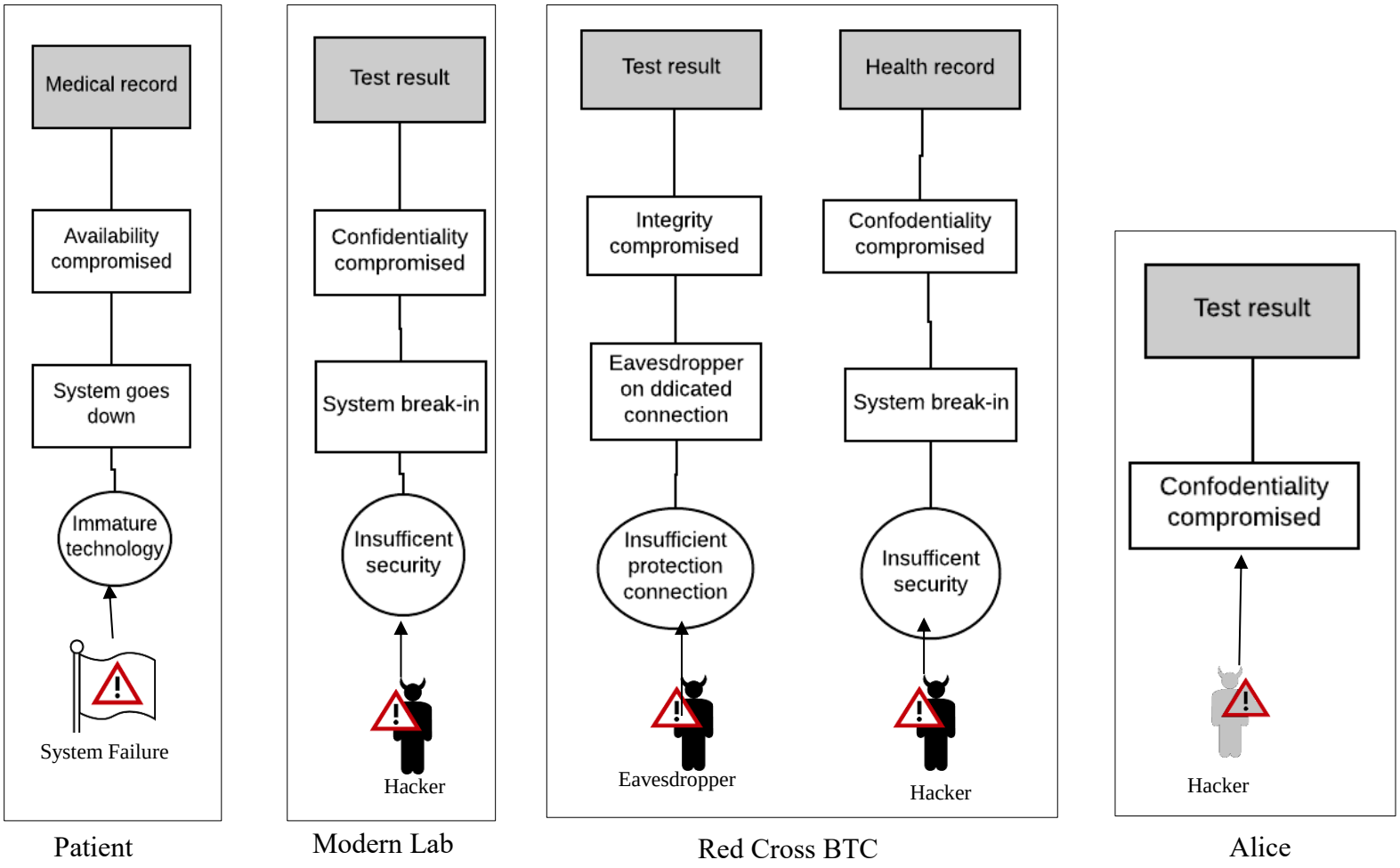

Figure 32-Threat View (II)

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.

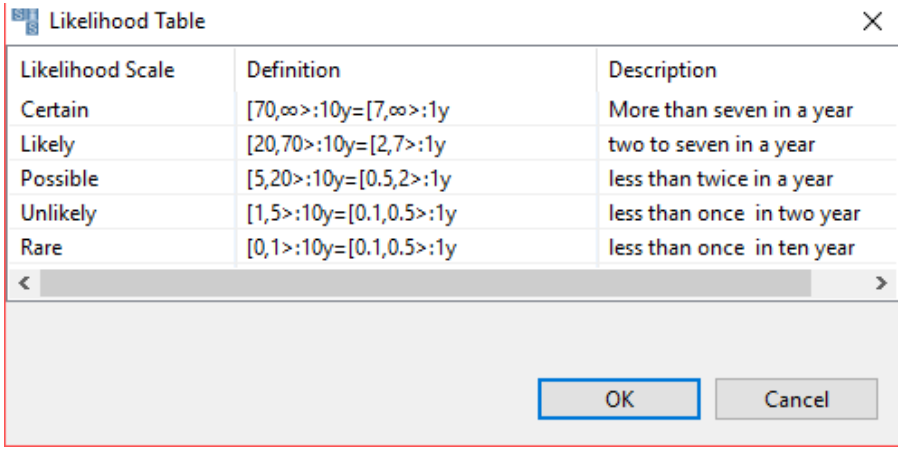

Figure 33-Alice Likelihood Table

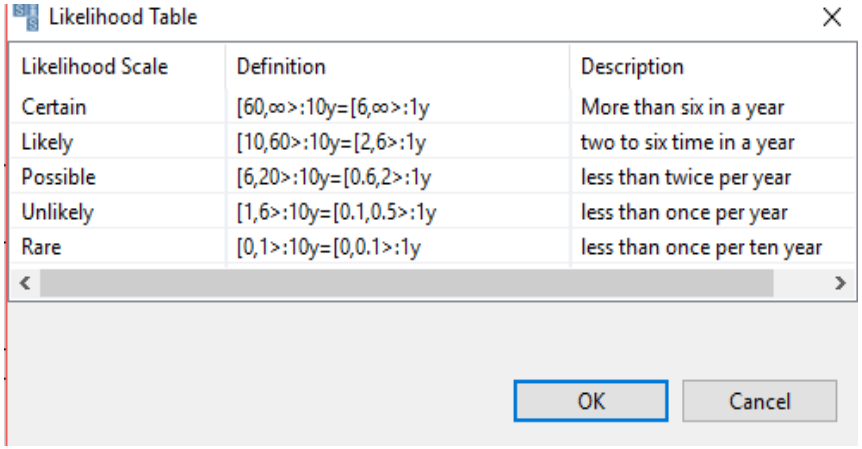

Figure 34- Modern lab Likelihood Table

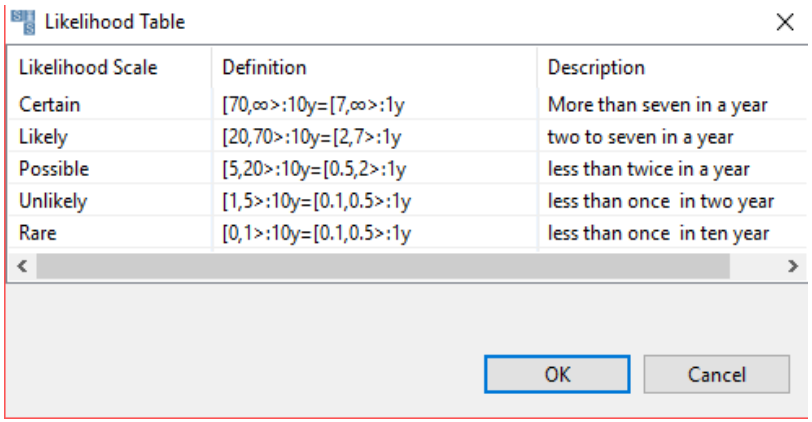

Figure 35-Red Cross BTC Likelihood Table

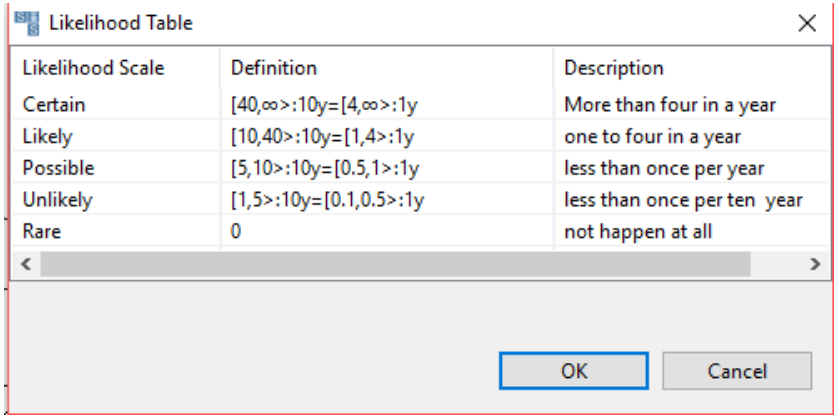

Figure 36- Patient Likelihood Table

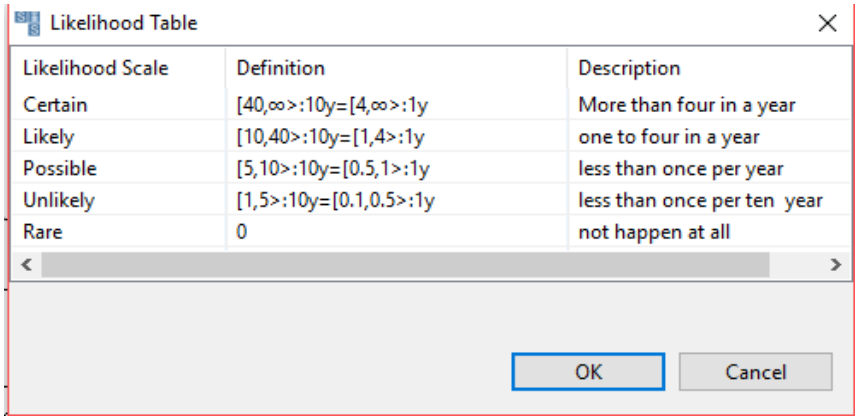

Figure 37- Hospital Likelihood Table

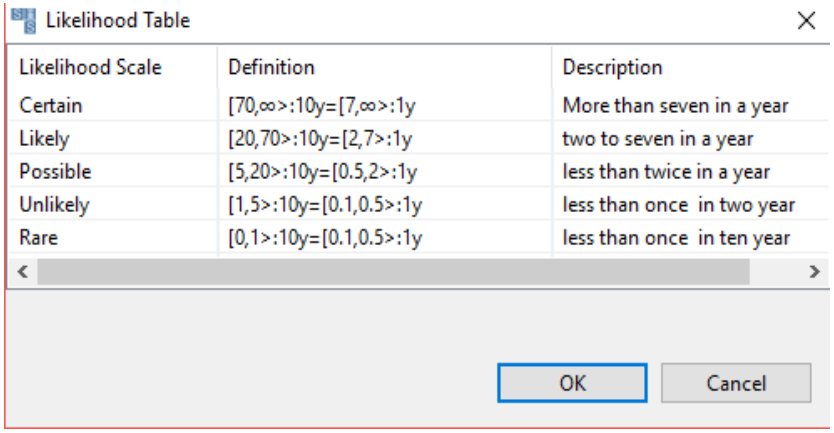

Figure 38- Physician Likelihood Table

Consequance Tables

Hospital Documents Affected Documents)

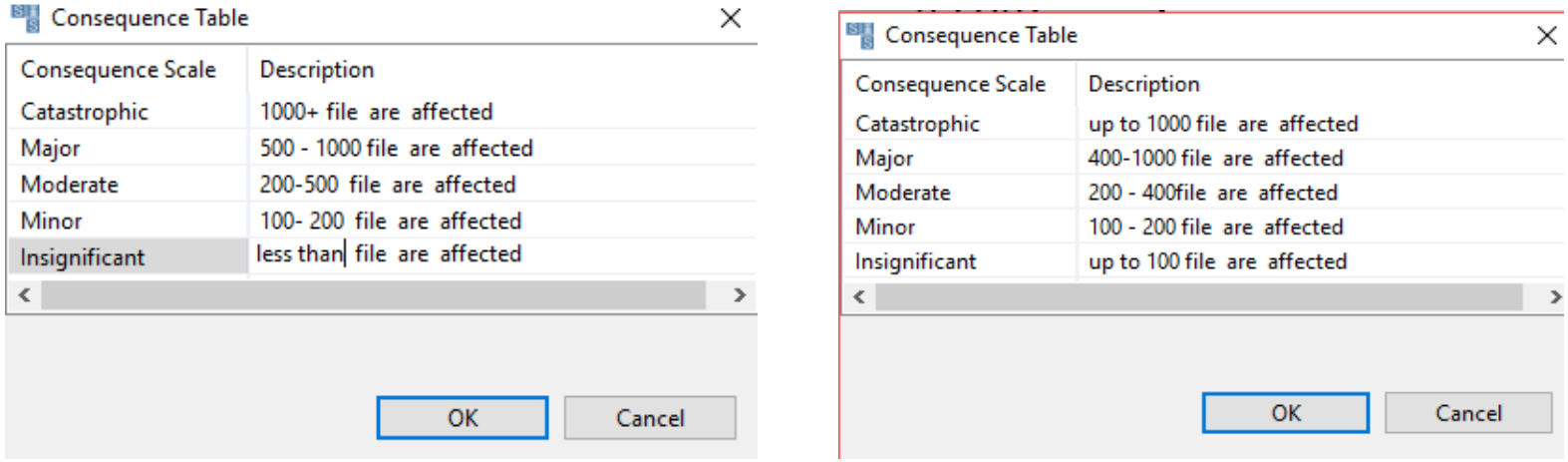

Figure 39. Blood Bank-Registration Record

Red Cross BTC Affected Documents

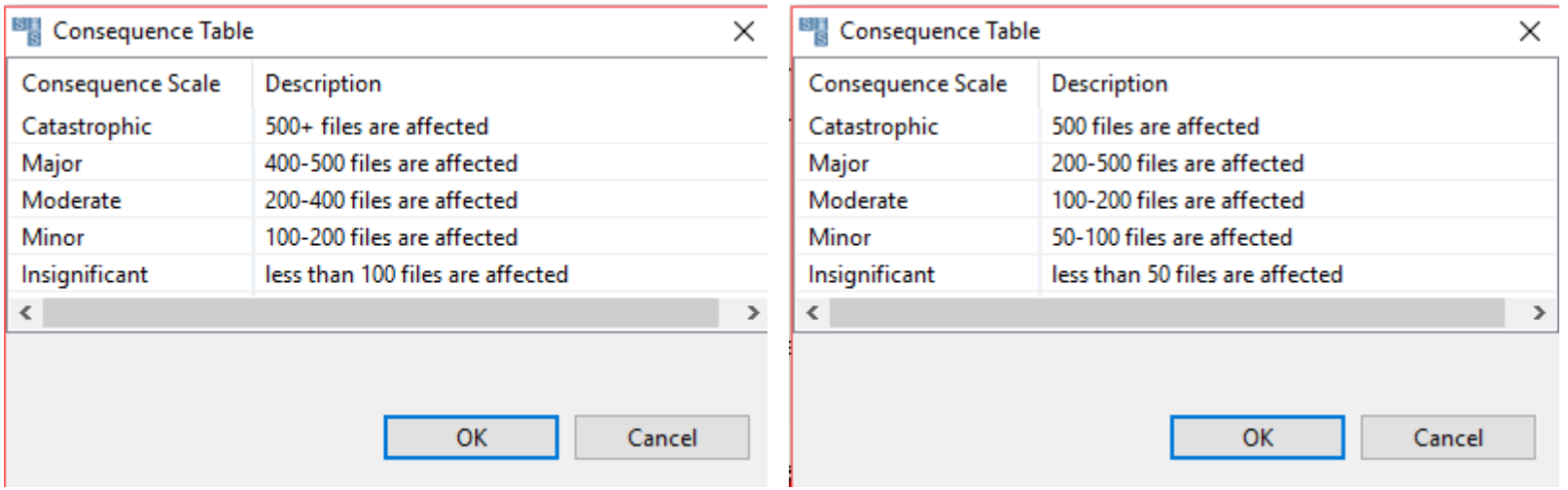

Figure 40.Test Result - Health Record

Modern Lab Affected Document

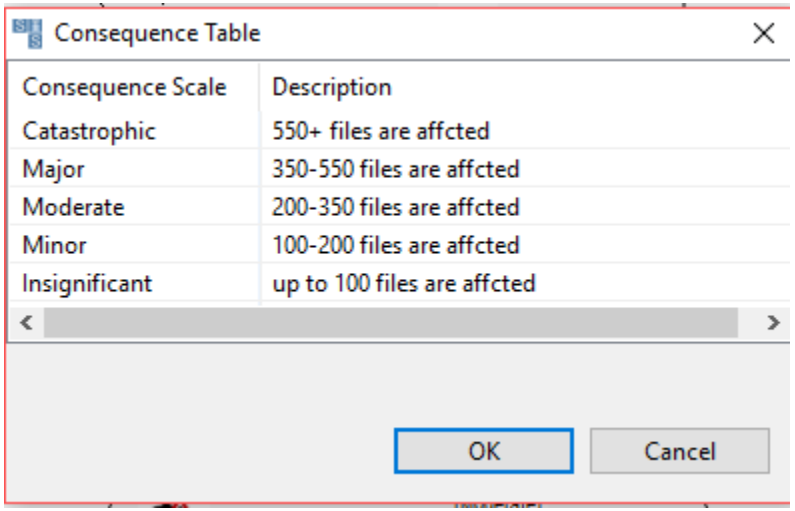

Figure 41.Test Result

Patient Affected Document

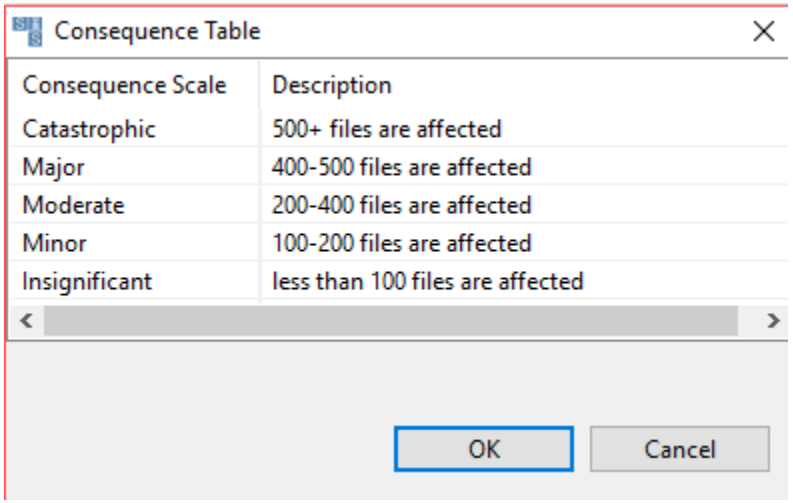

Figure 42. Medical Record

Alice Affected Document

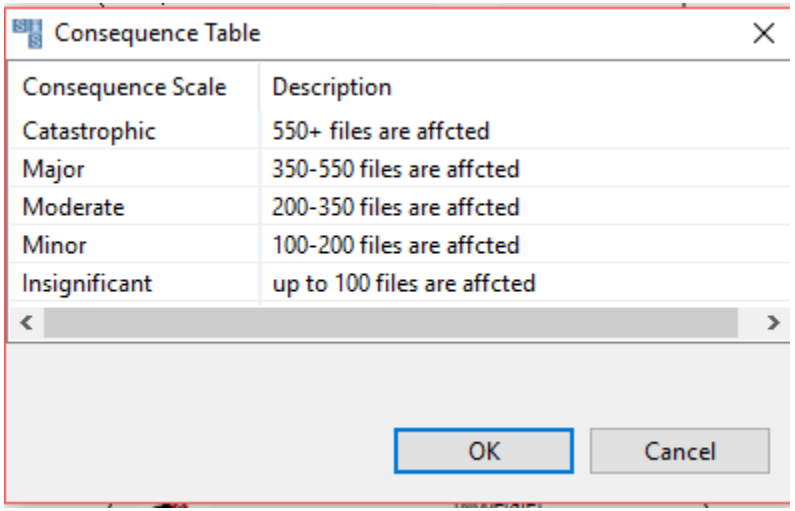

Figure 43.Test Result

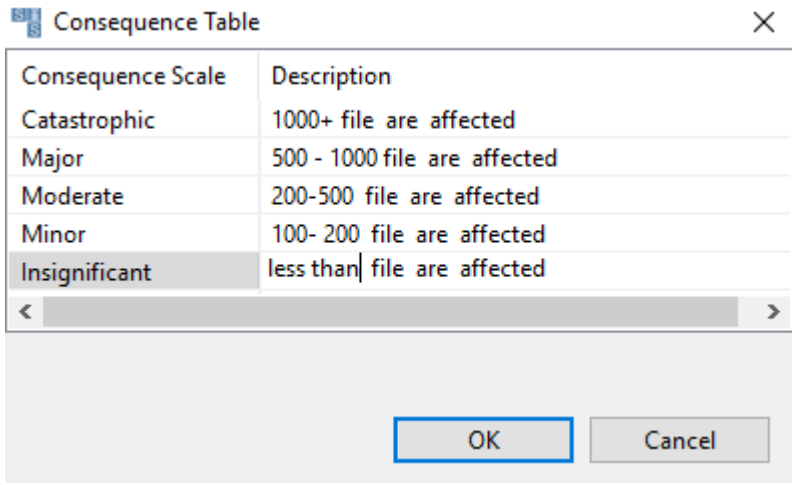

Figure 44. Blood Bank

Threat View Diagram Together with the Scales

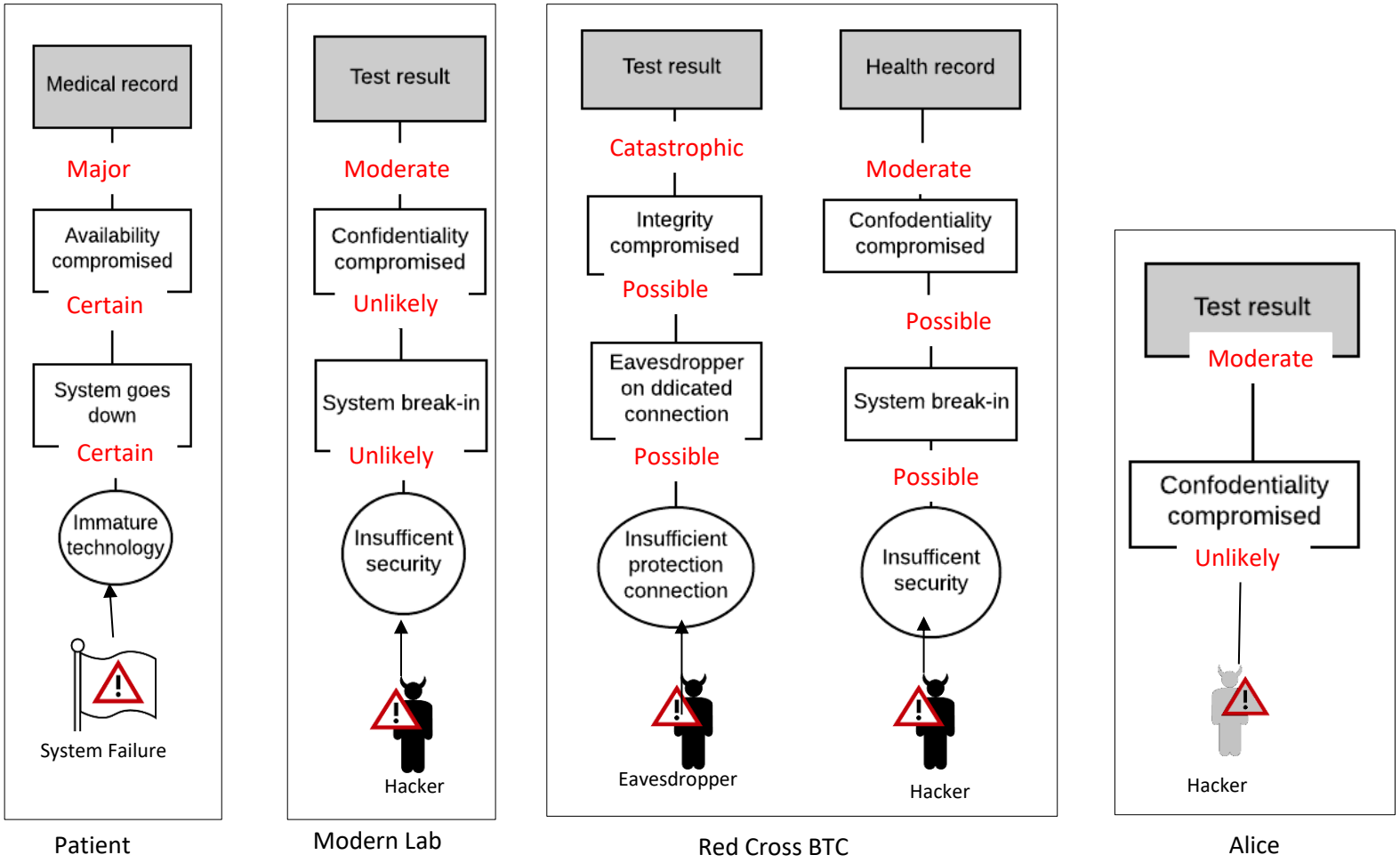

Figure 45-Threat View(I)- Scales Assigned

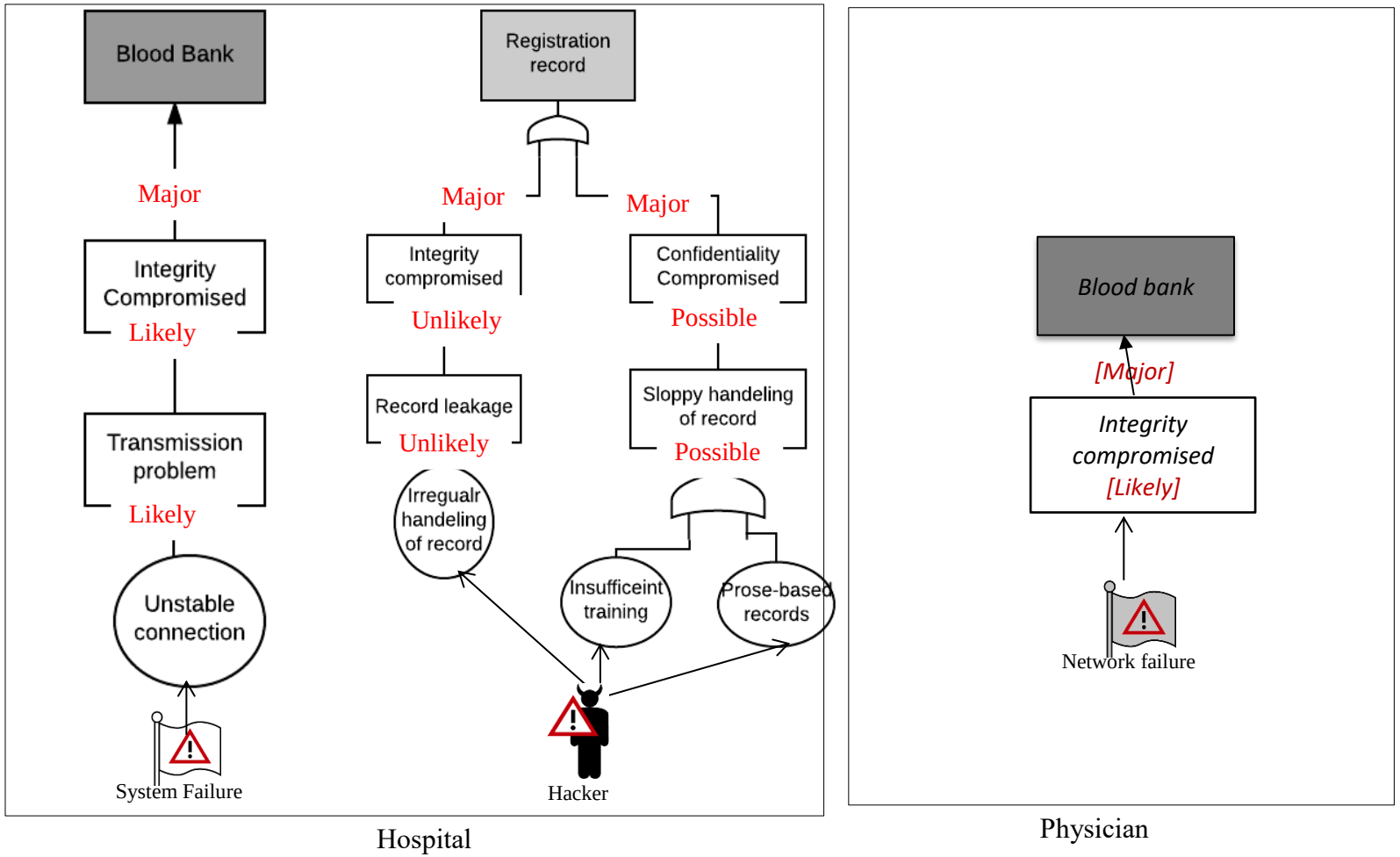

Figure 46-Threat View(II)- Scales Assigned

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.

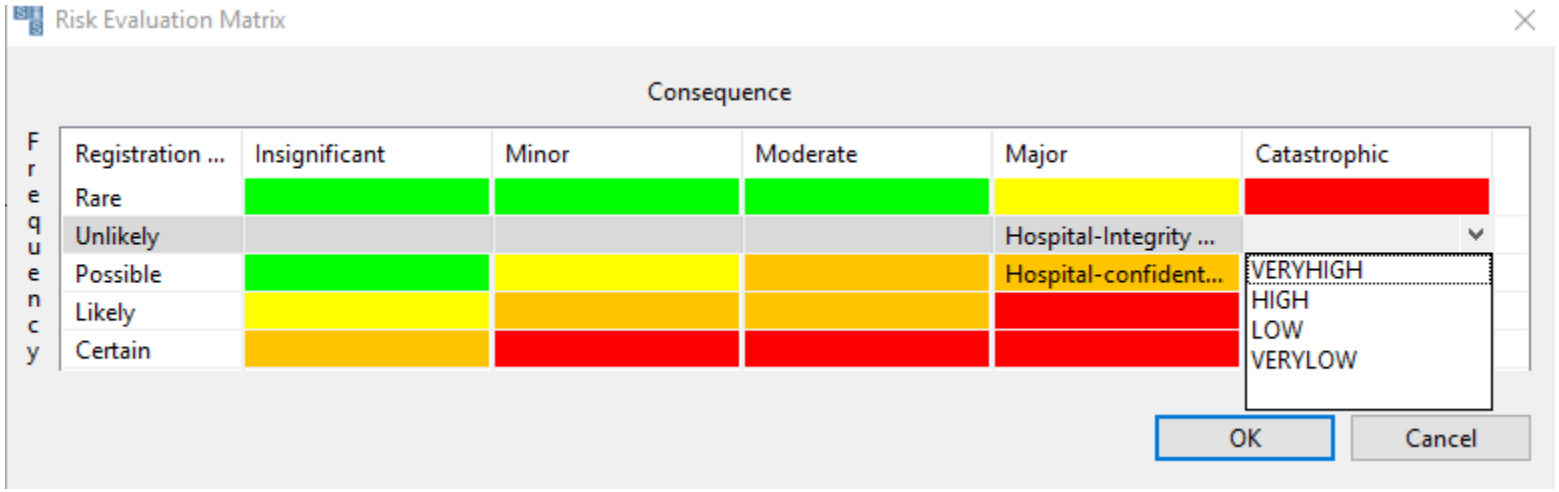

Figure 47. Hospital – Document Registration Record

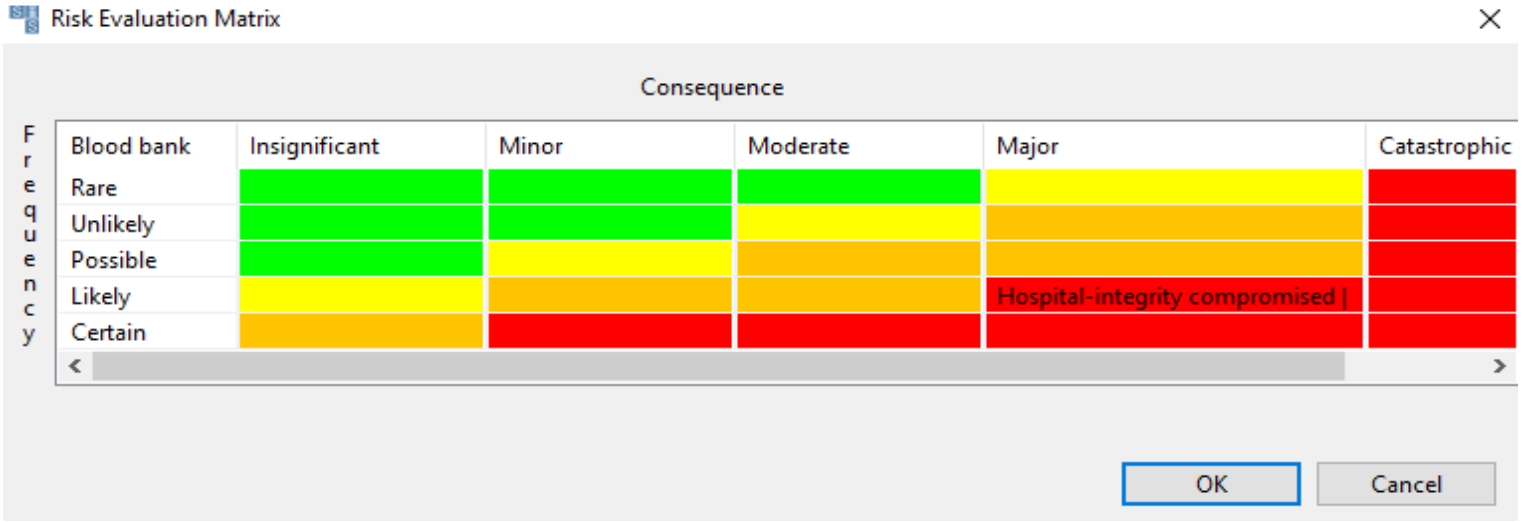

Figure 48- Hospital Bank Risk Evaluation matrix

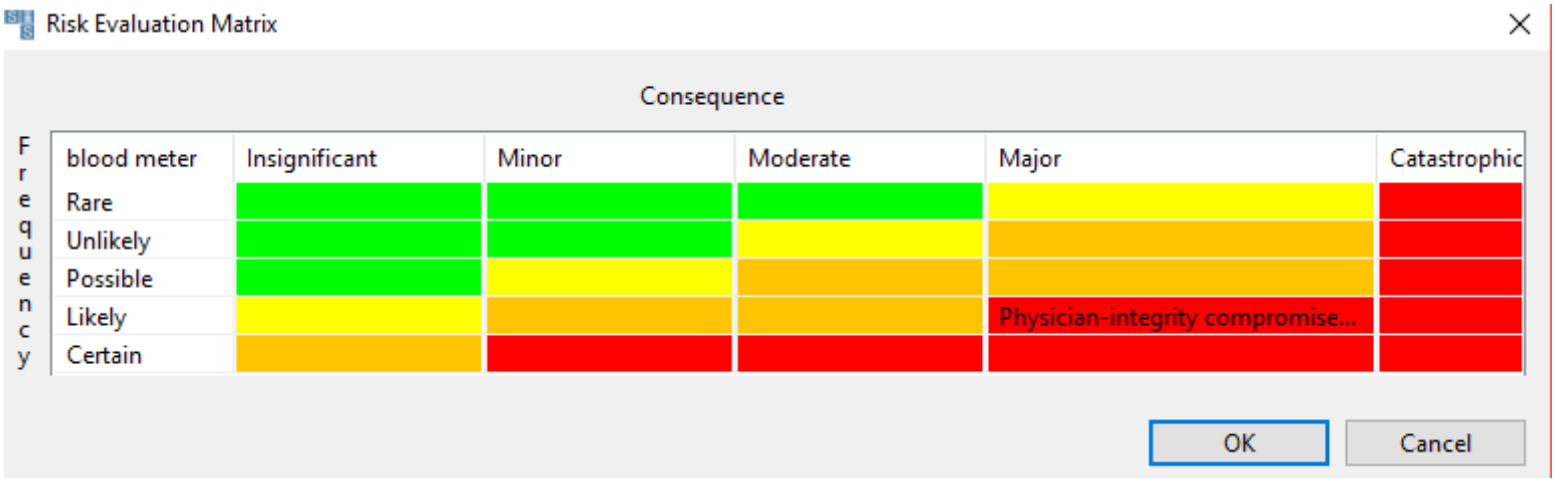

Figure 50- Physician Risk Evaluation matrix

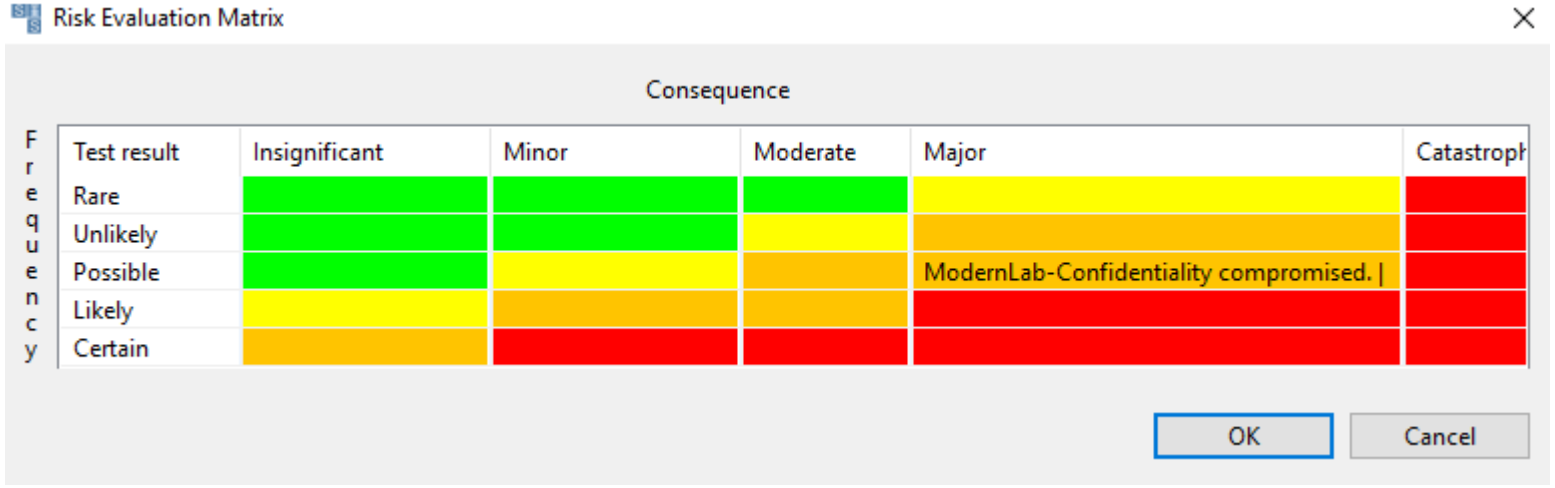

Figure 51 Modern Lab Risk Evaluation matrix

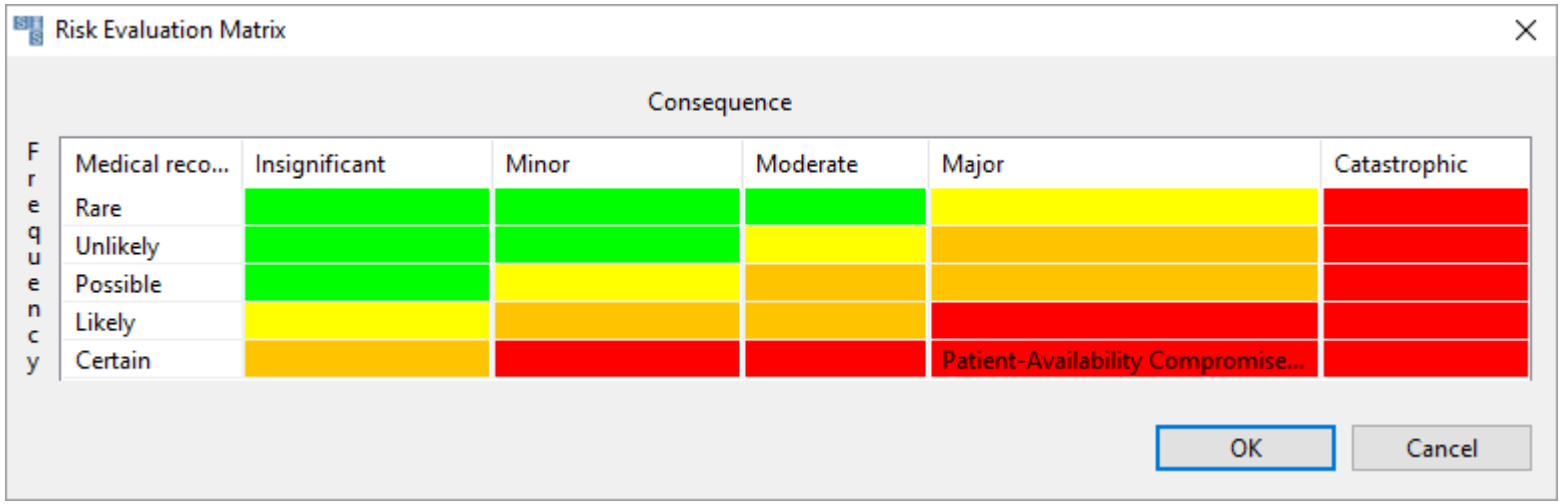

Figure 52- Patient Risk Evaluation matrix

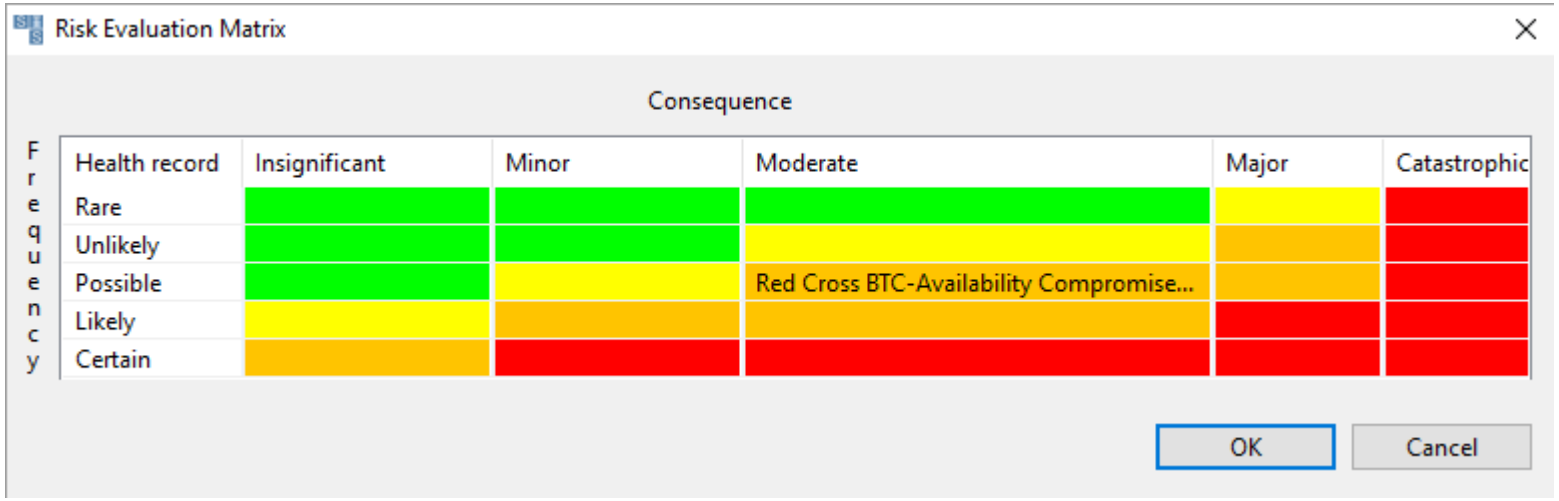

Figure 53- Red Cross Risk Evaluation matrix

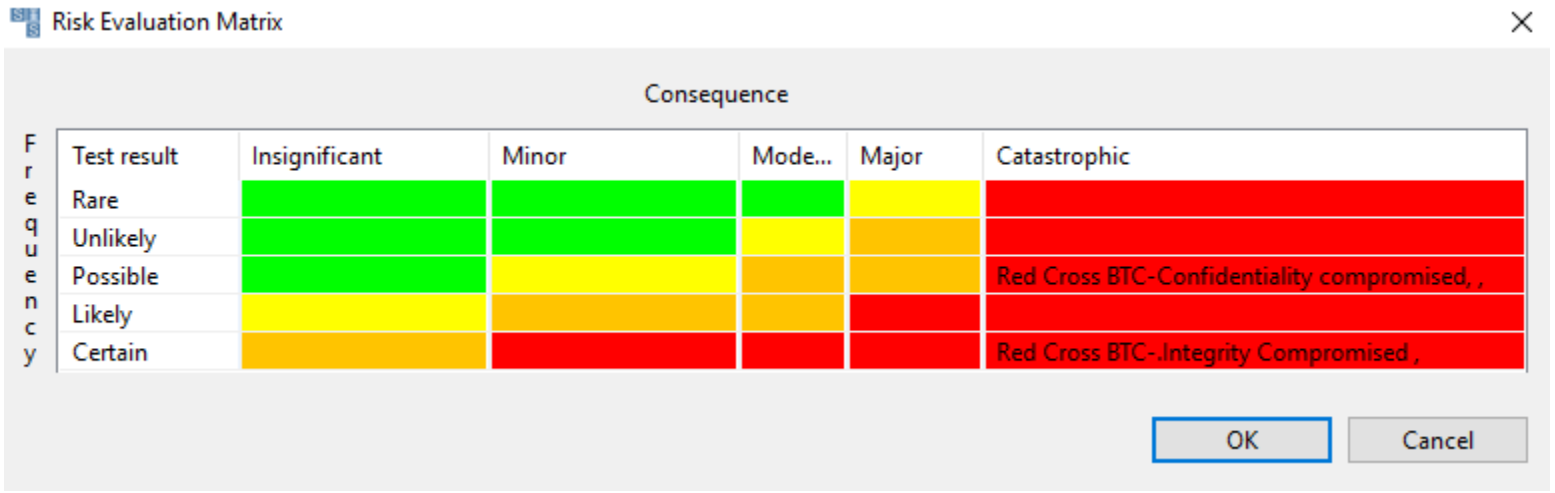

Figure 54-Risk Evaluation matrix

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.

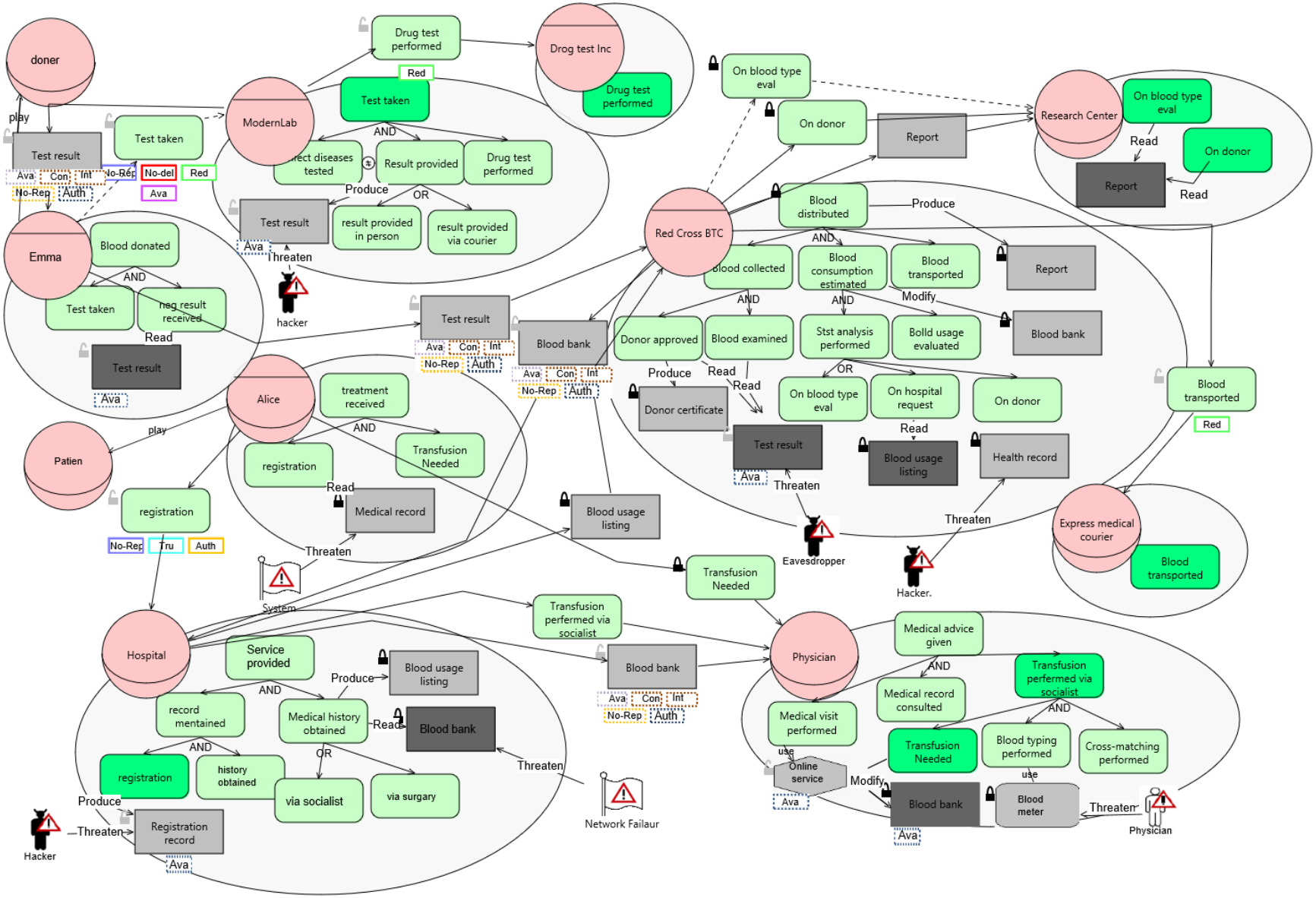

Figure 55- Improvement /added Security Requirements to the Social View as Treatment

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

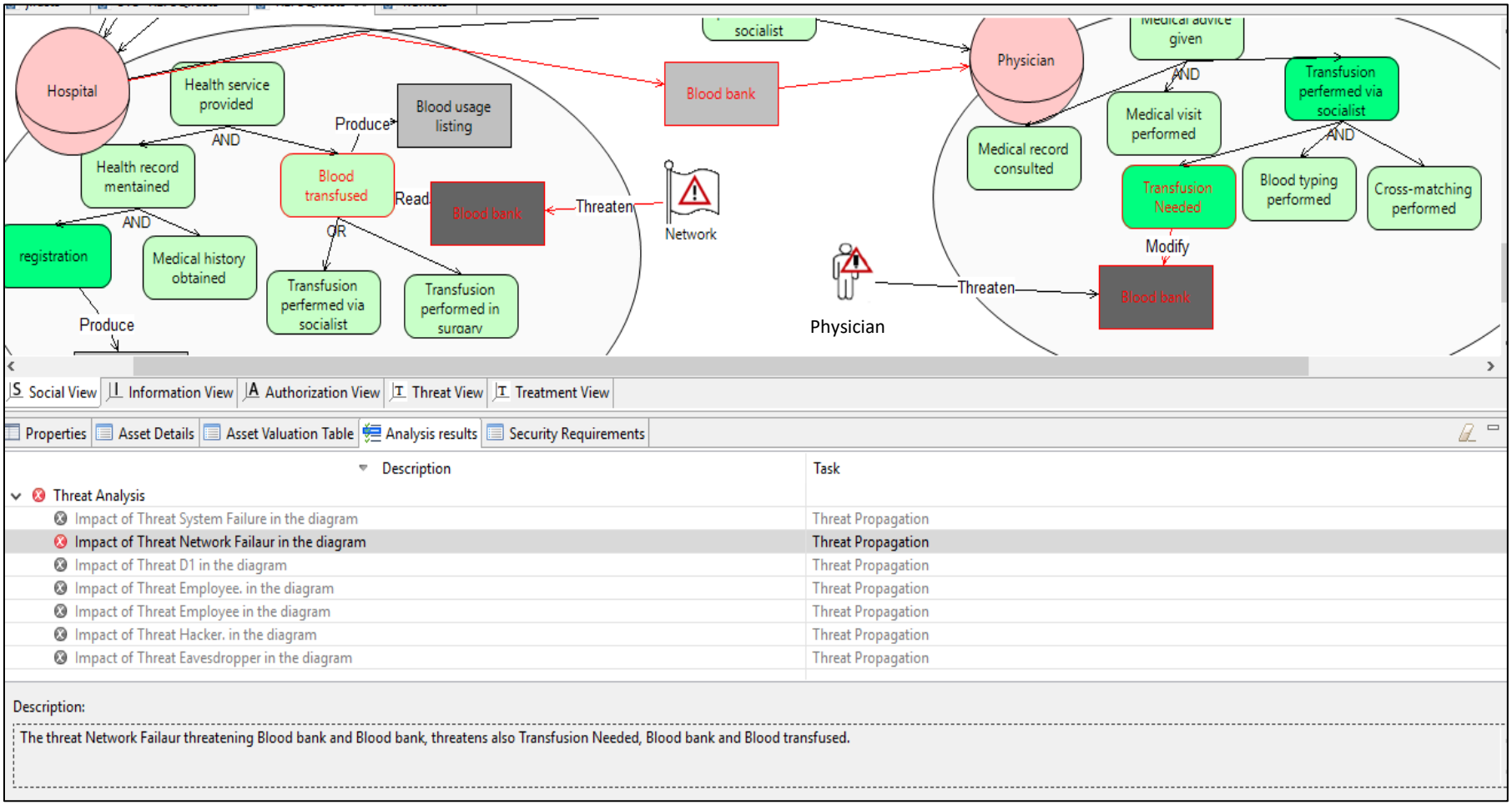

Figure 56.Propagation of via transmission and their impact on achieving goals

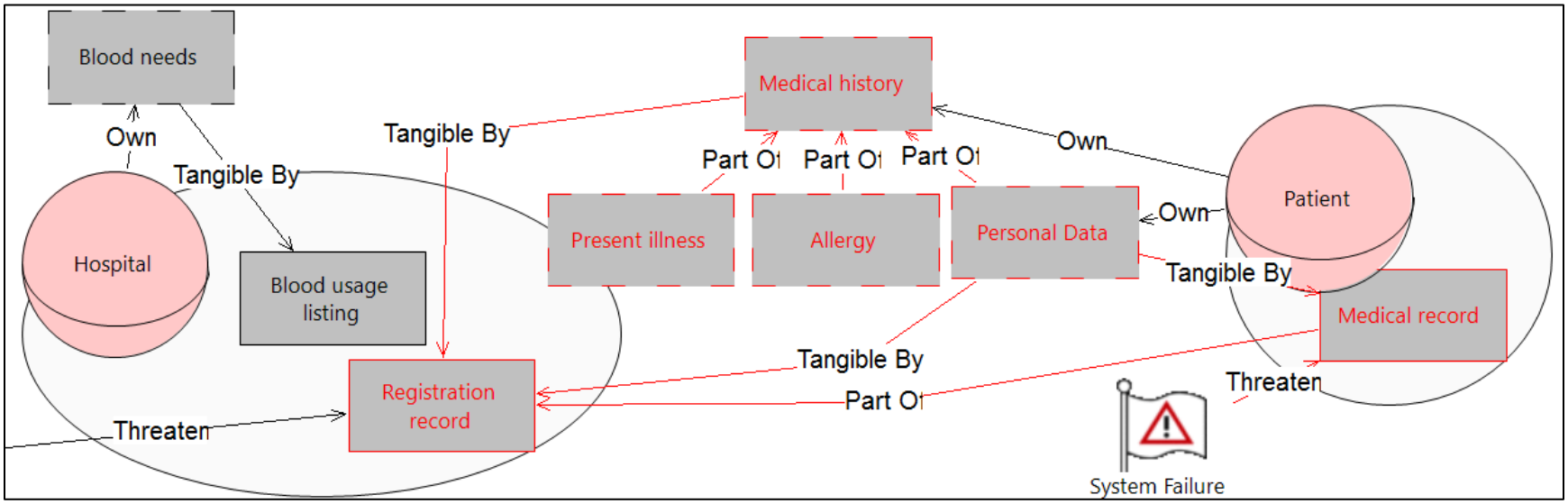

Figure 57, Propagation via Document/information structure

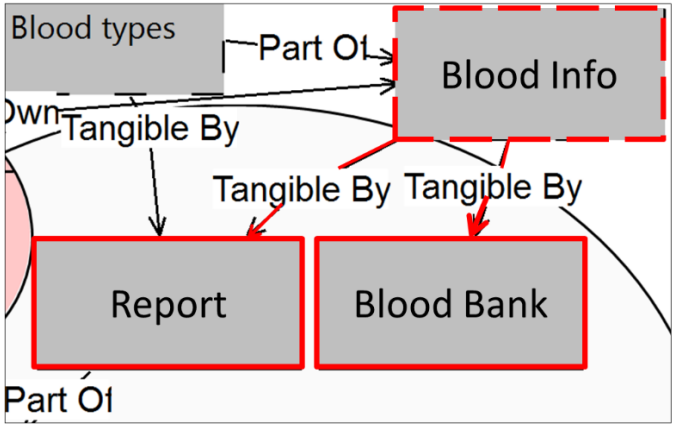

Figure 58.a. Number of Copy Violated

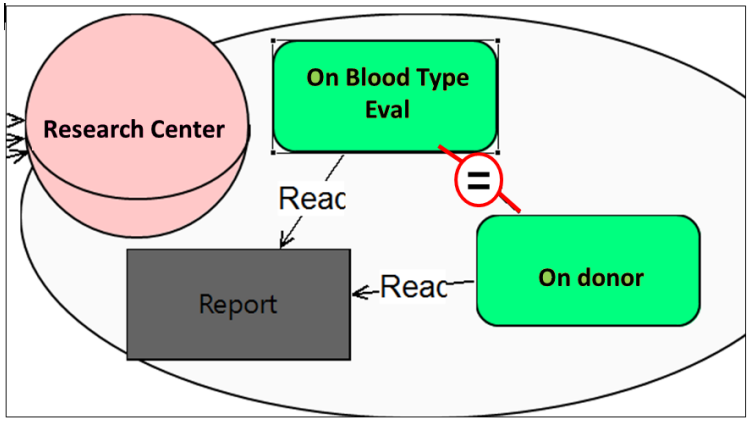

Figure 59.b. Number of User Violation