Security Analysis results
Inf 5150
Drop 2
Group 2
November 18, 2005

Table of contents

Introduction

This report documents the results of a risk analysis of the general BlindDate1 system as specified by the sequence diagrams RegisterCustomer, JoinEvent and NotifyCustomers. The analysis is done on behalf of the system owner.

We assume that BindDate is a system that is established and run as a business enterprise, i.e. that there exists a set of customers and that the enterprise has a regular income.

1 Context identification

1.1 Target of Evaluation

Type: Table
Name: Target of Evaluation
Short description:
Concern: Target of evaluation
Viewpoint:
Finalised:
Full description:

Table 1: Target Of Evaluation Table

Category	Value
Target	The BlindDate system as specified by the sequence diagrams RegisterCustomer, JoinEvent and NotifyCustomer. The target also includes the owner of the system and its customers.
Client	The BlindDate system owner.
Service/Function	Customer registration, the customers' activity of joining events and the systems communication of travel advice to the customers. These functions and services are described by the sequence diagrams RegisterCustomer, JoinEvent and NotifyCustomer, respectively.
Quality aspects	Confidentiality, integrity and availability of information in addition to service level.

1.2 Value Definitions

Type: Table
Name: Value Definitions
Short description:
Concern: Target of evaluation
Viewpoint:
Finalised:
Full description:

Table 2: Value Definition Table

Type	Domain	Allowed values	Description
Asset	NOK	Very low, Low, Medium, High, Very High	Very low: [0-10,000) Low: [10,000-100,000) Medium: [100,000-1mill) High: [1mill-10mill) Very high: [10 mill-)
Frequency	Occurences/ year	Rare, Unlikely, Possible, Likely, Certain	Rare: Less than 1/100, i.e. [0-0.01) Unlikely: [1/100-1/10), i.e. [0.01-0.1) Possible: [1/10-1/5), i.e [0.1-0.2) Likely: [1/5-1/1), i.e. [0.2-1) Certain: More than 1/1, i.e. 1
Consequence	NOK	Insignificant, Minor, Moderate, Major, Catastrophic	Insignificant: [0-10,000) Minor: [10,000-100,000) Moderate: [100,000-1mill) Major: [1mill-10mill) Catastrophic: [10 mill-)
Risk value		Low, Medium, High	

Risk Value Function

The risk value function is a function from a frequency value and a consequence value to a risk value. The function is for simplicity given as a matrix.

		Frequency				
		Rare	**Unlikely**	**Possible**	**Likely**	**Certain**
Consequence	**Insignificant**	Low	Low	Low	Low	Medium
	Minor	Low	Low	Low	Medium	Medium
	Moderate	Low	Low	Medium	Medium	High
	Major	Low	Medium	Medium	High	High
	Catastrophic	Medium	Medium	High	High	High

1.3 Assets

Type:	Table
Name:	Assets
Short description:	
Concern:	Assets
Viewpoint:	
Finalised:	
Full description:	

Table 3: Asset Table

Asset ID	Description	Category	Value
A1_Existing customers	Existing customers	Human	Very High
A2_Customer DB	Customer DB	Information	High
A3_Event DB	Event DB	Information	Medium
A4_Reputation	Reputation	Other	Medium
A5_Revenue	Revenue	Other	High
A6_Customer Trust	Customer Trust	Other	High

1.4 Risk Evaluation Criteria

Type:	Table
Name:	Risk Evaluation Criteria
Short description:	
Concern:	Risk evaluation criteria
Viewpoint:	
Finalised:	
Full description:	

Table 4: Risk Evaluation Criteria Table

Criteria ID	Criteria	Description	Applied for assets
C1	Risk value “Low”: Accept risk		All
C2	Risk value “Medium”: Monitor risk		All
C3	Risk value “High”: Treat risk		All

2 Risk identification

2.1 HazOp

Type: Table
Name: HazOp
Short description:
Concern: Threats
Viewpoint:
Finalised:
Full description:

Table 5: HazOp Table

Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
A2_Customer DB	BDSystem	Employee	Critical hardware unprotected	Critical hardware is damaged	Employee accidentally spills beverage on critical hardware
A3_Event DB	BDSystem	Employee	Critical hardware unprotected	Critical hardware is damaged	Employee accidentally spills beverage on critical hardware
A1_Existing customers	BDSystem	Employee	Critical hardware unprotected	Loss of customers	Employee accidentally spills beverage on critical hardware, critical hardware is damaged, system service is down
A5_Revenue	BDSystem	Employee	Critical hardware unprotected	Loss of customers	Employee accidentally spills beverage on critical hardware, critical hardware is damaged, system service is down
A1_Existing customers	BDSystem	Employee	Employees are allowed to connect personal laptop to system.	Loss of customers	Employee connects personal virus infected laptop to system, virus attack on system, system software is damaged, system service is down
A5_Revenue	BDSystem	Employee	Employees are allowed to connect personal laptop to system.	Loss of customers	Employee connects personal virus infected laptop to system, virus attack on system, system software is damaged, system service is down
A1_Existing customers	BDSystem	Employee	Employees are allowed to connect personal laptop to system.	Loss of customers	Employee connects personal virus infected laptop to system, virus attack on system, data is destroyed, system service is down
A5_Revenue	BDSystem	Employee	Employees are allowed to connect personal laptop to system.	Loss of customers	Employee connects personal virus infected laptop to system, virus attack on system, data is destroyed, system service is down
A2_Customer DB	:ControllerSM	Employee	Employees are allowed to connect personal laptop to system.	Data destroyed	Employee connects personal virus infected laptop to system, virus attack

Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
					on system
A3_Event DB	:Event	Employee	Employees are allowed to connect personal laptop to system.	Data destroyed	Employee connects personal virus infected laptop to system, virus attack on system
A2_Customer DB	BDSystem	Unfaithful employee	Insufficient background check of employees	Critical hardware is damaged	Employee deliberately damages hardware
A3_Event DB	BDSystem	Unfaithful employee	Insufficient background check of employees	Critical hardware is damaged	Employee deliberately damages hardware
A1_Existing customers	BDSystem	Unfaithful employee	Insufficient background check of employees	Loss of customers	Employee deliberately damages critical hardware, critical hardware is damaged, system service is down
A5_Revenue	BDSystem	Unfaithful employee	Insufficient background check of employees	Loss of customers	Employee deliberately damages critical hardware, critical hardware is damaged, system service is down
A1_Existing customers	BDSystem	Unfaithful employee	Insufficient background check of employees	Loss of customers	Employee deliberately damages system software, system service is down
A5_Revenue	BDSystem	Unfaithful employee	Insufficient background check of employees	Loss of customers	Employee deliberately damages system software, system service is down
A1_Existing customers	BDSystem	E-mail client, employee	Insufficient virus detection of e-mail	Loss of customers	Employee receives e-mail with virus, virus attack on system, system software is damaged, system service is down
A5_Revenue	BDSystem	E-mail client, employee	Insufficient virus detection of e-mail	Loss of customers	Employee receives e-mail with virus, virus attack on system, system software is damaged, system service is down
A1_Existing customers	BDSystem	E-mail client, employee	Insufficient virus detection of e-mail	Loss of customers	Employee receives e-mail with virus, virus attack on system, data is destroyed, system service is down
A5_Revenue	BDSystem	E-mail client, employee	Insufficient virus detection of e-mail	Loss of customers	Employee receives e-mail with virus, virus attack on system, data is destroyed, system service is down
A2_Customer DB	:ControllerSM	E-mail client, employee	Insufficient virus detection of e-mail	Data destroyed	Employee receives e-mail with virus, virus attack on system
A3_Event DB	:Event	E-mail client, employee	Insufficient virus detection of e-mail	Data destroyed	Employee receives e-mail with virus, virus attack on system
A4_Reputation	sd JoinEvent, sd NotifyCustomers	Eavesdropper	Weakness in firewall, communication not encrypted	Customer data is spread	Eavesdropper picks up data on customers
A6_Customer Trust	sd JoinEvent, sd	Eavesdropper	Weakness in	Customer data is	Eavesdropper picks

Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
	NotifyCustomers		firewall, communication not encrypted	spread	up data on customers
A1_Existing customers	sd JoinEvent, sd NotifyCustomers	Eavesdropper	Weakness in firewall, communication not encrypted	Customer data is spread	Eavesdropper picks up data on customers
A1_Existing customers	sd JoinEvent, sd NotifyCustomers	Eavesdropper	Weakness in firewall, communication not encrypted	Business competitor uses customer data	Eavesdropper picks up data on customers, customer data is spread
A5_Revenue	sd JoinEvent, sd NotifyCustomers	Eavesdropper	Weakness in firewall, communication not encrypted	Business competitor uses customer data	Eavesdropper picks up data on customers, customer data is spread
A1_Existing customers	sd JoinEvent, sd NotifyCustomers	Eavesdropper	Weakness in firewall, communication not encrypted	Loss of customers	Eavesdropper picks up data on customers, customer data is spread
A5_Revenue	sd JoinEvent, sd NotifyCustomers	Eavesdropper	Weakness in firewall, communication not encrypted	Loss of customers	Eavesdropper picks up data on customers, customer data is spread
A4_Reputation	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Customer data is spread	Unfaithful employee leaks customer data
A6_Customer Trust	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Customer data is spread	Eavesdropper picks up data on customers
A1_Existing customers	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Customer data is spread	Unfaithful employee leaks customer data
A1_Existing customers	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Business competitor uses customer data	Unfaithful employee leaks customer data, customer data is spread
A5_Revenue	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Business competitor uses customer data	Unfaithful employee leaks customer data, customer data is spread
A1_Existing customers	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Loss of customers	Unfaithful employee leaks customer data, customer data is spread
A5_Revenue	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Loss of customers	Unfaithful employee leaks customer data, customer data is spread
A1_Existing customers	sd JoinEvent, sd NotifyCustomers	Press	Weakness in firewall, communication not encrypted. Insufficient background check of employees	Negative press coverage	Eavesdropper or unfaithful employee leaks sensitive information
A4_Reputation	sd JoinEvent, sd NotifyCustomers	Press	Weakness in firewall, communication not encrypted. Insufficient background check of employees	Negative press coverage	Eavesdropper or unfaithful employee leaks sensitive information
A5_Revenue	sd JoinEvent, sd NotifyCustomers	Press	Weakness in firewall, communication not encrypted. Insufficient background check of employees	Negative press coverage	Eavesdropper or unfaithful employee leaks sensitive information
A6_Customer Trust	sd JoinEvent, sd NotifyCustomers	Press	Weakness in firewall,	Negative press coverage	Eavesdropper or unfaithful employee

Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
			communication not encrypted. Insufficient background check of employees		leaks sensitive information
A1_Existing customers	sd JoinEvent, sd NotifyCustomers	Press	Weakness in firewall, communication not encrypted. Insufficient background check of employees	Loss of customers	Eavesdropper or unfaithful employee leaks sensitive information, negative press coverage
A5_Revenue	sd JoinEvent, sd NotifyCustomers	Press	Weakness in firewall, communication not encrypted. Insufficient background check of employees	Loss of customers	Eavesdropper or unfaithful employee leaks sensitive information, negative press coverage
A2_Customer DB	:ControllerSM	Unfaithful employee	Insufficient background check of employees	Data destroyed	Unfaithful employee deliberately destroys data
A3_Event DB	:Event	Unfaithful employee	Insufficient background check of employees	Data destroyed	Unfaithful employee deliberately destroys data
A1_Existing customers	BDSystem	Unfaithful employee	Insufficient background check of employees	Loss of customers	Unfaithful employee deliberately destroys data, service is down
A5_Revenue	BDSystem	Unfaithful employee	Insufficient background check of employees	Loss of customers	Unfaithful employee deliberately destroys data, service is down
A2_Customer DB	:ControllerSM	Hacker	Weakness in firewall	Data destroyed	Hacker hacks into the system, unauthorised access
A3_Event DB	:Event	Hacker	Weakness in firewall	Data destroyed	Hacker hacks into the system, unauthorised access
A1_Existing customers	:ControllerSM	Hacker	Weakness in firewall	Customer data is spread	Hacker hacks into the system, unauthorised access
A6_Customer Trust	:ControllerSM	Hacker	Weakness in firewall	Customer data is spread	Hacker hacks into the system, unauthorised access
A4_Reputation	:ControllerSM	Hacker	Weakness in firewall	Customer data is spread	Hacker hacks into the system, unauthorised access
A1_Existing customers	:ControllerSM	Hacker	Weakness in firewall	Business competitor uses customer data	Hacker hacks into the system, unauthorised access, customer data is spread
A5_Revenue	:ControllerSM	Hacker	Weakness in firewall	Business competitor uses customer data	Hacker hacks into the system, unauthorised access, customer data is spread
A1_Existing customers	BDSystem	Hacker	Weakness in firewall	Loss of customers	Hacker hacks into the system, unauthorised access, data destroyed, system service is down
A5_Revenue	BDSystem	Hacker	Weakness in firewall	Loss of customers	Hacker hacks into the system, unauthorised access, data destroyed, system service is down
A1_Existing customers	:ControllerSM	Hacker	Weakness in firewall	Loss of customers	Hacker hacks into the system, unauthorised access, customer data is spread

Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
A5_Revenue	:ControllerSM	Hacker	Weakness in firewall	Loss of customers	Hacker hacks into the system, unauthorised access, customer data is spread
A2_Customer DB	:ControllerSM	Hacker	Weakness in firewall	Data destroyed	Hacker hacks into the system, unauthorised access
A3_Event DB	:Event	Hacker	Weakness in firewall	Data destroyed	Hacker hacks into the system, unauthorised access

Unwanted Incident Diagram

The following CORAS UML profile diagram models the risks that of a level that demands treatments. Table 6 below documents the risk value of all the identified unwanted incidents, and we see that it is the “Loss of customers” and the “Data destroyed” scenarios whose frequency and/or consequence that must be reduced.

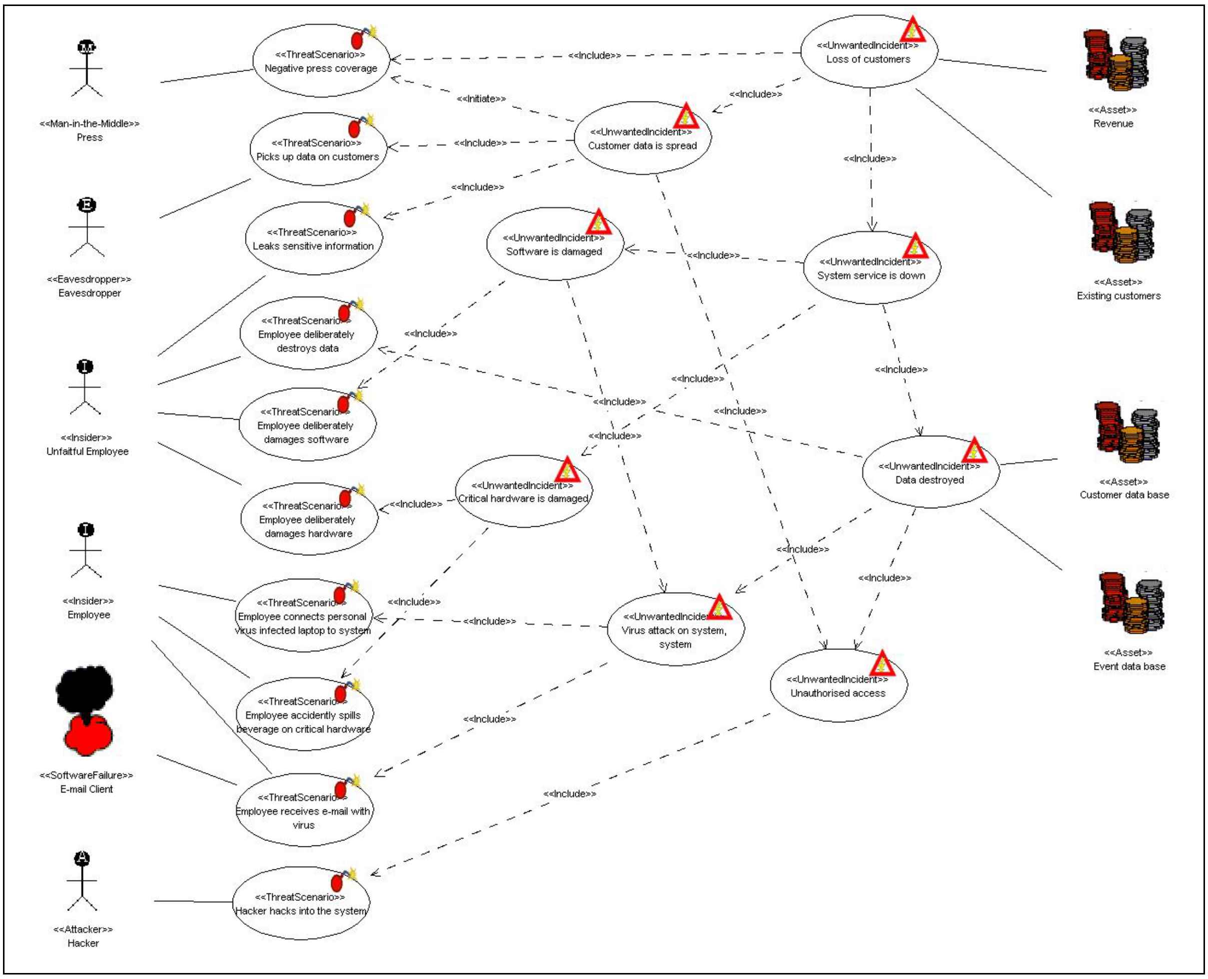

Figure 1: Unwanted incidents

3 Risk analysis

3.1 Consequence and Frequency

Type: Table
Name: Consequence and Frequency
Short description:
Concern: Consequence
Viewpoint:
Finalised:
Full description:

Table 6: Consequence and Frequency Table

Risk ID	Asset ID	Incident	Consequence Value	Frequency Value	Risk Value
R1	A2_Customer DB	Critical hardware is damaged	Catastrophic	Unlikely	Medium
R2	A3_Event DB	Critical hardware is damaged	Catastrophic	Unlikely	Medium
R3	A1_Existing customers	Loss of customers	Moderate	Certain	High
R4	A5_Revenue	Loss of customers	Moderate	Certain	High
R5	A2_Customer DB	Data destroyed	Catastrophic	Possible	High
R6	A3_Event DB	Data destroyed	Catastrophic	Possible	High
R7	A4_Reputation	Customer data is spread	Minor	Possible	Low
R8	A6_Customer Trust	Customer data is spread	Minor	Possible	Low
R9	A1_Existing customers	Customer data is spread	Minor	Possible	Low
R10	A1_Existing customers	Business competitor uses customer data	Moderate	Possible	Medium
R11	A5_Revenue	Business competitor uses customer data	Moderate	Possible	Medium
R12	A1_Existing customers	Negative press coverage	Major	Unlikely	Medium
R13	A4_Reputation	Negative press coverage	Major	Unlikely	Medium
R14	A5_Revenue	Negative press coverage	Major	Unlikely	Medium
R15	A6_Customer Trust	Negative press coverage	Major	Unlikely	Medium

4 Risk evaluation

Risk Matrix

The risk matrix below shows the consequence and frequency of each of the identified unwanted incidents. Each cell corresponds to a risk level: The light grey area corresponds to low risks, the white area to medium risks and the dark grey area to high risks. According to the risk evaluation criteria, the row risks are acceptable, the medium risks should be monitored, while the high risks should be treated.

		Frequency				
		Rare	**Unlikely**	**Possible**	**Likely**	**Certain**
Consequence	**Insignificant**					
	Minor			R7 R8 R9		
	Moderate			R10 R11		R3 R4
	Major		R12 R13 R14 R15			
	Catastrophic		R1 R2	R5 R6		

5 Risk treatment

Risk Treatment Diagram

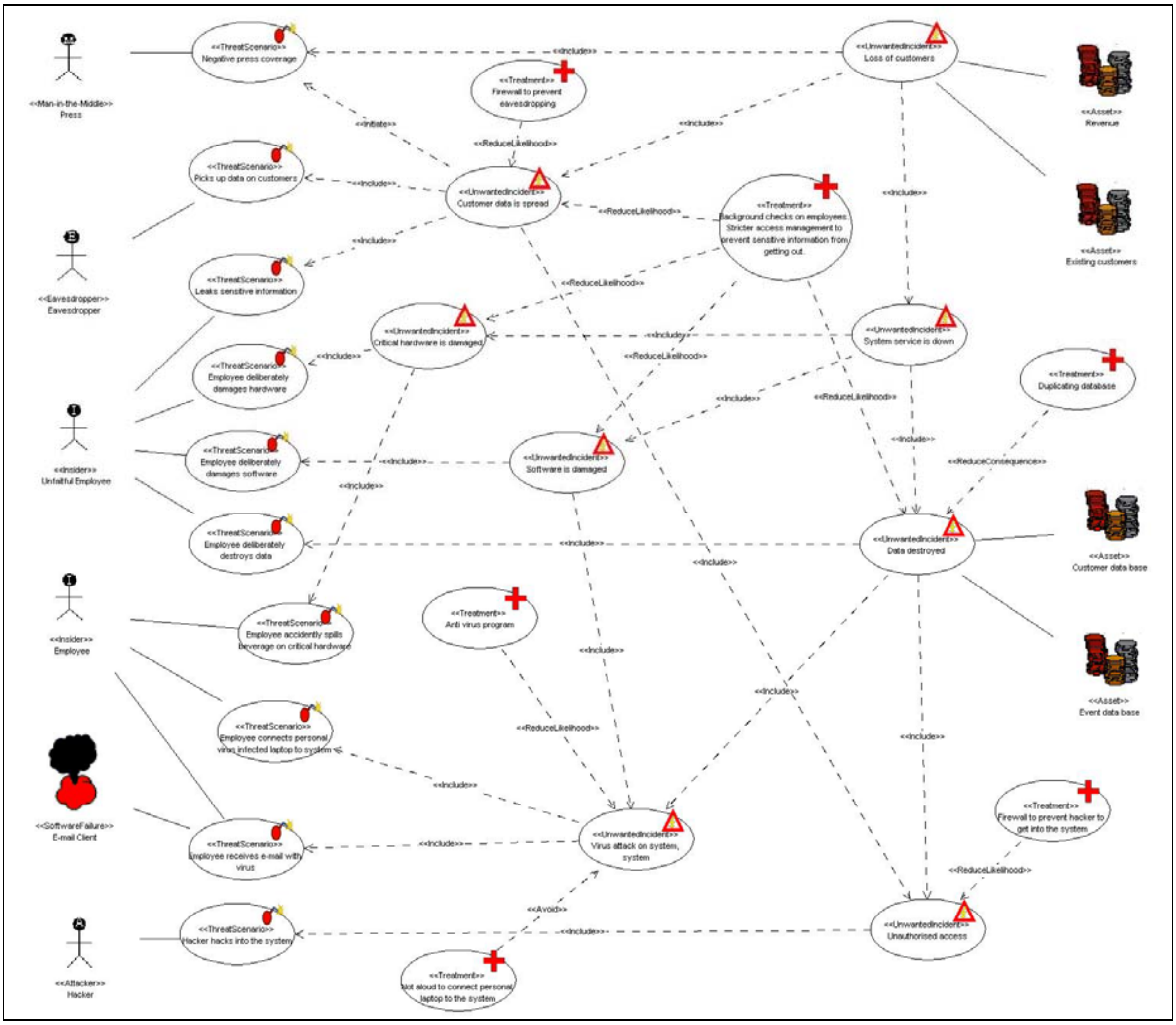
<<Man-in-the-Middle>> Press
<<ThreatScenario>> Negative press coverage
<<Include>>
<<UnwantedIncident>> Loss of customers
<<Asset>> Revenue
<<Treatment>> Firewall to prevent eavesdropping
<<Initiate>>
<<ReduceLikelihood>>
<<Include>>
<<ThreatScenario>> Picks up data on customers
<<Include>>
<<UnwantedIncident>> Customer data is spread
<<ReduceLikelihood>>
<<Treatment>> Background checks on employees. Stricter access management to prevent sensitive information from getting out.
<<Include>>
<<Asset>> Existing customers
<<Eavesdropper>> Eavesdropper
<<Include>>
<<ThreatScenario>> Leaks sensitive information
<<ReduceLikelihood>>
<<UnwantedIncident>> Critical hardware is damaged
<<Include>>
<<UnwantedIncident>> System service is down
<<Include>>
<<ReduceLikelihood>>
<<Treatment>> Duplicating database
<<ThreatScenario>> Employee deliberately damages hardware
<<Include>>
<<ReduceLikelihood>>
<<Include>>
<<Insider>> Unfaithful Employee
<<ThreatScenario>> Employee deliberately damages software
<<Include>>
<<UnwantedIncident>> Software is damaged
<<Include>>
<<ReduceConsequence>>
<<Include>>
<<ThreatScenario>> Employee deliberately destroys data
<<Include>>
<<UnwantedIncident>> Data destroyed
<<Asset>> Customer data base
<<Include>>
<<Insider>> Employee
<<ThreatScenario>> Employee accidently spills beverage on critical hardware
<<Treatment>> Anti virus program
<<Include>>
<<Include>>
<<Asset>> Event data base
<<ThreatScenario>> Employee connects personal virus infected laptop to system
<<ReduceLikelihood>>
<<Include>>
<<SoftwareFailure>> E-mail Client
<<Include>>
<<ThreatScenario>> Employee receives e-mail with virus
<<Include>>
<<UnwantedIncident>> Virus attack on system, system
<<Treatment>> Firewall to prevent hacker to get into the system
<<ReduceLikelihood>>
<<Avoid>>
<<ThreatScenario>> Hacker hacks into the system
<<Include>>
<<UnwantedIncident>> Unauthorised access
<<Attacker>> Hacker
<<Treatment>> Not aloud to connect personal laptop to the system

Figure 2: Treatments