

NET CENTRIC THREAT DETECTION SYSTEM (NTDS)

DNSSC 6254: Risk Management – Fall 2018

Presented By: Harold Hackstall and William Jenkins
Professor Forman

George Washington University School of Business

Contents

1. INTRODUCTION	2
2. Project Structure	3
2.1 Identifying Risk Events	3
2.2 Identifying Risk Objectives	3
2.3 Identifying Sources	4
2.4 Participants and Roles	5
3. Source Mapping	7
3.1 Likelihood of Events	7
3.2 Consequences Grid	7
4. Risk Measurements and Judgements	8
5. Project Synthesis	11
5.1 Synthesis Likelihood of Events	11
5.2 Synthesis Impact of Events	12
6. Risk Review	13
6.1 Overall Risk Without Controls	13
6.2 Risk Maps Without Controls	16
6.3 Identifying and Selecting Controls	17
6.4 Overall Risk with Controls	18
7. Recommendations and Conclusion	25
References	26

1. INTRODUCTION

TotalSource Solutions Inc. (TSSI) is a Virginia Corporation focused on Public Safety Security Systems Solutions through innovative technology integrations, engineered processes, artificial intelligence (AI), and robotic implementations. We are currently developing a concept product design that we hope will revolutionize their markets.

Due to the recent mass shootings (i.e. school, clubs, malls, airports etc.) the **Net Centric Threat Detection System (NTDS)** is being developed to provide a **three-zone** approach to stand-off threat surveillance, detection, and mitigation or containment.

The system will be used in a Public Safety context with applications in a broad array of venues (i.e. airports, schools, federal buildings, hospitals etc.) and most notably for gun free zone enforcement. Capabilities will include detecting a range of threats such as concealed weapons, explosives, and dangerous chemicals and toxins. Additionally, it provides a tool used in preventing exposure to undue dangers for first responders and law enforcement.

- **Zone 3 (Z-3)** – Outer boundary and provides top-level screening and identification prior to the inner zones; identifies large and overt threats; determines and detects restricted area breaches (perimeter and access roadways etc.); identifies developing threat scenarios. Integrates with and augments existing infrastructure and implements aerial drone capability.
- **Zone 2 (Z-2)** – An inner boundary which serves as a gateway (approach) corridor. Focus is detection and containment of both concealed/unconcealed threats (e.g. rifles, assault weapons, knives/machetes, handguns, explosives, flammables, and chemicals). Implements the Robotic “Bear Hugg” Sentries.
- **Zone 1 (Z-1)** - The innermost zone, serves as an entry boundary into the sterile (protected) environment. It provides for the finest level of inspection and detects potential weapons at the finest level of detail. Implements Mantrap Vestibule Inspection Que (MIQ) detection & containment.

2. Project Structure

2.1 Identifying Risk Events

Using Expert Choice Riskion software to structure our risk model, we identified (13) risk events with the potential to cause loss to the implementation of the Net-Centric Threat Detection System (NTDS). A risk event is a risk likely to happen that could result in a loss. Figure 1 shows a list of the identified risk events.

Unique ID		Events
[06]	i	Laws/regulations being violated
[15]	i	Politicians questions the need of the system.
[02]	i	The system being compromised
[05]	i	Loss of power during operations
[04]	i	Public not understanding the system
[07]	i	System has poor threat detection
[12]	i	System database cant integrate with other databases
[01]	i	System footprint cant be modified
[08]	i	The public viewing the system as harmful
[09]	i	The system being complicated to operate
[10]	i	Vendor files bankruptcy
[11]	i	Vendor threat library not updated with current/emerging threats
[14]	i	Public viewing system as invading privacy

Figure 1 Risk Events

2.2 Identifying Risk Objectives

The team next identified (4) objectives and (7) subobjectives that could be impacted by risk events. These objectives were hierarchal order. Figure 2 displays the identified objectives and sub-objectives.

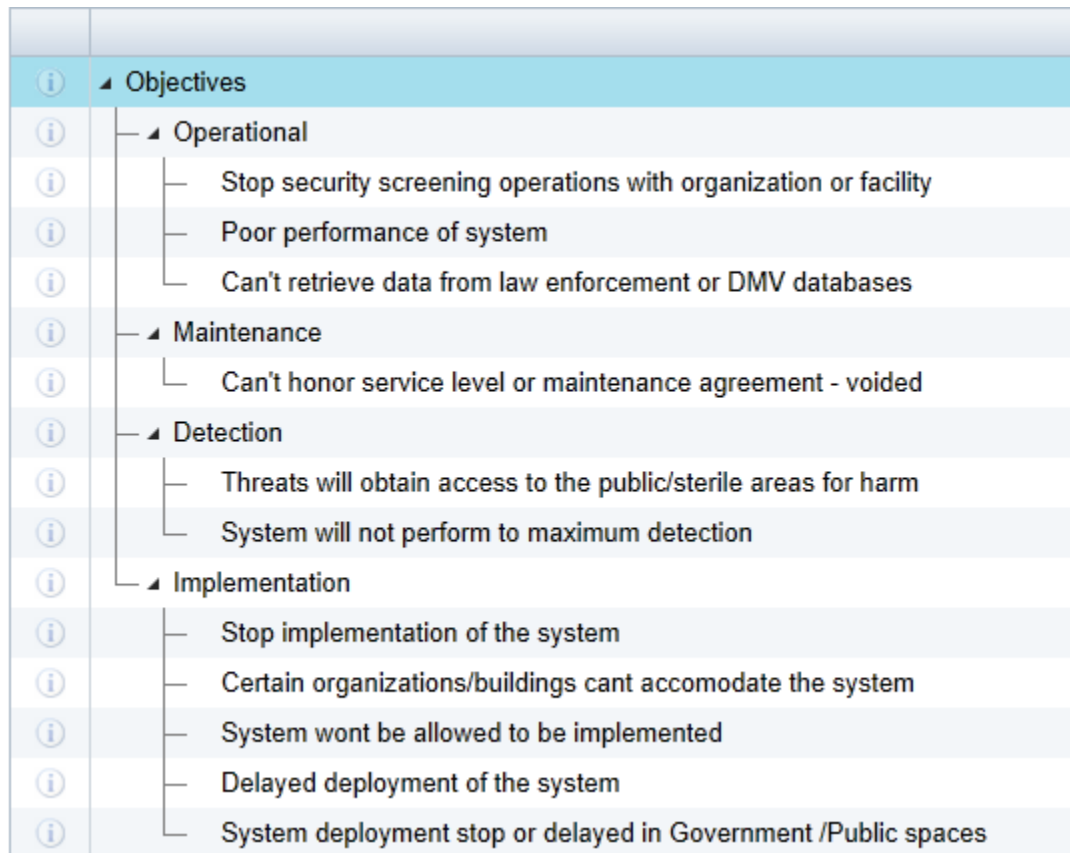


Figure 2 Hierarchy of Objectives

2.3 Identifying Sources

The team identified (18) sources that could impact a risk event. The team placed the sources into hierarchal order by: Laws/regulations, Operational, Training/Visual Aids, Weather /Temperature, System Specification/designs, Financial. Figure 3 shows the risk sources in hierarchal order.


























	▲ Sources
	— ▲ Laws/regulations
	— Not understanding all laws/regulations
	— Laws /regulations doesn't allow the particular technology of system
	— New laws established after system implementation
	— ▲ Operational
	— System threat library not updated with latest/emerging threats
	— Overheating of sytem processors
	— System cant process new/emerging threats
	— Federal, international, state, and local databases not integrated. Systems not compatible.
	— ▲ Training/Visual Aids
	— Insufficient system literature/brochures
	— Lack of personnel training
	— Lack of system labeling/markig
	— Media misrepresentation of system
	— Constituents voice concerns over tax dollars/safety/privacy
	— ▲ Weather /Temperature
	— Extreme cold temperature affects system detection performace (i.e -30 F)
	— Extreme heat temperature affects system detection performance(i.e 130 degrees Fahrenheit)
	— ▲ System specifications/designs
	— Designed with one specification /footprint
	— System detection zones designed to be concurrent
	— ▲ Financial
	— Vendor recieved insufficient system orders
	— Lost market share to competing vendor

Figure 3 Hierarchy of Sources

2.4 Participants and Roles

There are several individuals who are critical to the success of the NTDS. These individuals were crucial to identifying and evaluating risks. The evaluating of the risks was assigned based on the risk source and the individual's position and level of involvement with the project. The participants are identified in Figure 4. A sample of participant roles for sources and events are displayed in Figure 5 and Figure 6, respectively.

<input type="checkbox"/>	Email Address	Participant Name	Permission
<input type="checkbox"/>	wljenkins85@gwu.edu	BJ Jenkins	Project Manager
<input type="checkbox"/>	cap1@gmail.com	Chief Operating Officer /Steven Rogers	Evaluator
<input type="checkbox"/>	stark1@yahoo.com	Chief Risk Officer /John Stark	Evaluator
<input type="checkbox"/>	hackstall4@gwu.edu	Harold Hackstall	Project Manager
<input type="checkbox"/>	nstavrakakis@gwu.edu	Nicholas Stavrakakis	Project Manager
<input type="checkbox"/>	forman@gwu.edu	Professor Forman	Project Manager
<input type="checkbox"/>	falcon88@gmail.com	Risk Analyst / Samuel Wilson	Evaluator
<input type="checkbox"/>	bucky85@yahoo.com	Risk Manager /James Barnes	Evaluator

Figure 4 List of Participants

Participants

Groups

Participant Name

☐ BJ Jenkins
☐ Chief Operating Officer /Steven Rogers
☐ Chief Risk Officer /John Stark
☐ Harold Hackstall
☐ Nicholas Stavrakakis
☐ Professor Forman
☐ Risk Analyst / Samuel Wilson
☒ Risk Manager /James Barnes
☐ Tamara Brevton

Sources

Laws/regulations

☐ Not understanding all laws/regulations
☐ Laws /regulations doesn't allow the particular technology of system
☐ New laws established after system implementation

Operational

☐ System threat library not updated with latest/emerging threats
☐ Overheating of system processors
☐ System cant process new/emerging threats
☐ Federal, international, state, and local databases not integrated. Systems not compatible

Training/Visual Aids

☐ Insufficient system literature/brochures
☐ Lack of personnel training
☐ Lack of system labeling/markings
☐ Media misrepresentation of system
☐ Constituents voice concerns over tax dollars/safety/privacy

Weather /Temperature

☐ Extreme cold temperature affects system detection performance (i.e -30 F)
☐ Extreme heat temperature affects system detection performance (i.e 130 degrees Fahrenheit)

System specifications/designs

☐ Designed with one specification /footprint
☐ System detection zones designed to be concurrent

Financial

☐ Vendor received insufficient system orders
☐ Lost market share to competing vendor

Figure 5 Sample of Participant Roles for Sources

Participants

Groups

Participant Name

☐ BJ Jenkins
☐ Chief Operating Officer /Steven Rogers
☐ Chief Risk Officer /John Stark
☐ Harold Hackstall
☐ Nicholas Stavrakakis
☐ Professor Forman
☒ Risk Analyst / Samuel Wilson
☐ Risk Manager /James Barnes
☐ Tamara Brevton

Events

☒ Laws/regulations being violated
☒ Politicians questions the need of the
☒ The system being compromised
☐ Loss of power during operations
☐ Public not understanding the system
☐ System has poor threat detection
☒ System database cant integrate with
☒ System footprint cant be modified
☒ The public viewing the system as har
☐ The system being complicated to ope
☐ Vendor files bankruptcy
☒ Vendor threat library not updated with
☒ Public viewing system as invading pr

Sources

No specific Sources

Laws/regulations

☒ Not understanding
☒ Laws /regulation
☒ New laws establis

Operational

☐ System threat lib
☐ Overheating of sy
☐ System cant proc
☐ Federal, internat
☐ Insufficient syste

Training/Visual Aids

☐ Lack of persone
☐ Lack of system la
☐ Media misrepres
☐ Constituents voic
☐ Extreme cold tem
☐ Extreme heat tem

System specific

☐ Designed with on
☐ System detection
☐ Vendor received
☐ Lost market share

Figure 6 Sample of Participant Roles for Events

3. Source Mapping

3.1 Likelihood of Events

The vulnerability grid in Figure 7 shows the likelihood of events based on the sources. The purpose of the vulnerability grid is to map events to sources that may contribute to the events occurrence. There are some sources that may contribute to multiple events, such as, overheating of system processors contributing to loss of power during operation and system has poor threat detection. Similarly, most of the events have more than one source.

Events	Sources															
	Laws/regulations				Operational				Training/Visual Aids				Weather /Temperature		System specifications	
	<input type="checkbox"/> Not understood	<input type="checkbox"/> Law /regulations	<input type="checkbox"/> New law established	<input type="checkbox"/> System threat lib	<input type="checkbox"/> Overheating of sys	<input type="checkbox"/> System cant proc	<input type="checkbox"/> Federal, internal	<input type="checkbox"/> Insufficient system	<input type="checkbox"/> Lack of personnel	<input type="checkbox"/> Lack of system in	<input type="checkbox"/> Media misappreh	<input type="checkbox"/> Continuous voice	<input type="checkbox"/> Extreme cold temp	<input type="checkbox"/> Extreme hot temp	<input type="checkbox"/> Designed with on	<input type="checkbox"/> System detection
<input type="checkbox"/> Laws/regulations being violated	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Politicians questions the need of the system.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The system being compromised	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Loss of power during operations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Public not understanding the system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> System has poor threat detection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> System database cant integrate with other databases	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> System footprint cant be modified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> The public viewing the system as harmful	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> The system being complicated to operate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Vendor files bankruptcy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Vendor threat library not updated with current/emerging threats	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Public viewing system as invading privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 7 Vulnerability Grid

3.2 Consequences Grid

After identifying the sources, risk events, and objectives, the team utilized the consequences grid to map the consequences of events to objectives, shown in Figure 8. This step allows us to see which events have a direct impact on which objective. If an event happens, such as the vendor filing bankruptcy, then one or more objectives cannot be met. In this instance, the vendor filing bankruptcy would cause the service agreements to not be honored.

Events	Objectives/Consequences											
	Operational			Maintenance	Detection		Implementation					
	Stop security score	Poor performance	Can't retrieve data	Can't honor service	Threats will obtain	System will not perform	Stop implementation	Certain organization	System won't be as	Delayed deployment	System deployment	
<input type="checkbox"/> Laws/regulations being violated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> Politicians questions the need of the system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> The system being compromised	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Loss of power during operations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Public not understanding the system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> System has poor threat detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> System database cant integrate with other databases	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> System footprint cant be modified	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> The public viewing the system as harmful	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> The system being complicated to operate	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Vendor files bankruptcy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Vendor threat library not updated with current/emerging threats	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> Public viewing system as invading privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Figure 8 Consequences Grid

4. Risk Measurements and Judgements

Once source, event, and objectives were identified and mapped, the team used the Expert Choice Riskion software to determine the appropriate measurements to utilize for the project's objectives. Riskion uses the analytical hierarchy process (AHP) integrated model and provides relative and absolute measurements. AHP uses a ratio scale method to weigh all possibilities of events and objectives. The measurement types we used were rating scale and pairwise. Ratings scale provided the absolute measurement and pairwise provided the relative measurements. Figure 9 shows an example of the questions asked to participants to get the ratings scale measurement. Figure 10 shows an example of a pairwise comparison measurement. Figure 11 and Figure 12 show the measurement methods for likelihood of events for sources and likelihood of events for events. Figure 13 and Figure 14 depict measurement methods for impact events for objectives and events.

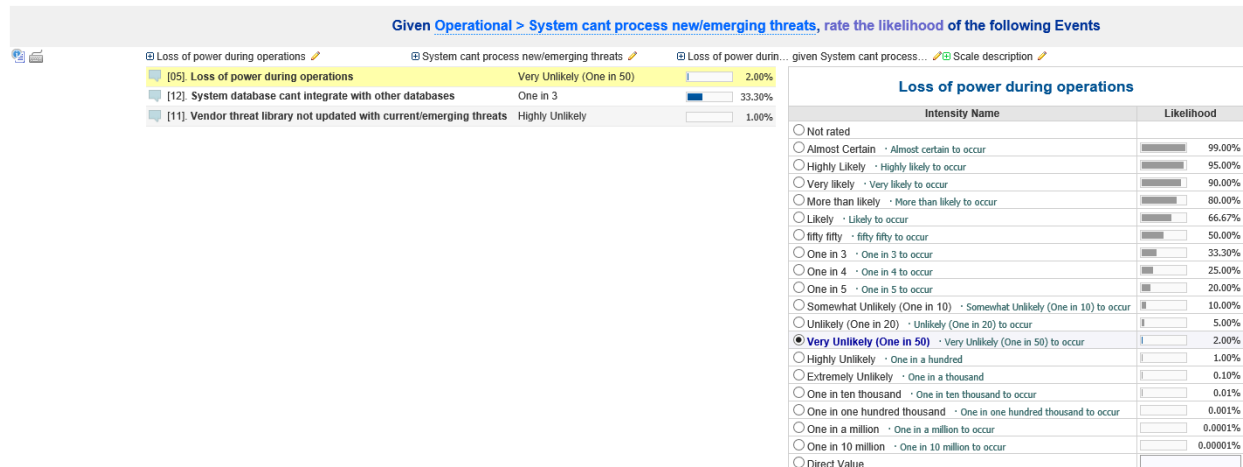


Figure 9 Ratings Scale Measurement

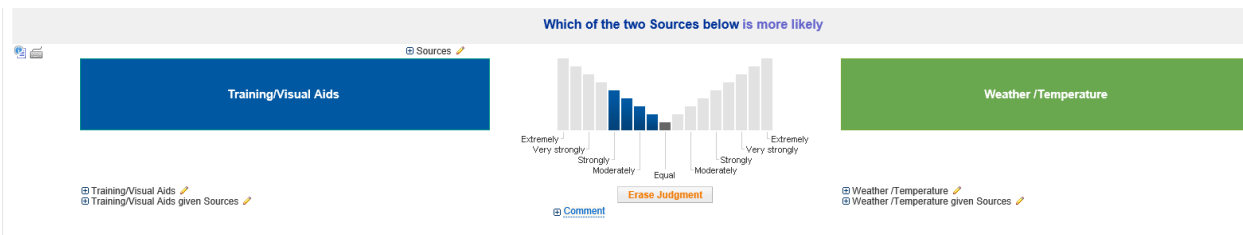


Figure 10 Pairwise Comparison Measurement

Measure Likelihood	Measurement Type	Measurement Scale or Given Likelihood	Action	# of Elements, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: One pair	Pairwise Type Default: Verbal
▲ Sources	Pairwise with Give	Laws/regulations: 0.55	Copy	6	6*(6-1)/2 = 15	All pairs (maximum accuracy)	One pair	Verbal
└ Laws/regulations	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	3	3			
└ Not understanding all laws/regulations								
└ Laws /regulations doesn't allow the partic								
└ New laws established after system imple								
▲ Operational	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	4	4			
└ System threat library not updated with lat								
└ Overheating of sytem processors								
└ System cant process new/emerging thre								
└ Federal, international, state, and local da								
▲ Training/Visual Aids	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	5	5			
└ Insufficient system literature/brochures								
└ Lack of personnel training								
└ Lack of system labeling/markings								
└ Media misrepresentation of system								
└ Constituents voice concerns over tax dol								
▲ Weather /Temperature	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	2	2			
└ Extreme cold temperature affects system								
└ Extreme heat temperature affects system								
▲ System specifications/designs	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	2	2			
└ Designed with one specification /footprin								
└ System detection zones designed to be c								
▲ Financial	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	2	2			
				Total 33				

Figure 11 Likelihoods of Events: Measurement Methods for Sources
(Pairwise with given Likelihood of events, Rating scale – wide likelihood rating scale)

Measure Event Likelihoods	Measurement Type Default: Rating Scale	Measurement Scale or Given Likelihood	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: All pairs	Pairwise Type Default: Verbal
▲ Sources								
▲ Laws/regulations								
Not understanding all laws/regulations	Rating Scale	Default Likelihood Scale	Copy Edit	1	1			
Laws /regulations doesn't allow the partic	Pairwise with	Laws/regulations being violate....: 0.5	Copy	1		All pairs (maximum a	All pairs	Verbal
New laws established after system imple	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	1	1			
▲ Operational								
System threat library not updated with la	Pairwise with	System has poor threat detecti....: 0.6	Copy	2	2*(2-1)/2 = 1	All pairs (maximum a	All pairs	Graphics
Overheating of sytem processors	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	2	2			
System cant process new/emerging thre	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	3	3			
Federal, international, state, and local da	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	0				
▲ Training/Visual Aids								
Insufficient system literature/brochures	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	4	4			
Lack of personnel training	Pairwise with	Public viewing system as invad....: 0.4	Copy	1		All pairs (maximum a	All pairs	Verbal
Lack of system labeling/markin	Rating Scale	Default Likelihood Scale	Copy Edit	0				
Media misrepresentation of system	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	1	1			
Constituents voice concerns over tax do	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	1	1			
▲ Weather /Temperature								
Extreme cold temperature affects system	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	2	2			
Extreme heat temperature affects system	Pairwise with	System has poor threat detecti....: 0.3	Copy	3	3*(3-1)/2 = 3	All pairs (maximum a	All pairs	Graphics
▲ System specifications/designs								
Designed with one specification /footprin	Pairwise with	System footprint cant be modif....: 0.3	Copy	1		All pairs (maximum a	All pairs	Verbal
System detection zones designed to be c	Rating Scale	WIDE LIKELIHOOD RATING SCALE	Copy Edit	1	1			
▲ Financial								
				Total 22				

Figure 12 Likelihood of Events: Measurement Methods for Events
(Rating scale, Pairwise with given likelihood)

Measure Importance With Respect To	Measurement Type	Measurement Scale	Action	# of Elements, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: One pair	Pairwise Type Default: Verbal
▲ Objectives	Pairwise Compari		Copy	4	4*(4-1)/2 = 6	All pairs (maximum a	One pair	Verbal
▲ Operational	Pairwise Compari		Copy	3	3*(3-1)/2 = 3	All pairs (maximum a	One pair	Graphics
Stop security screening operations with c								
Poor performance of system								
Can't retrieve data from law enforcement								
▲ Maintenance	Pairwise Compari		Copy	1		All pairs (maximum a	One pair	Verbal
Can't honor service level or maintenance								
▲ Detection	Pairwise Compari		Copy	2	2*(2-1)/2 = 1	All pairs (maximum a	One pair	Graphics
Threats will obtain access to the public/s								
System will not perform to maximum det								
▲ Implementation	Pairwise Compari		Copy	5	5*(5-1)/2 = 10	All pairs (maximum a	One pair	Verbal
Stop implementation of the system								
Certain organizations/buildings cant acc								
System wont be allowed to be implemen								
Delayed deployment of the system								
System deployment stop or delayed in G								

Figure 13 Impact of Events: Measurement Methods used for Objectives
(Pairwise Comparison)

Measure Events With Respect To	Measurement Type Default: Rating Scale	Measurement Scale	Action	# of Events, # of Probabilities	# of Judgments in Cluster	# of Comparisons Default: All pairs (maximum accuracy)	Display Default: All pairs	Pairwise Type Default: Verbal
Objectives								
Operational								
Stop security screening operations with	Rating Scale	Default Impact Scale	Copy Edit	4	4			
Poor performance of system	Rating Scale	Default Impact Scale	Copy Edit	5	5			
Can't retrieve data from law enforcement	Rating Scale	Default Impact Scale	Copy Edit	4	4			
Maintenance								
Can't honor service level or maintenance	Rating Scale	Default Impact Scale	Copy Edit	1	1			
Detection								
Threats will obtain access to the public's	Rating Scale	Default Impact Scale	Copy Edit	6	6			
System will not perform to maximum det	Rating Scale	Default Impact Scale	Copy Edit	6	6			
Implementation								
Stop implementation of the system	Rating Scale	Default Impact Scale	Copy Edit	3	3			
Certain organizations/buildings cant acc	Rating Scale	Default Impact Scale	Copy Edit	1	1			
System wont be allowed to be implemen	Rating Scale	Default Impact Scale	Copy Edit	5	5			
Delayed deployment of the system	Rating Scale	Default Impact Scale	Copy Edit	6	6			
System deployment stop or delayed in G	Rating Scale	Default Impact Scale	Copy Edit	5	5			

Figure 14 Impact of Events: Measurement method used for Events
(Rating Scale – default impact scale)

5. Project Synthesis

Project synthesis is the computation of the likelihood and impact of the events. We used the Riskion software to make the computations and make meaningful conclusions of the likelihood of the events on a percentage scale.

5.1 Synthesis Likelihood of Events

Figure 15 shows the likelihood of events for all sources. We see that the source, laws/regulations, has a 55% probability of occurrence. Figure 16 shows the dynamic sensitivity analysis as depicted in the Riskion software. The dynamic view allows the user to adjust the source likelihood probability to see what a higher or lower percentage would have on event likelihood.

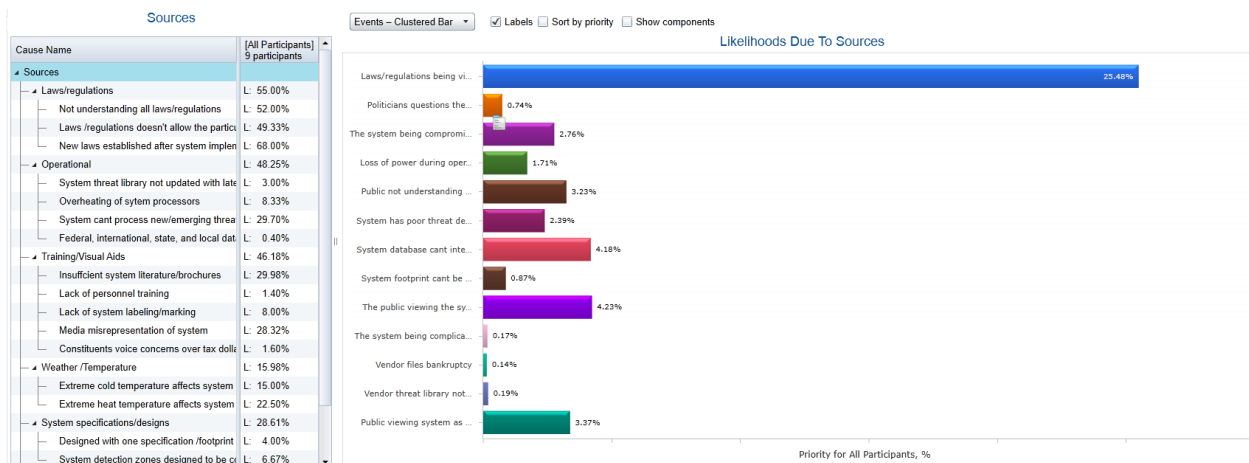


Figure 15 Sensitivity Analysis Likelihood of Events for Sources/Threats

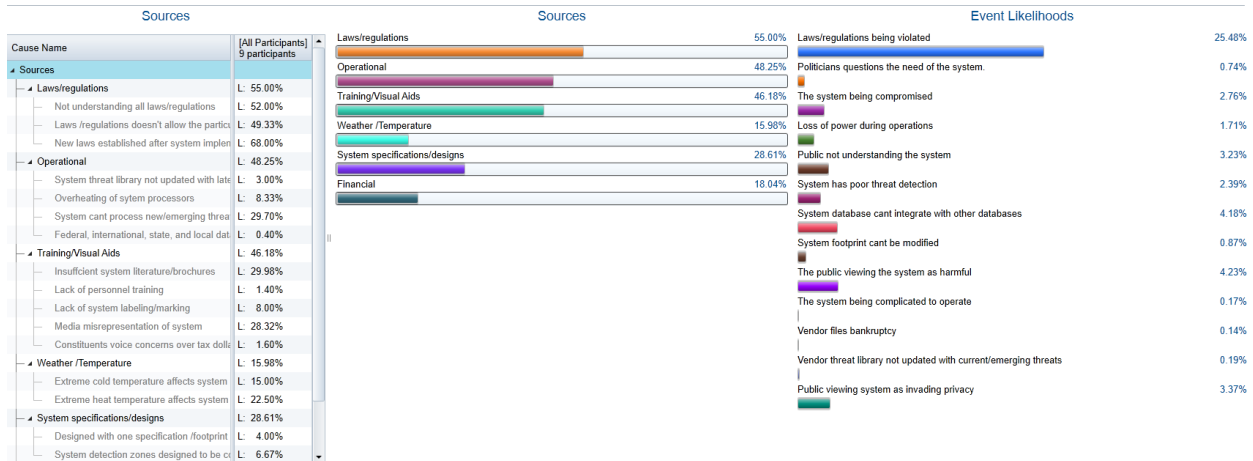


Figure 16 Sensitivity Analysis (Dynamic) Likelihood of Events for Sources/Threats

5.2 Synthesis Impact of Events

Figure 17 shows the computation of the impact of risk events for the objectives. For all objectives, we see that detection is the highest priority objectives at 51.53%. Figure 18 shows the dynamic view for impact of events.

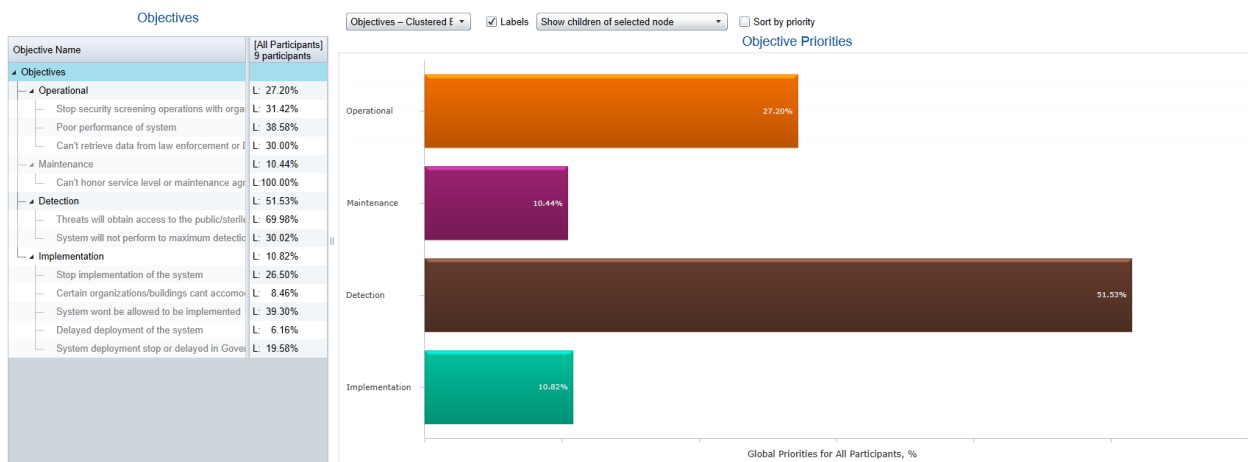


Figure 17 Sensitivity Analysis Impact of Events for Objectives

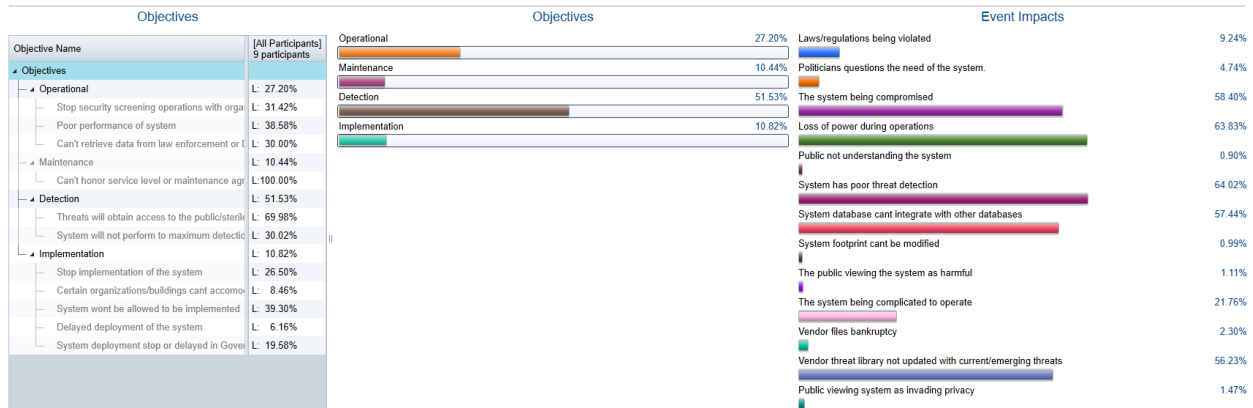


Figure 18 Sensitivity Analysis (Dynamic) Impact of Events for Objectives

6. Risk Review

6.1 Overall Risk Without Controls

Risk is the expected value of a loss. Assessing risk is partly subjective, however, it is possible to ascertain a financial value. Because we have identified and measured the likelihood of events and the impact of those events, we can determine what the greatest risk is to the NTDS. The NTDS has been valued at \$95,291,048. Based on this assessment the overall computed and simulated financial values of likelihood and impact, of events are shown Figure 19 and Figure 20. The computed value of all risks is \$8,863,415 and the simulated value of all risk is \$7,770,227. Computed results account for possible results applicable which makes the results exaggerated due to double counting, while simulated values are calculated using the Monte Carlo simulation method.

Overall Likelihoods, Impacts, and Risks for RM Project 2018:HH_BJ_Net Centric Threat Detection System

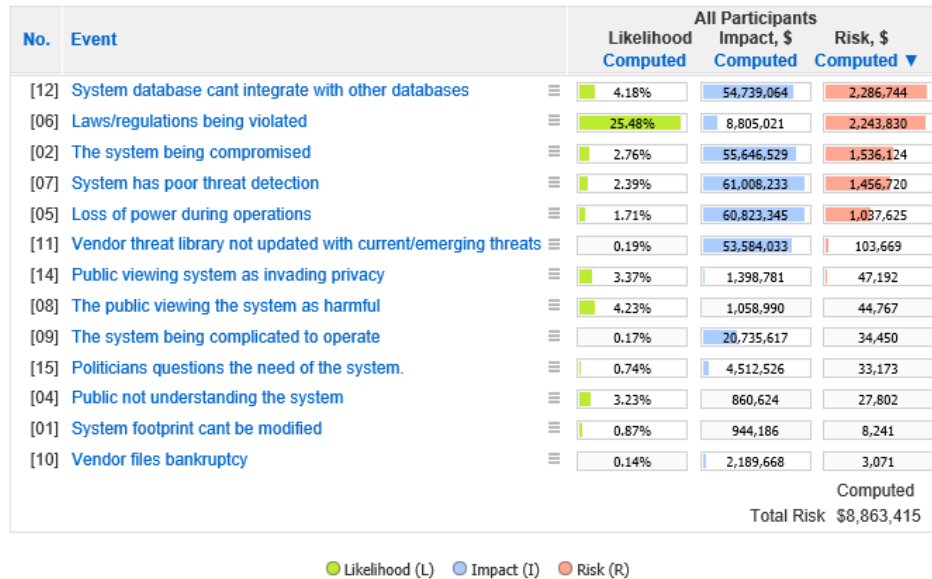


Figure 19 Overall Computed Likelihood, Impact, and Risk

Overall Likelihoods, Impacts, and Risks for RM Project 2018:HH_BJ_Net Centric Threat Detection System

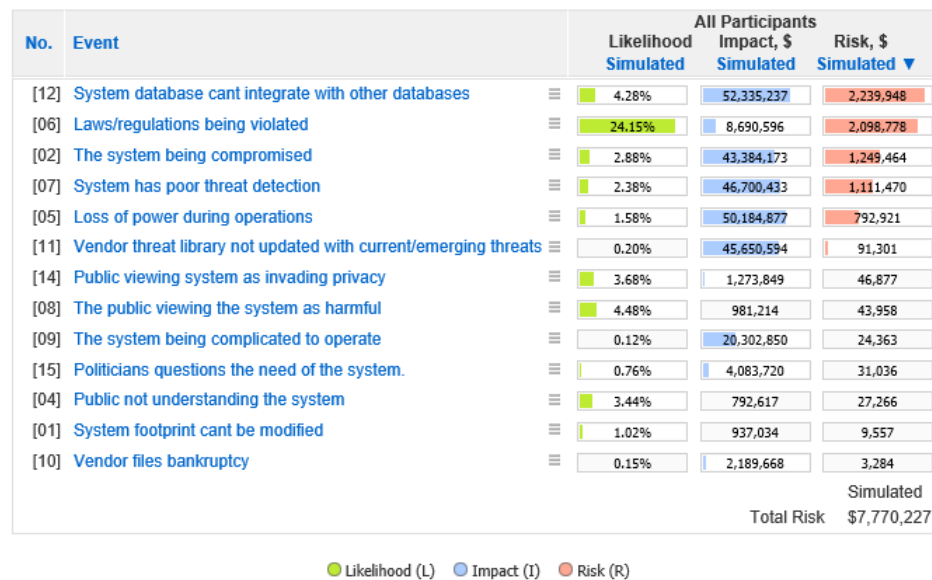


Figure 20 Overall Simulated Likelihood, Impact, and Risk

Figure 21 shows the loss exceedance curve, which represents the possibility that the loss will be greater than the total corresponding financial values. Using the Riskion software we ran 10,000 trials and concluded that the average risk is approximately \$7.77 million with approximately a 30% chance of exceeding the average risk. Additionally, there is a 5% probability that the risk

would exceed \$59.78 million and a 9% chance that the loss would exceed \$47.65 million, or half the enterprise value.

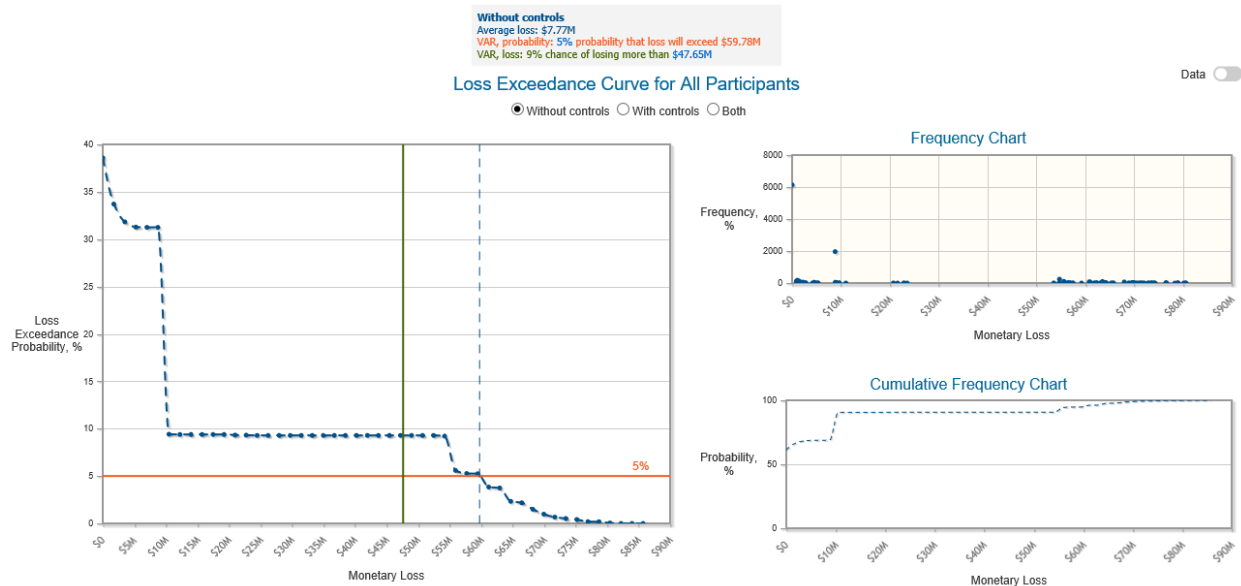


Figure 21 Loss Exceedance Curve

Figure 22 shows an example of a bow tie diagram. The bow tie diagram shows the causes (likelihood) of an event on the left and the objectives (impact) of the event on the right. In the center is the risk impact which is likelihood percentage multiplied by the impact value. The bow tie diagram shows the event laws/regulations being violated with a likelihood of 24.15% and an impact of \$8.69 million for a risk of \$2.10 million.

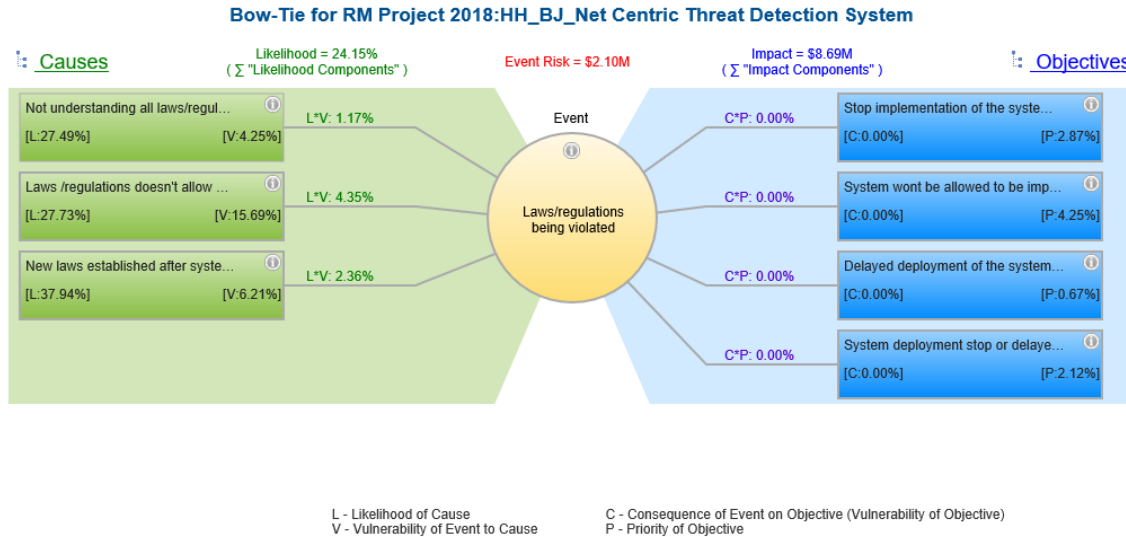


Figure 22 Bow-Tie Diagram

6.2 Risk Maps Without Controls

Figure 23 shows the likelihood and impact of risk events represented in a risk/heat map. The size of the bubble indicates the likelihood and impact on project. The larger the bubble, the greater the likelihood and impact to the project. The color regions represent iso curves and help show the relationship of the risks to the events. The color transitions are set to levels the decision makers find acceptable. It is shown that the event laws/regulations being violated has a likelihood of 24.15%, an impact of \$8.69 million, and a risk of \$2.10 million.

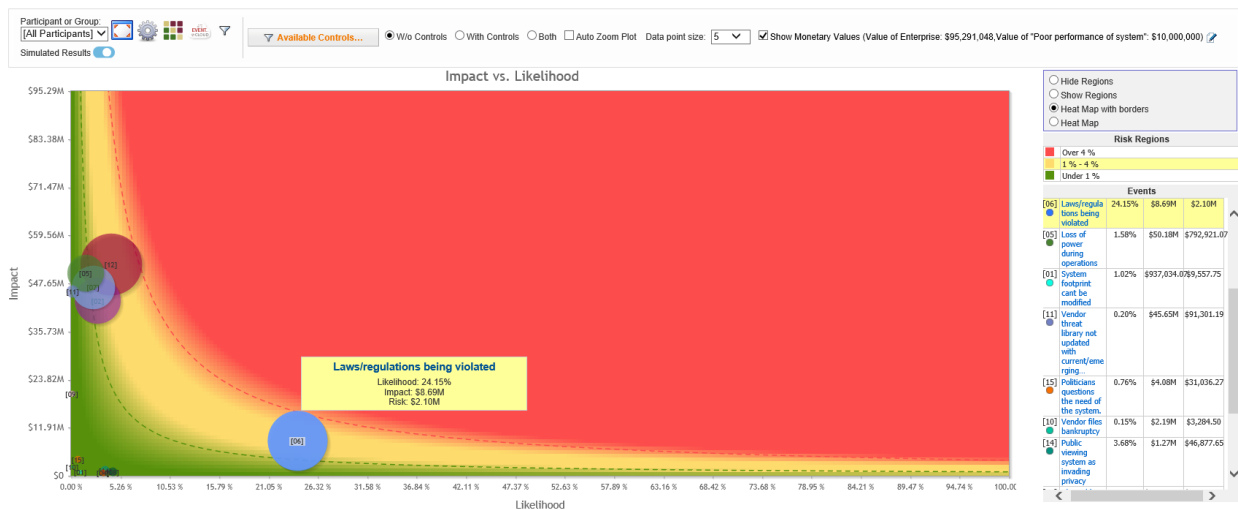


Figure 23 Risk Map and Risk Priority Matrix

6.3 Identifying and Selecting Controls

Before deciding to proceed or stop the project, controls need to be identified to help mitigate risk events and the likelihood of importance. Controls can be applied to sources, events, and/or objectives. For this project we identified 20 controls which would cost approximately \$6.3 million. Figure 24 contains a table detailing the controls for the project.

Select Controls									
Total Risk*: \$7,726,682 Risk With Selected Controls*: \$8,054,800 (Δ: \$-309,337) Risk With All Controls: \$5,332,440 (Δ: \$4,385,122)					Simulations Settings Number of trials: 10000 Seed: 900 <input type="checkbox"/> Keep Seed				
Selected controls: 0 Cost Of Selected Controls: \$0 (unfunded: \$8,308,800) Total Cost Of All Controls: \$8,308,800 <input checked="" type="checkbox"/> Show Monetary Values (Value of Enterprise: \$95,291,048, Value of "Poor performance of system": \$10,000,000)									
Index	Selected	Control Name	Control for	Selected	Cost	Applications	Categories	Must	Must Not
01	<input type="checkbox"/>	International laws/regulations translation guide	Cause		120000	8		<input type="checkbox"/>	<input type="checkbox"/>
02	<input type="checkbox"/>	Universal software hub system	Cause		1500000	4		<input type="checkbox"/>	<input type="checkbox"/>
03	<input type="checkbox"/>	Remote detection processor controllers	Cause		2000000	4		<input type="checkbox"/>	<input type="checkbox"/>
04	<input type="checkbox"/>	NTDS adapter kit	Cause		400000	7		<input type="checkbox"/>	<input type="checkbox"/>
05	<input type="checkbox"/>	Internal System Cooling system	Cause		2000	3		<input type="checkbox"/>	<input type="checkbox"/>
06	<input type="checkbox"/>	System Signage - all areas of facility/organization	Cause		1000	4		<input type="checkbox"/>	<input type="checkbox"/>
07	<input type="checkbox"/>	Post Implementation Law Clause	Cause		10000	8		<input type="checkbox"/>	<input type="checkbox"/>
08	<input type="checkbox"/>	Internal system heater	Cause		5000	4		<input type="checkbox"/>	<input type="checkbox"/>
09	<input type="checkbox"/>	Monthly training program	Cause		1500	4		<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	Anti Hacking system software	Vulnerability		2000000	7		<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	Random Threat generator	Vulnerability		30000	12		<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	Backup Power Generator	Vulnerability		10000	8		<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	Backup System Batteries	Vulnerability		500	8		<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	Custom System Build	Vulnerability		50000	14		<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	System training simulator	Vulnerability		2000	1		<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	System Info Commercialis	Consequence		40000	44		<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	On line/Net Training Modules	Consequence		130000	26		<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	Pre Deployment checklist	Consequence		300	25		<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	Vendor refunds for service agreements	Consequence		2500	17		<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	BI Annual Congressional hearings	Consequence		2000	3		<input type="checkbox"/>	<input type="checkbox"/>

Figure 24 Identified Controls

Once the controls were identified, they were mapped to their sources, events, and objectives. This was done by selecting a control for a source, event, or an objective if it had a positive effect on the risk event. The figures below show a table depicting the controls for cause likelihoods.

Controls for Cause Likelihoods												
Control Name	Sources											
	Laws/regulations			Operational				Training/Visual Aids				
	<input type="checkbox"/> Not understanding all laws/regulations	<input type="checkbox"/> Laws regulations doesn't allow the particular technology of system	<input type="checkbox"/> New laws established after system implementation	<input type="checkbox"/> System threat library not updated with latest/emerging threats	<input type="checkbox"/> Overheating of system processors	<input type="checkbox"/> System cant process new/emerging threats	<input type="checkbox"/> Federal, international, state, and local databases not integrated. Systems not compatible.	<input type="checkbox"/> Insufficient system literature/brochures	<input type="checkbox"/> Lack of personnel training	<input type="checkbox"/> Lack of system labeling/markings	<input type="checkbox"/> Media misrepresentation of system	<input type="checkbox"/> Constituents v concerns over dollars/safety/type
<input type="checkbox"/> 1. International laws/regulations translation guide	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> 2. Universal software hub system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 3. Remote detection processor controllers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 4. NTDS adapter kit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 5. Internal System Cooling system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 6. System Signage - all areas of facility/organization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> 7. Post Implementation Law Clause	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 8. Internal system heater	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 9. Monthly training program	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 25 Control for Likelihoods

Next the participants were asked to measure the effectiveness of controls. For each control the participants were ask to rate its effectiveness on a scale between 0 and 1. Below is an example of the control effectiveness measure.

Percent Effectiveness of Control 19. Vendor refunds for service agreements to reduce the Impact of Event Public viewing system as invading privacy on Objective System deployment stop or delayed in Government /Public spaces

19. Vendor refunds for service agreements

Please enter a value between 0 and 1:

0.28

Comment

19. Vendor refunds for service agreements
 System deployment stop or delayed in Governm...
 Public viewing system as invading privacy

Figure 26 Control Effectiveness

6.4 Overall Risk with Controls

Once the participants selected their judgements, we analyzed the results of the impact of the controls. In the first chart we have manually selected all controls, which has a cost of \$6,306,800, but it only results in a risk reduction of little more than \$7 million.

Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018:HH_BJ_Net Centric Threat Detection System
(Controls are optimized based on simulated input and output)

No.	Event		All Participants Likelihood Simulated	Impact, \$ Simulated	Risk, \$ Simulated
[12]	System database cant integrate with other databases	≡	2.53%	23,642,959	598,166
[07]	System has poor threat detection	≡	0.11%	27,648,300	30,413
[02]	The system being compromised	≡	0.39%	7,525,565	29,349
[06]	Laws/regulations being violated	≡	0.89%	2,391,098	21,280
[05]	Loss of power during operations	≡	0.23%	5,106,383	11,744
[11]	Vendor threat library not updated with current/emerging threats	≡	0.02%	25,905,115	5,181
[01]	System footprint cant be modified	≡	0.92%	466,487	4,291
[10]	Vendor files bankruptcy	≡	0.14%	91,115	127
[15]	Politicians questions the need of the system.	≡	0.10%	32,868	32
[14]	Public viewing system as invading privacy	≡	0.04%	27,338	10
[08]	The public viewing the system as harmful	≡	0.00%	0	0
[09]	The system being complicated to operate	≡	0.00%	0	0
[04]	Public not understanding the system	≡	0.00%	0	0
# Controls			Total Risk		
Cost of Controls			Risk Reduction		
How Selected			Residual Risk		
15			Simulated		
\$404,800			\$7,770,227		
Optimized based on simulated input and output with budget of \$500,000			\$7,069,628		
			\$700,599		

● Likelihood (L) ● Impact (I) ● Risk (R)

Figure 27 Overall Likelihoods, Impacts, and Risks with Controls

Looking at the Risk Map, with all controls selected, we see that there is a big shift in the bubbles. Figure 28 shows the new heat map without controls and Figure 29 shows the heat map with the controls selected. We noticed that the majority of the bubbles were in the green with a less than 1% likelihood when controls are implemented.

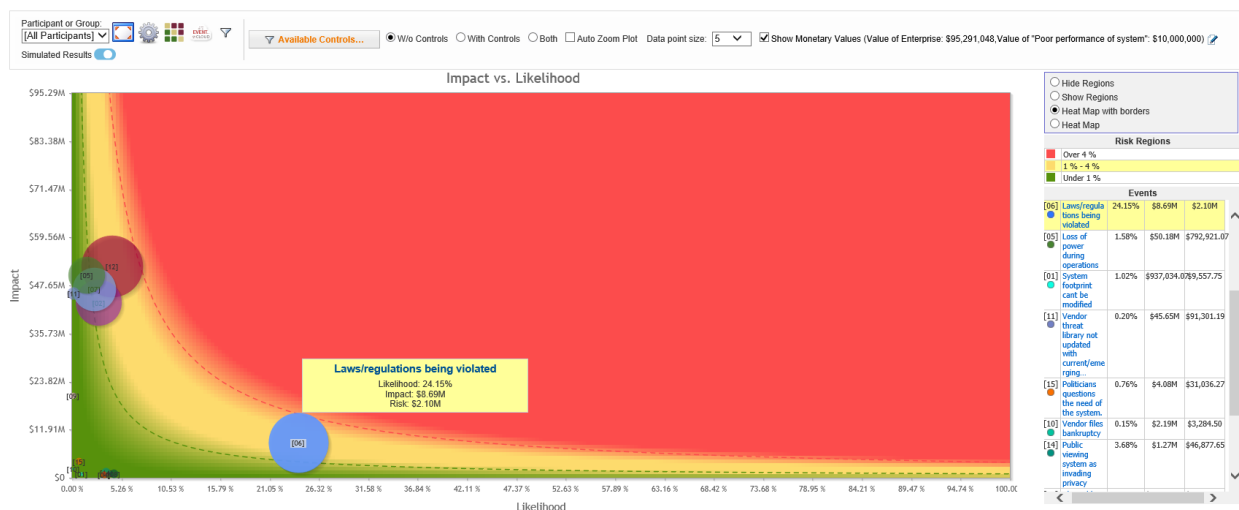


Figure 28 Risk Map without Controls

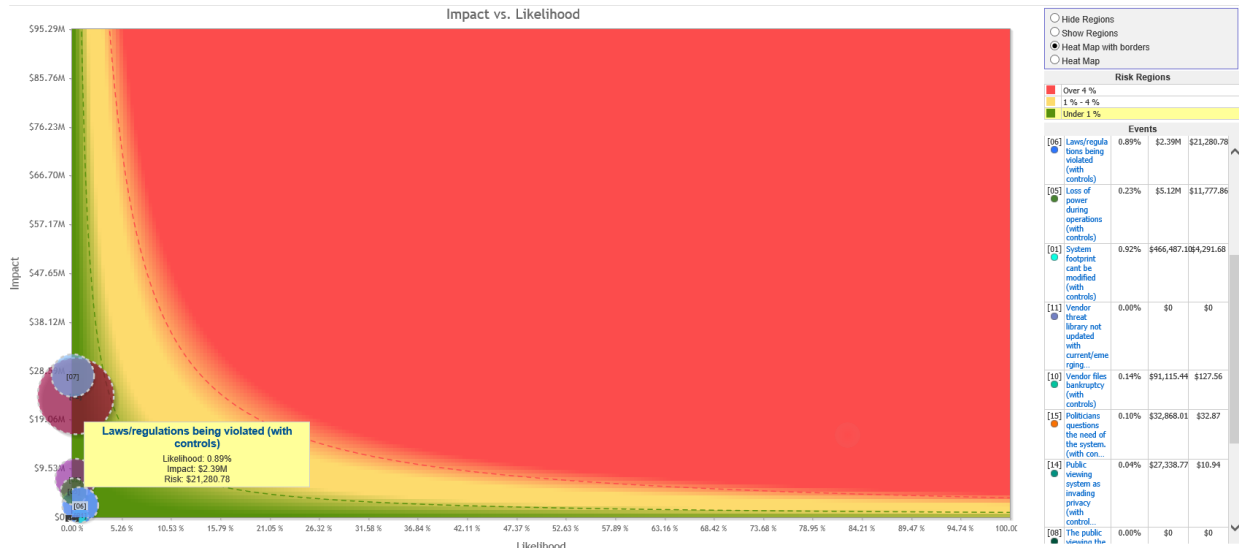


Figure 29 Risk Map with Controls

Looking at the loss exceedance curve without controls, we saw an average loss of \$7.77 million with a 5% probability of losing more than \$59.78 million. When controls are applied, the average loss drops to \$700,599, with a 5% probability of exceeding \$306,206. Additionally, we see that once the controls are implemented, the probability to exceed \$47.65 million drops to approximately 0%. Figure 29 depicts the loss exceedance curve of both with and without controls. The blue line represents without controls and the green line represents with controls.

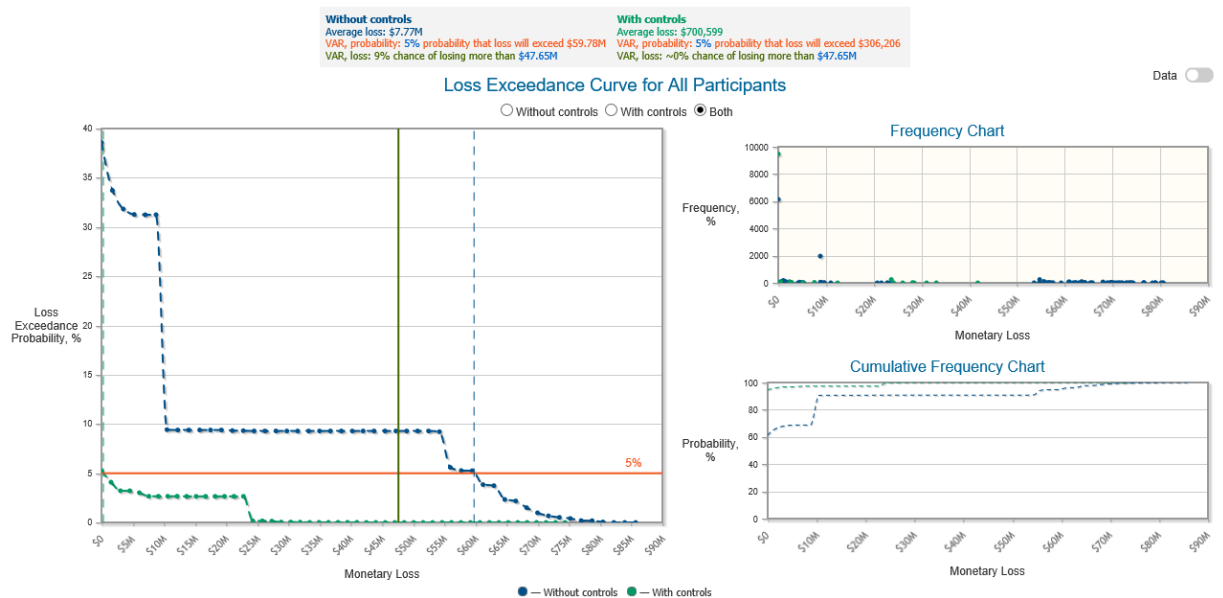


Figure 29 Loss Exceedance Curve without and with Controls

Because trying to implement all controls would be less advantageous and not cost effective, we decided on a control budget of \$500,000. After establishing a budget for controls, we entered that amount into the Riskion software and allowed the software to select the controls by clicking the optimize button. This provided us with the controls that would have the most positive impact on the project. Figure 30 shows the controls that were selected through optimization, and Figure 31 shows the impact those controls have on the project. Note, that there were 15 controls selected and the cost is \$404,800 to implement and has a risk reduction of just over \$7 million. The team tested several different control budgets and optimized for different control scenarios. When we input a control budget of \$1,000,000 and optimized, 17 controls were selected, with a cost of \$806,800 and the risk reduction was just over \$7.1 million. If the budget was reduced to \$250,000 13 controls were selected at a cost of \$244,800 with a risk reduction of just over \$6.8 million. Figure 32 and Figure 33 depict the maximum and minimum budgets alternative budgets the team looked at.

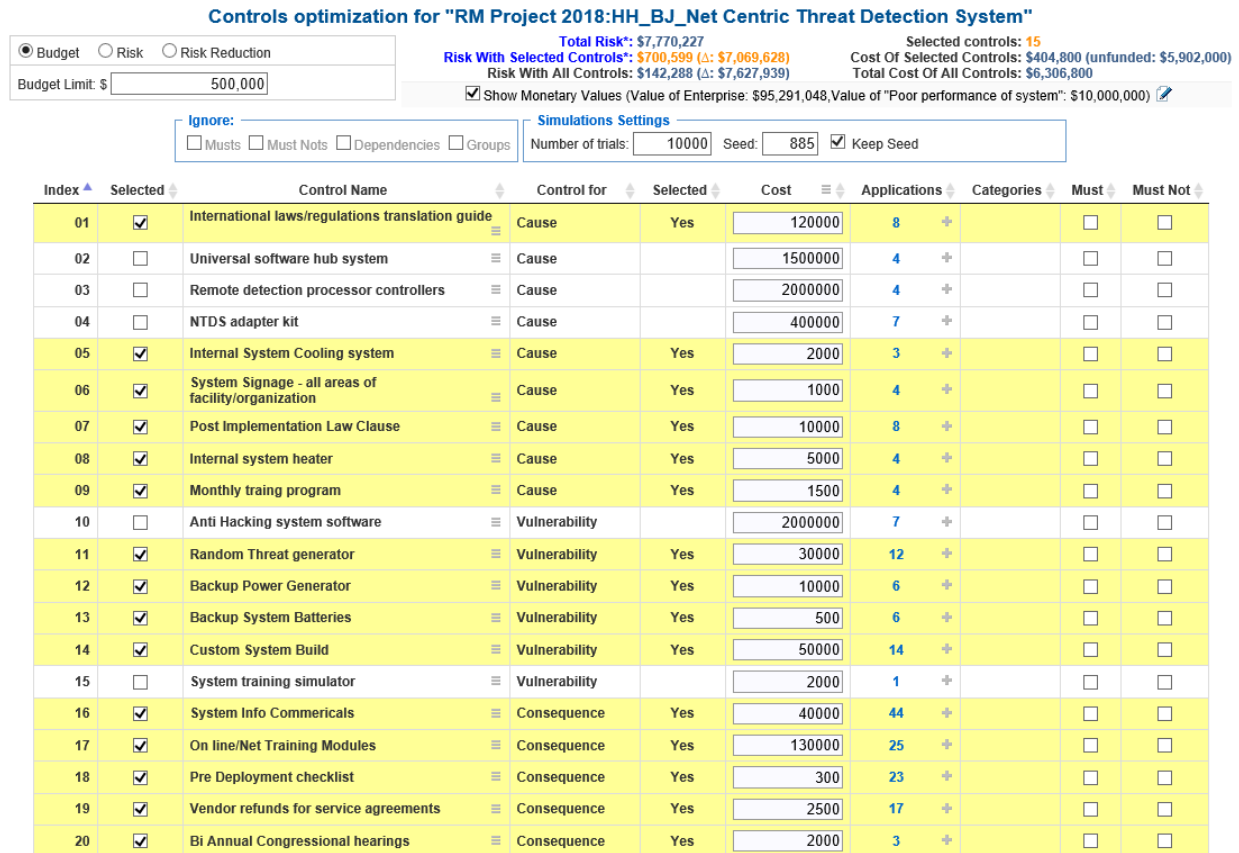


Figure 30 Selected Controls (Optimized)

Overall Likelihoods, Impacts, and Risks (With Controls) for RM Project 2018:HH_BJ_Net Centric Threat Detection System
(Controls are optimized based on simulated input and output)

No.	Event		All Participants		
			Likelihood Simulated	Impact, \$ Simulated	Risk, \$ Simulated
[12]	System database cant integrate with other databases		2.53%	23,642,959	598,166
[07]	System has poor threat detection		0.11%	27,648,300	30,413
[02]	The system being compromised		0.39%	7,525,565	29,349
[06]	Laws/regulations being violated		0.89%	2,391,098	21,280
[05]	Loss of power during operations		0.23%	5,106,383	11,744
[11]	Vendor threat library not updated with current/emerging threats		0.02%	25,905,115	5,181
[01]	System footprint cant be modified		0.92%	466,487	4,291
[10]	Vendor files bankruptcy		0.14%	91,115	127
[15]	Politicians questions the need of the system.		0.10%	32,868	32
[14]	Public viewing system as invading privacy		0.04%	27,338	10
[08]	The public viewing the system as harmful		0.00%	0	0
[09]	The system being complicated to operate		0.00%	0	0
[04]	Public not understanding the system		0.00%	0	0
# Controls Cost of Controls How Selected			Total Risk \$7,770,227		
15 \$404,800 Optimized based on simulated input and output with budget of \$500,000			Risk Reduction \$7,069,628		
			Residual Risk \$700,599		

● Likelihood (L) ● Impact (I) ● Risk (R)

Figure 31 Overall Likelihoods, Impacts, and Risks (with Controls)

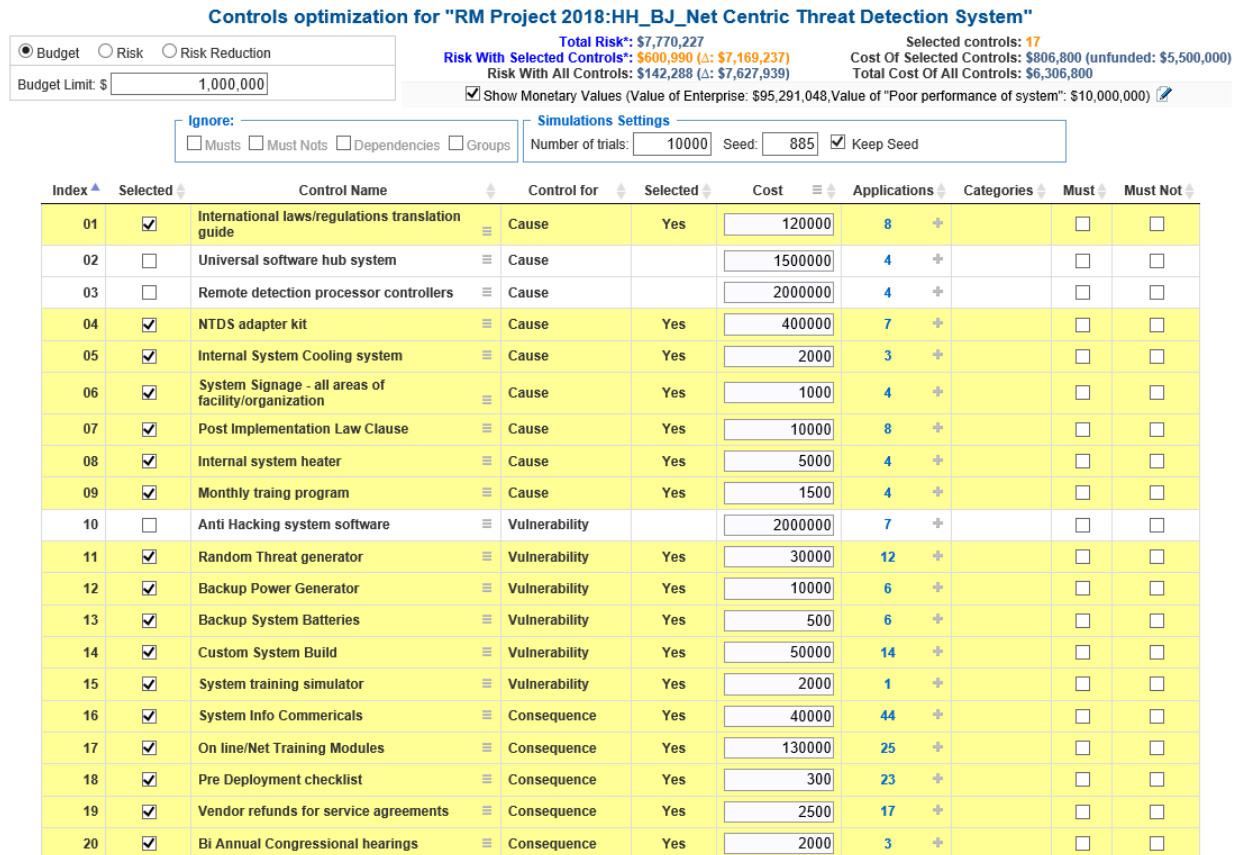


Figure 32 Selected Controls (Optimized Max Budget)

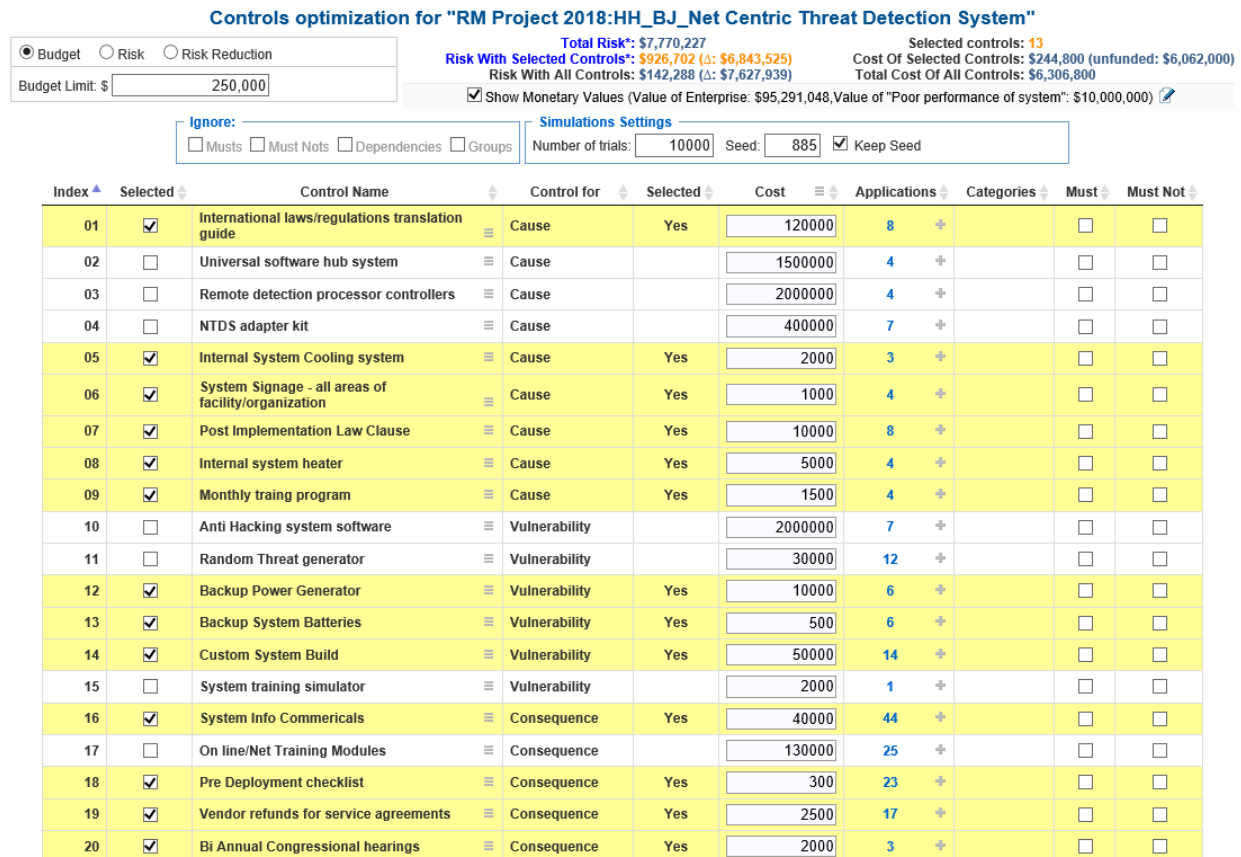


Figure 33 Selected Controls (Optimized Minimum Budget)

Based on the Efficient Frontier, we can see that we can further reduce the budget to \$275,300. Once the budget exceeds \$400,000, the risk value becomes stagnant, and any increase in the budget becomes negligible.

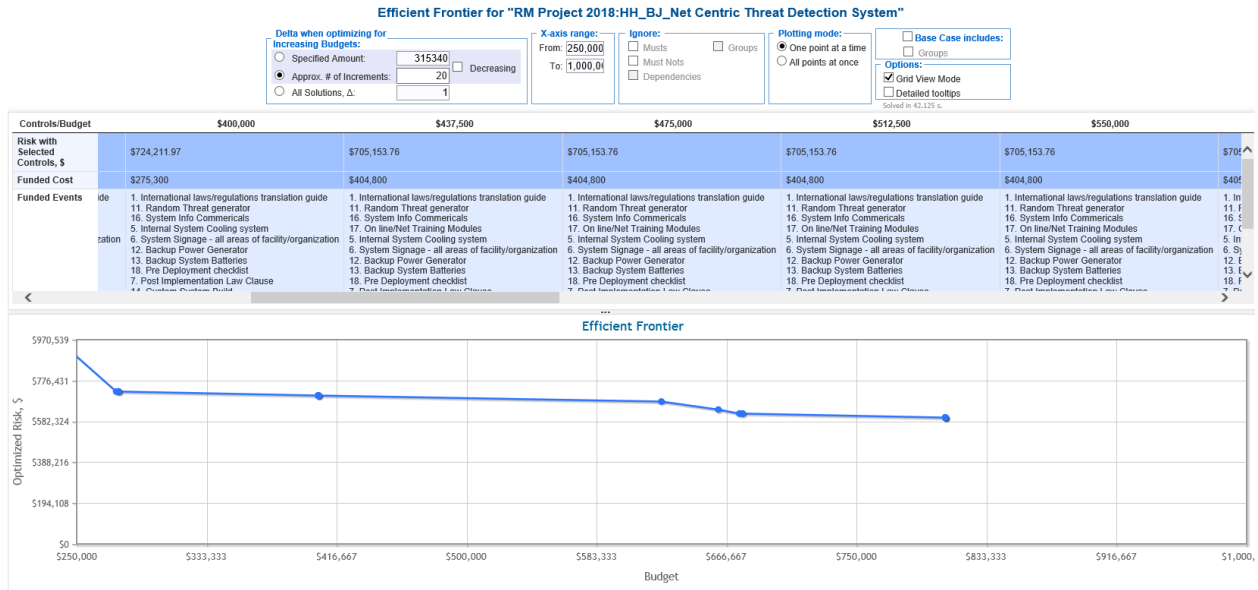


Figure 34 Efficient Frontier

7. Recommendations and Conclusion

Based on our results, it would be in the best interest of TotalSource Solutions Inc. to proceed with the project and implement the selected controls. The 15 selected controls show a risk reduction by more than half. Once more controls are implemented, the control cost goes up, but the risk reduction remains almost the same.

Public Safety is a great concern for all leaders throughout the world. Many try to provide safety without infringing on the rights and privacy of their citizenry. With the right configuration, the Net Centric Threat Detection System can bridge the gap between nation leaders and their citizens by providing wide-ranging safety without encroaching into privacy and rights. However, as our analysis has shown, the highest event likelihood is laws/regulations being violated, which could deter many people who would be needed to implement the system. By selecting a team of highly qualified individuals to mitigate the risks, the NTDS could be the answer to public safety around the world.

References

<https://www.expertchoice.com>

Risk Management Lecture Slides -Fall 2018