Cyber Risk Assessment of Suncoast Federal Credit Union

DNSC 6254 Risk Management, Fall 2017

Professor Ernest Forman

By Chris Taysom and Maria Martinez

Table of Contents

Introduction and background

The Regional Board for the Suncoast Federal Credit Union (Suncoast FCU) in Hillsborough County Florida was concerned about several cyber incidences that have occurred recently across multiple different industries. The recent international Equifax data breach demonstrated the need of a thorough understanding of the organization’s strengths and weaknesses in relation to a possible cyber event. Suncoast FCU determined to perform a cyber risk assessment of its readiness for cyber vulnerabilities and threats for the remainder of the fiscal year.

Terminology

The Chairwoman of the board wanted to be clear regarding terminology before initializing the risk assessment. She was aware that certain terms are used interchangeably in the risk management industry and felt clarity was important to get good results. First and foremost, she emphasized that a risk, a risk event, and an event are synonymous, and all refer to the same thing. These terms refer to an occurrence that may or may not actually happen – but if it did, it would inflict a *loss* on one of the Credit Union’s objectives.

She also clarified that source, threat, and hazard were also synonymous – and referred to something that may *lead* to a risk event. She was careful to point out that a source, threat, or hazard did not carry a loss in and of themselves.

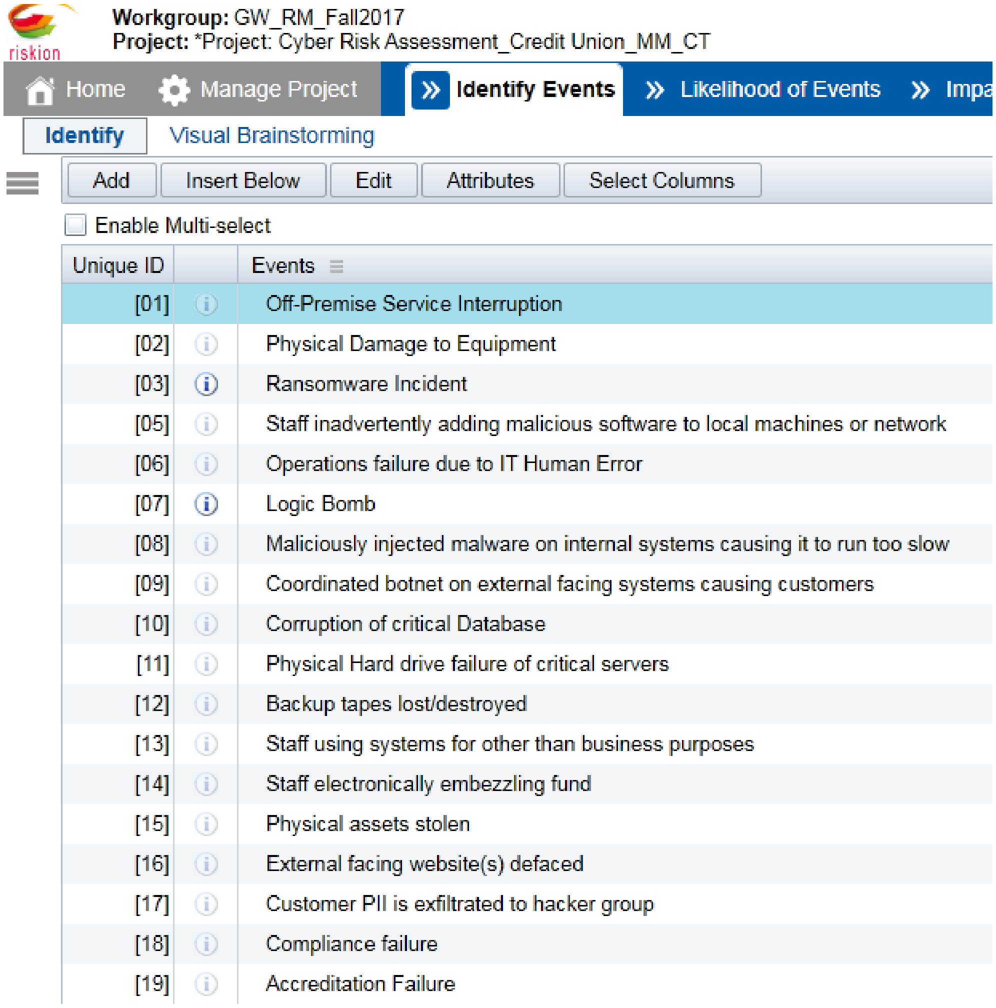
With these important terms clarified, the risk assessment was started with an identification of risk events.

The Board collectively determined that to provide a proper risk assessment, they would need a software tool. Riskion was chosen as the preferred software tool.

Identifying Risk Events and Objectives

As can be seen, there were numerous risks events identified.

FIGURE 1



Workgroup: GW_RM_Fall2017
Project: *Project: Cyber Risk Assessment_Credit Union_MM_CT

□ Enable Multi-select

Unique ID		Events
[01]	ⓘ	Off-Premise Service Interruption
[02]	ⓘ	Physical Damage to Equipment
[03]	ⓘ	Ransomware Incident
[05]	ⓘ	Staff inadvertently adding malicious software to local machines or network
[06]	ⓘ	Operations failure due to IT Human Error
[07]	ⓘ	Logic Bomb
[08]	ⓘ	Maliciously injected malware on internal systems causing it to run too slow
[09]	ⓘ	Coordinated botnet on external facing systems causing customers
[10]	ⓘ	Corruption of critical Database
[11]	ⓘ	Physical Hard drive failure of critical servers
[12]	ⓘ	Backup tapes lost/destroyed
[13]	ⓘ	Staff using systems for other than business purposes
[14]	ⓘ	Staff electronically embezzling fund
[15]	ⓘ	Physical assets stolen
[16]	ⓘ	External facing website(s) defaced
[17]	ⓘ	Customer PII is exfiltrated to hacker group
[18]	ⓘ	Compliance failure
[19]	ⓘ	Accreditation Failure

This preliminary list of risk events are better understood in the context of the Credit Union's objectives. The Chairwoman helped her team formulate this list of risk events by asking her team 'what keeps you up at night?'

The ensuing discussion revealed that the primary worry among all team members was that customer PII (personally identifiable information) would not be safeguarded. The damage to the Credit Union's reputation, along with any accompanying fines or lawsuits, could cause irreparable harm.

The complement of these worries translated into a clear *objective*: Safeguard all customer PII and ensure that the community and customer base had a high level of confidence that this was the case.

Two other concerns were compliance and accreditation. Fines could be levied against the firm for noncompliance and accreditation failures. Official compliance failures occur relatively infrequently but when they happen, it causes a financial loss in addition to the reputation of the firm.

This concern translated this into an objective. It was determined that one of the firms objectives was to reduce the risk of compliance or accreditation failure to 1%.

The third objective was to Achieve a Tier 4 Maturity Rating as Measured by the NIST CSF. The Chairwoman wanted to make sure that the risk assessment laid the groundwork to transform any elements of the culture of the organization into one that utilized repeatable and adaptable process that supported sound cyber security practices.

She felt her organization was very good at this already but didn't know how to measure it. She also knew that many of the events that they listed would be indicative of what level the organization was at in terms of cyber maturity.

This translated into an objective of achieving a Tier 4 mature rating. In its online Cybersecurity Framework, the NIST defines a Tier 4 maturity rating as follows:

Adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. – Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner (NIST, 2014).

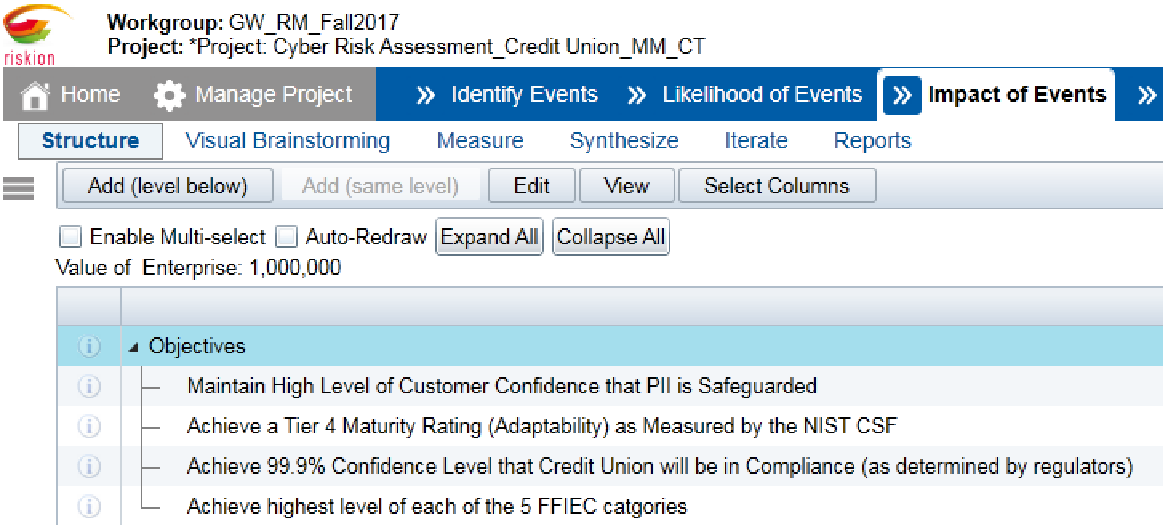
The final objective also related to organizational readiness in regard to cyber threats. The FFIEC has 5 categories of Cyber domains and a rating for each one.

1. Cyber Risk Management & Oversight
2. Threat Intelligence & Collaboration
3. Cybersecurity Controls
4. External Dependency Management
5. Cyber Incident Management & Resilience

The board defined an objective to achieve a level of 5 in each category. These objectives were aggressive to be sure, but the Chairwoman felt that a true understanding of the state of the Credit Union was required.

Objectives

FIGURE 2



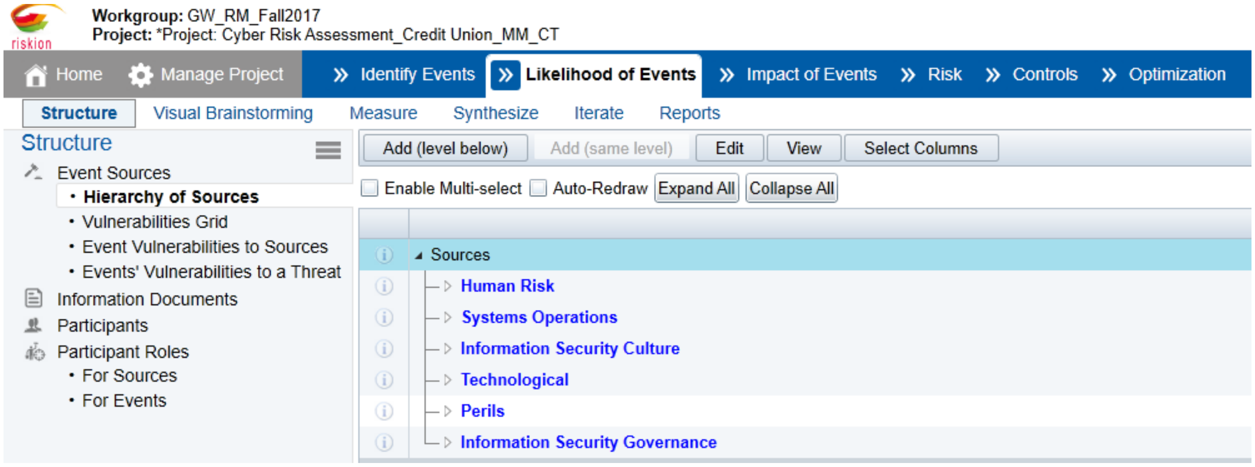
Workgroup: GW_RM_Fall2017
Project: *Project: Cyber Risk Assessment_Credit Union_MM_CT

Value of Enterprise: 1,000,000

- Objectives
  - Maintain High Level of Customer Confidence that PII is Safeguarded
  - Achieve a Tier 4 Maturity Rating (Adaptability) as Measured by the NIST CSF
  - Achieve 99.9% Confidence Level that Credit Union will be in Compliance (as determined by regulators)
  - Achieve highest level of each of the 5 FFIEC catgories

Hierarchy

<u>FIGURE 3</u>



Workgroup: GW_RM_Fall2017
Project: *Project: Cyber Risk Assessment_Credit Union_MM_CT

- Sources
  - Human Risk
  - Systems Operations
  - Information Security Culture
  - Technological
  - Perils
  - Information Security Governance

As stated previously, the Chairwoman indicated that there is a difference between a Risk Event and a Source. A risk event is something that may or may not happen, but if it were to happen there would be a *loss.*

The risk sources that were identified were categorized and defined as follows:

Human Risk: Human risk is a key element regarding cyber security. It is essential that skilled team members are aware of cyber intrusions, systems functions. Likewise, team members should be trained to handle a disaster, cyber event, or incidents related to system failures. Adequate screening and knowledge of cyber and information management is critical.

Systems Operations: Systems operations entails a rigorous understanding of systems applications, system hardware and third-party and external software – all in relation to access controls and information management controls.

Information Security Culture: Information security culture is real but difficult to define. What is sure is that a culture that understands the importance of information security must be a priority of top management. Information security culture is a set of activities and practices that foster awareness and appreciation of the importance of safeguarding data throughout all levels of the organization.

Technological: Technology consists of hard and soft assets that must have security configurations, applied access controls, acceptable vendor relationships with outsourced technology and information management services.

Perils: Perils are unpredictable and unpreventable natural or external events. These events can be mitigated to some extent by Business Continuity Planning. Some risks can also be transferred to an Insurance Company.

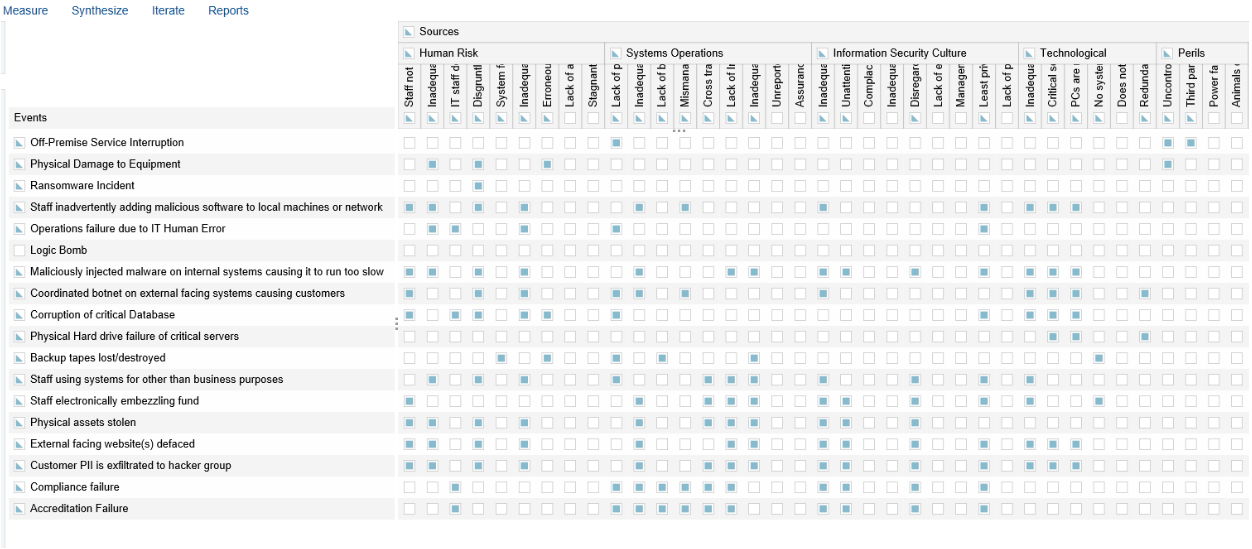
Information Security Governance: Information security governance is a framework that includes policies, procedures, standards and guidelines for information security management.

Mapping sources to events

As previously mentioned, risk events are not synonymous with sources. Sources do not have loss. Risk events do. A crucial step in the risk assessment process is to identify how sources can *contribute* to an event.

Riskion software enables this mapping.

FIGURE 4



	◣ Sources																																				
	◣ Human Risk									◣ Systems Operations									◣ Information Security Culture									◣ Technological						◣ Perils			
	Staff not	Inadequa	IT staff d	Disgruntl	System fi	Inadequa	Erroneou	Lack of a	Stagnant	Lack of p	Inadequa	Lack of b	Mismana	Cross tra	Lack of li	Inadequa	Unreport	Assuranc	Inadequa	Unattenti	Complac	Inadequa	Disregar	Lack of e	Manager	Least pri	Lack of p	Inadequa	Critical s	PCs are	No syste	Does not	Redunda	Uncontro	Third par	Power fa	Animals
Events	◣	◣	◣	◣	◣	◣	◣	□	□	◣	◣	◣	◣	◣	◣	◣	□	□	◣	◣	□	□	◣	□	□	◣	□	◣	◣	◣	◣	□	◣	◣	◣	□	□
◣ Off-Premise Service Interruption	□	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	■	□	□
◣ Physical Damage to Equipment	□	■	□	■	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	□	□	□
◣ Ransomware Incident	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
◣ Staff inadvertently adding malicious software to local machines or network	■	■	□	■	□	■	□	□	□	□	■	□	■	□	□	□	□	□	■	□	□	□	□	□	□	■	□	■	■	■	□	□	□	□	□	□	□
◣ Operations failure due to IT Human Error	□	■	■	□	□	■	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□
□ Logic Bomb	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
◣ Maliciously injected malware on internal systems causing it to run too slow	■	■	□	■	□	■	□	□	□	□	■	□	□	□	■	■	□	□	■	■	□	□	■	□	□	■	□	■	■	■	□	□	□	□	□	□	□
◣ Coordinated botnet on external facing systems causing customers	■	□	□	■	□	■	□	□	□	■	■	□	■	□	□	□	□	□	■	□	□	□	□	□	□	□	□	■	■	■	□	□	■	□	□	□	□
◣ Corruption of critical Database	■	□	■	■	□	■	■	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	□	■	■	■	□	□	□	□	□	□	□
◣ Physical Hard drive failure of critical servers	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	■	□	□	■	□	□	□	□
◣ Backup tapes lost/destroyed	□	□	□	□	■	□	■	□	□	■	□	■	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□
◣ Staff using systems for other than business purposes	□	■	□	■	□	■	□	□	□	■	□	□	□	■	■	■	□	□	■	□	□	□	■	□	□	■	□	■	□	□	□	□	□	□	□	□	□
◣ Staff electronically embezzling fund	■	□	□	□	□	□	□	□	□	□	■	□	□	■	■	■	□	□	■	■	□	□	■	□	□	■	□	■	□	□	■	□	□	□	□	□	□
◣ Physical assets stolen	■	■	□	■	□	■	□	□	□	□	■	□	□	■	■	■	□	□	■	■	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□
◣ External facing website(s) defaced	■	■	□	■	□	■	□	□	□	□	■	□	□	□	■	■	□	□	■	■	□	□	■	□	□	■	□	■	■	■	□	□	□	□	□	□	□
◣ Customer PII is exfiltrated to hacker group	■	■	□	■	□	■	□	□	□	□	■	□	□	■	■	■	□	□	■	■	□	□	■	□	□	■	□	■	■	■	□	□	□	□	□	□	□
◣ Compliance failure	□	□	■	□	□	□	□	□	□	■	■	■	■	■	■	□	□	□	■	■	□	□	■	□	□	■	□	□	□	□	□	□	□	□	□	□	□
◣ Accreditation Failure	□	□	■	□	□	□	□	□	□	■	■	■	■	■	■	□	□	□	■	■	□	□	■	□	□	■	□	□	□	□	□	□	□	□	□	□	□

Participants

The following participants were chosen to provide judgements in regards to different areas of the risk assessment.

Janice Lopez – Chairwoman of the Board of Directors

Peter Flynn – Vice Chairman of the Board of Directors

Anthony Satchel – Risk Committee Chair

Brian Feldman – Director of Operations

Velia Pedrero – Customer Relations Committee Chair

Margaret Campbell – Director of IT operations

In relation to categories of risk events, different members of the board were asked to provide judgements for their specific area of expertise.

Anthony Satchel was asked to provide judgements about the possibility of different Human Risk factors. This was deemed appropriate as he serves as Risk Committee Chair.

Another example is Margaret Campbell, the Director of IT operations. She was asked to provide judgements in regard to Technological risks.

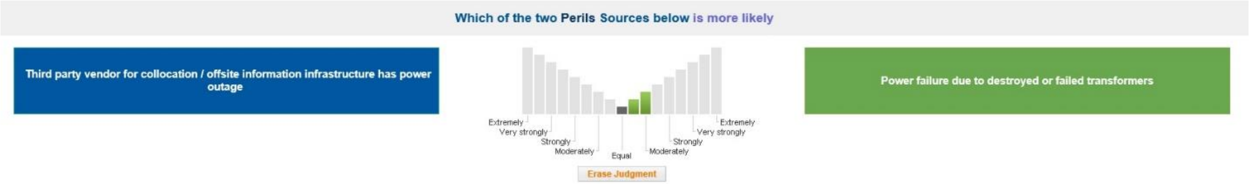
Each participant was invited to provide judgements in their specific area.

Pairwise Comparison

To assess the likelihood of different risk events, the participants were presented a series of Pairwise comparisons and other methods. Riskion is software that uses mathematical processes to derive ratio scale data as an output of verbal judgements.

Here is an example.

FIGURE 5



Which of the two Perils Sources below is more likely

Third party vendor for collocation / offsite information infrastructure has power outage

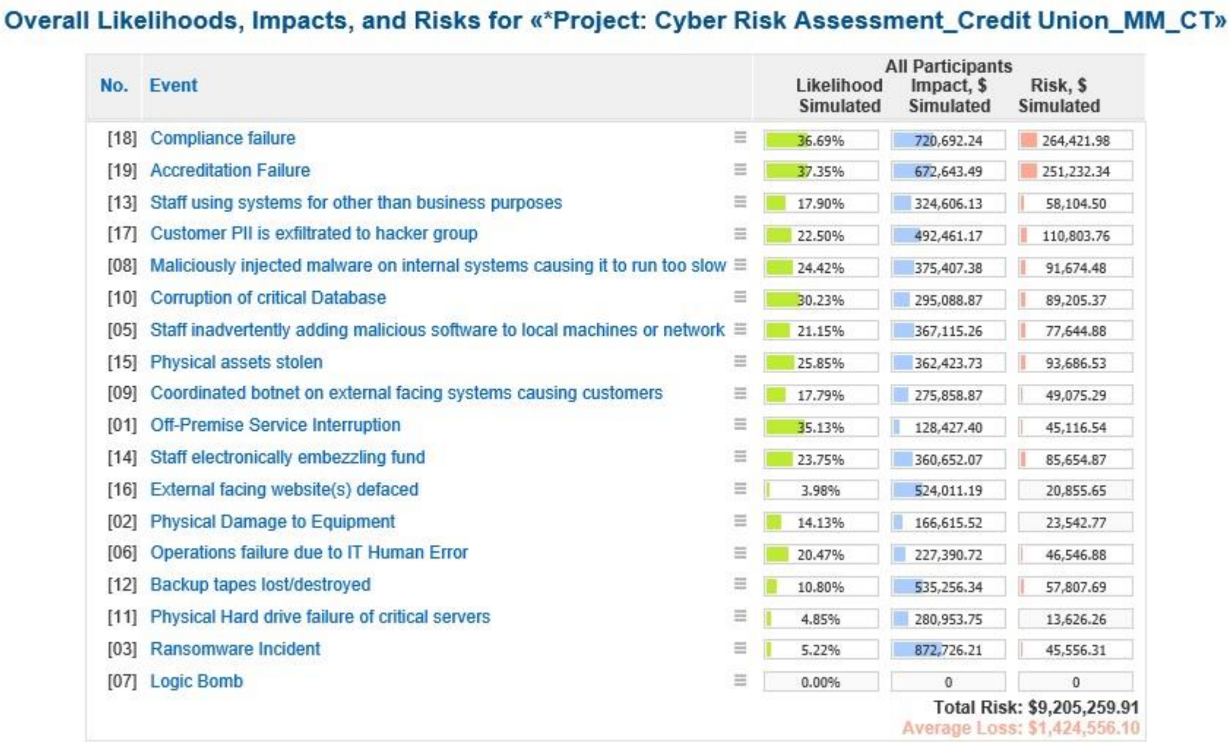
Power failure due to destroyed or failed transformers

Though the above is just one example of the different methods to get inputs from participants, it should be noted that the process to complete the survey is long and involved. The Chairwoman made sure that everybody had plenty of time to complete their surveys without a sense of being rushed.

Overall Risks

Using this and other methods to derive ratio scale values of the participants, a final picture of risk was assessed. An independent expert was brought in to ascribe financial aspects of each of the risk events the Credit Union was concerned with.

FIGURE 6



Overall Likelihoods, Impacts, and Risks for «*Project: Cyber Risk Assessment_Credit Union_MM_CT»

No.	Event		All Participants	
		Likelihood Simulated	Impact, $ Simulated	Risk, $ Simulated
[18]	Compliance failure	36.69%	720,692.24	264,421.98
[19]	Accreditation Failure	37.35%	672,643.49	251,232.34
[13]	Staff using systems for other than business purposes	17.90%	324,606.13	58,104.50
[17]	Customer PII is exfiltrated to hacker group	22.50%	492,461.17	110,803.76
[08]	Maliciously injected malware on internal systems causing it to run too slow	24.42%	375,407.38	91,674.48
[10]	Corruption of critical Database	30.23%	295,088.87	89,205.37
[05]	Staff inadvertently adding malicious software to local machines or network	21.15%	367,115.26	77,644.88
[15]	Physical assets stolen	25.85%	362,423.73	93,686.53
[09]	Coordinated botnet on external facing systems causing customers	17.79%	275,858.87	49,075.29
[01]	Off-Premise Service Interruption	35.13%	128,427.40	45,116.54
[14]	Staff electronically embezzling fund	23.75%	360,652.07	85,654.87
[16]	External facing website(s) defaced	3.98%	524,011.19	20,855.65
[02]	Physical Damage to Equipment	14.13%	166,615.52	23,542.77
[06]	Operations failure due to IT Human Error	20.47%	227,390.72	46,546.88
[12]	Backup tapes lost/destroyed	10.80%	535,256.34	57,807.69
[11]	Physical Hard drive failure of critical servers	4.85%	280,953.75	13,626.26
[03]	Ransomware Incident	5.22%	872,726.21	45,556.31
[07]	Logic Bomb	0.00%	0	0

Total Risk: $9,205,259.91
Average Loss: $1,424,556.10

Controls

With the risks presented, an examination of varying controls (along with their respective costs) was evaluated. A total of 19 controls were identified.

1) Comprehensive Cisco Security Infrastructure
2) Quarterly Employee Training Program
3) IT Staff Salary Budget Increase
4) Annual Security IT Assessments
5) The Creation of a Chief Compliance Officer Position
6) Cyber Performer of the Month Award Program
7) Onboarding Process Modification
8) Quarterly Penetration Testing
9) NIST Framework Establishment (Outside Consultants)
10) Cyber Initiation Program
11) Data at Rest Encryption Implementation
12) Perimeter Defense (Firewalls, Proxy, IPS etc.) Upgrade Project
13) Thin Clients with Outsourced Threat Analysis Contract

14) 3rd Party Data Warehousing Change
15) Job Rotation Implementation
16) Daily Logon Cyber Awareness Reminder
17) Implement Rainbow Table Solution in All Databases
18) Public Relations Firm – On Retainer
19) Insurance – Breach Coverage

Controls for Threats, Vulnerabilities, and Consequence

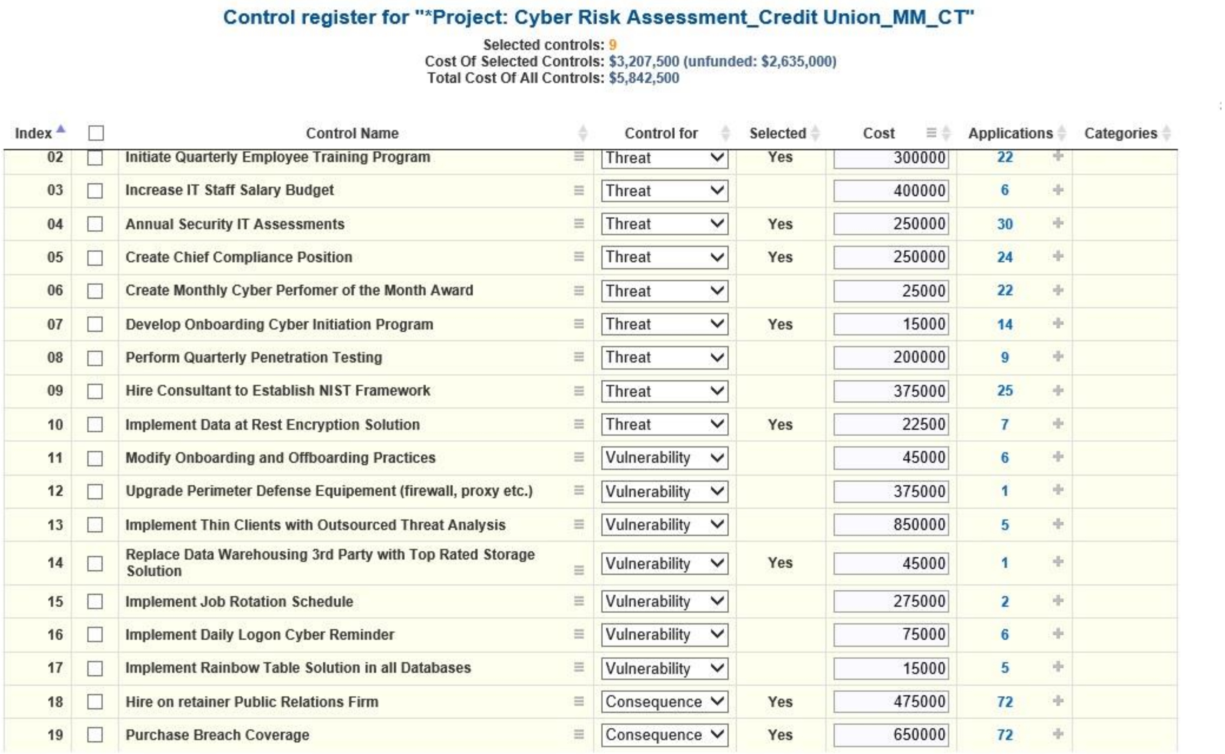
It is important to understand that all these identified controls are implement a mitigation for one of the following:

1) Threat
2) Vulnerability
3) Consequence

If a control is implemented for a threat, it will reduce the likelihood of that threat. If a control is implemented for a vulnerability, it will reduce the likelihood of a vulnerability, *given* a threat. Lastly a control for consequence is to mitigate the impact of an event after it has already occurred.

The following Figure encapsulates the controls, their respective costs, what the control is for (threat, vulnerability, or consequence), and how many different applications the control can be applied to.

FIGURE 7



Control register for "*Project: Cyber Risk Assessment_Credit Union_MM_CT"

Selected controls: 9
Cost Of Selected Controls: $3,207,500 (unfunded: $2,635,000)
Total Cost Of All Controls: $5,842,500

Index	□	Control Name	Control for	Selected	Cost	Applications	Categories
02	□	Initiate Quarterly Employee Training Program	Threat	Yes	300000	22	
03	□	Increase IT Staff Salary Budget	Threat		400000	6	
04	□	Annual Security IT Assessments	Threat	Yes	250000	30	
05	□	Create Chief Compliance Position	Threat	Yes	250000	24	
06	□	Create Monthly Cyber Perfomer of the Month Award	Threat		25000	22	
07	□	Develop Onboarding Cyber Initiation Program	Threat	Yes	15000	14	
08	□	Perform Quarterly Penetration Testing	Threat		200000	9	
09	□	Hire Consultant to Establish NIST Framework	Threat		375000	25	
10	□	Implement Data at Rest Encryption Solution	Threat	Yes	22500	7	
11	□	Modify Onboarding and Offboarding Practices	Vulnerability		45000	6	
12	□	Upgrade Perimeter Defense Equipement (firewall, proxy etc.)	Vulnerability		375000	1	
13	□	Implement Thin Clients with Outsourced Threat Analysis	Vulnerability		850000	5	
14	□	Replace Data Warehousing 3rd Party with Top Rated Storage Solution	Vulnerability	Yes	45000	1	
15	□	Implement Job Rotation Schedule	Vulnerability		275000	2	
16	□	Implement Daily Logon Cyber Reminder	Vulnerability		75000	6	
17	□	Implement Rainbow Table Solution in all Databases	Vulnerability		15000	5	
18	□	Hire on retainer Public Relations Firm	Consequence	Yes	475000	72	
19	□	Purchase Breach Coverage	Consequence	Yes	650000	72	

Optimization

The team was directed to input a few constraints, indicate which controls were mandatory, and then utilize Riskion software to automatically calculate an optimized selection of controls.

The Board authorized a $3,300,000 USD budget. While this budget was initially viewed as too costly, the Chairwoman was convinced that it was a good investment. Most of the costs were upfront capital expenditures so subsequent annual maintenance costs would be dramatically lower. More importantly, the Chairwoman felt that a powerful message from upper management would help solidify the culture of the Credit Union as one that considered cyber security a top priority.

In addition to the budget, there were four controls that were considered so vital to Board that they were required to be selected. These controls are listed below along with the reasoning behind why they were selected as 'must dos.'

1) Implement Data at Rest Controls – This was considered a must because of the primary consideration above all to keep customer PII out of the hands of a determined hacker group. Even if the other controls broke down and a hacker group could exfiltrate

customer data, proper Data at Rest controls would man they could not feasibly *decrypt* said data.

2) Replace Data Warehousing 3rd Party – Like the Data at Rest concerns, the most important issue was keeping a hacker group from exfiltrating data. The worry with a sub-par 3rd party who stored backup data was that once said data was out of the purview of the credit union, strict cyber controls could no longer be enforced.
3) Hire on Retainer a Public Relations Firm – The Board determined that there must be a professional group on hand that could deal with the public relations challenge in the event a cyber event did occur. The Chairwoman had noticed over the years that one of the primary problems with cyber events was an improper public response once a breach had been detected.
4) Purchase Breach Coverage – The Chairwoman finally insisted that in case of the breach, some of the financial risk could be transferred by way of insurance.

Riskion yielded the following selection with these considerations in place.

TABLE 1

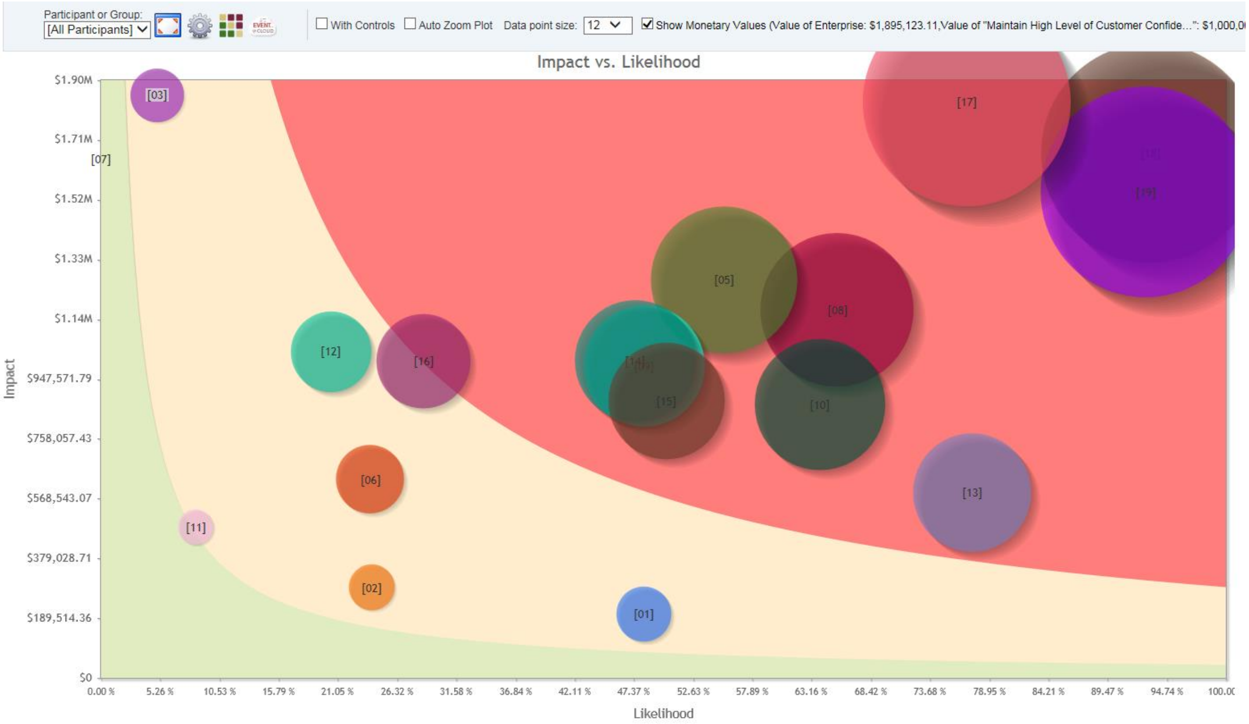
Control Name	Control for	Cost	Applications	Must
Comprehensive Cisco Security Infrastructure	Threat	$1,200,000.00	16	
Initiate Quarterly Employee Training Program	Threat	$300,000.00	22	
Annual Security IT Assessments	Threat	$250,000.00	30	
Create Chief Compliance Position	Threat	$250,000.00	24	
Develop Onboarding Cyber Initiation Program	Threat	$15,000.00	14	
Implement Data at Rest Encryption Solution	Threat	$22,500.00	7	Yes
Replace Data Warehousing 3rd Party with Top Rated Storage Solution	Vulnerability	$45,000.00	1	Yes

Hire on retainer Public Relations Firm	Consequence	$475,000.00	72	Yes
Purchase Breach Coverage	Consequence	$650,000.00	72	Yes

Using the Riskion software, a Risk Map was created to visualize overall risk with and without the controls.

Without controls

FIGURE 8

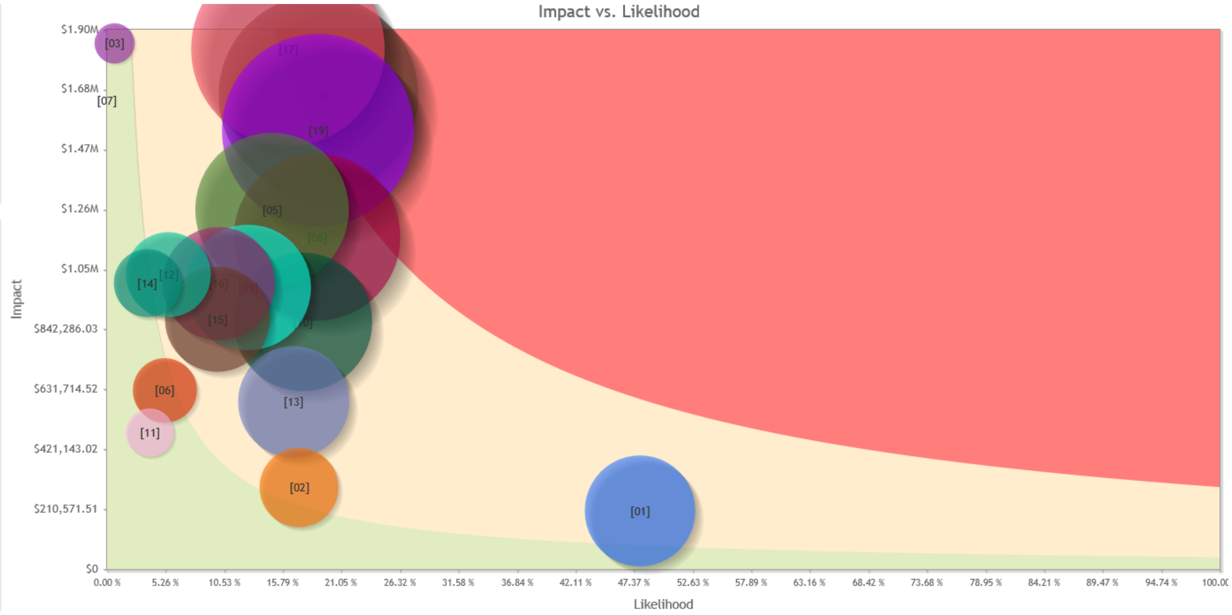


Participant or Group: [All Participants]

□ With Controls □ Auto Zoom Plot Data point size: 12 ☑ Show Monetary Values (Value of Enterprise: $1,895,123.11,Value of "Maintain High Level of Customer Confide...": $1,000,0

With Controls

FIGURE 9

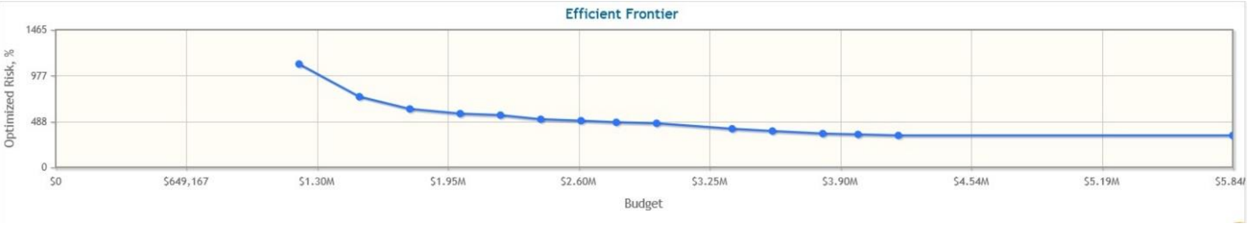


Efficient Frontier

The concept of Efficient Frontier is most often used in the context of investment strategies in the stock market. However, Efficient Frontier can be generalized to describe an analysis that will take a range of expenditures as an input and produce an output of a subset of that range – a subset that *most* maximizes risk reduction.

In the case of Suncoast Credit Union, the Riskion Software was used to produce an Efficient Frontier Analysis.

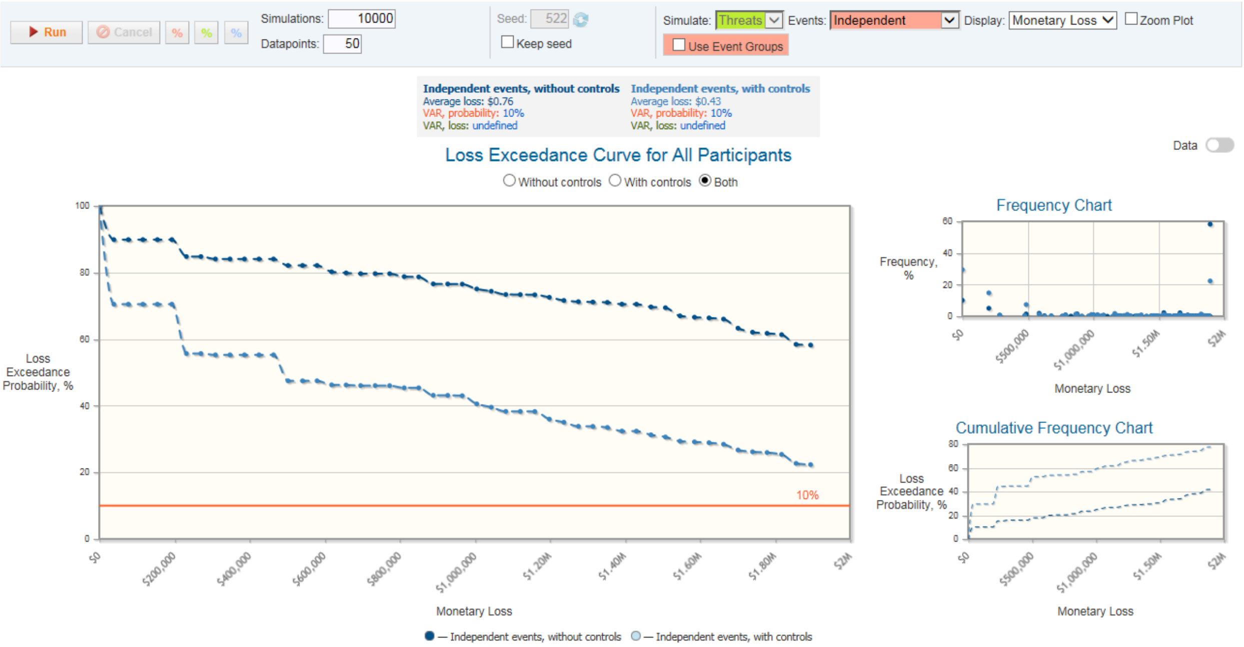
FIGURE 10



We can see that optimized risk of the controls level off at around the $4,000,000-dollar mark.

Loss Exceedance Curve

A loss exceedance curve was also generated



▶ Run | Cancel | % | % | %

Simulations: 10000

Datapoints: 50

Seed: 522

□ Keep seed

Simulate: Threats

Events: Independent

Display: Monetary Loss

□ Zoom Plot

□ Use Event Groups

Independent events, without controls
Average loss: $0.76
VAR, probability: 10%
VAR, loss: undefined

Independent events, with controls
Average loss: $0.43
VAR, probability: 10%
VAR, loss: undefined

Data

Loss Exceedance Curve for All Participants

○ Without controls ○ With controls ● Both

Citations

NIST. “NIST Cybersecurity Framework”. Page 14. NIST, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf