Simulating Cybersecurity Risk Using Advanced Quantitative Risk Assessment Techniques: A Teaching Case Study

Basil Hamdan, Ph.D.
Associate Professor - Cybersecurity
Utah Valley University

26th Colloquium for Information Systems Security Education
November 14, 2022

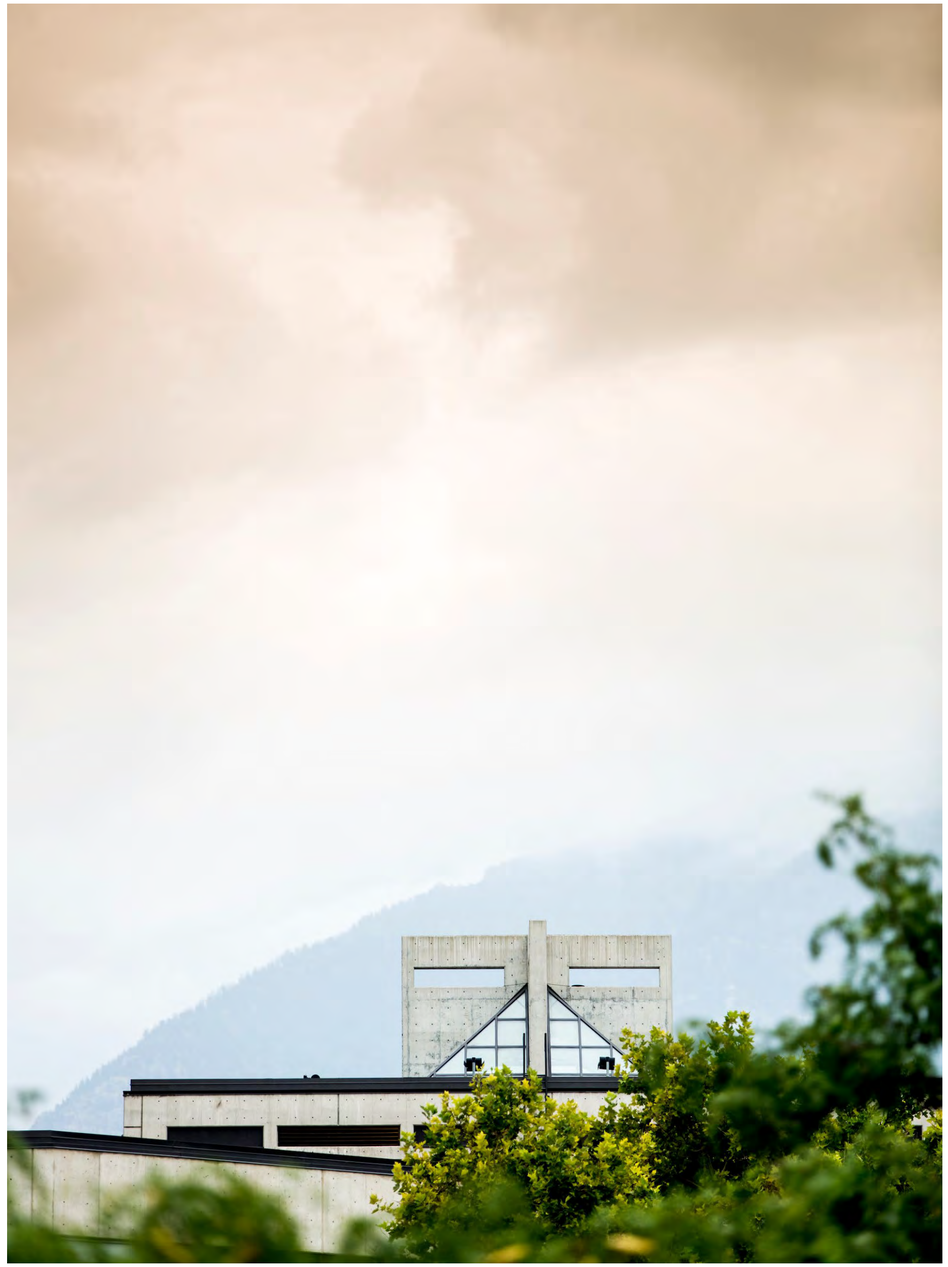
AGENDA

- Motivation
- Case Study
  - Case Scenario
  - Data Collection
  - Data Analysis
- Conclusion & Future Directions

MOTIVATION

Risk Assessment Approaches

- **Qualitative** :based on nonnumerical categories or levels (e.g., low, moderate, high).
- **Quantitative**: based on the use of numbers (e.g., 1, 2, 3)
- **Semi-Quantitative**: bins (e.g., 0-15, 16-35, 36-70, 71-85, 86-100), scales (e.g., 1-10) that translate easily into qualitative terms (e.g., a score of 95 can be interpreted as very high).



MOTIVATION

		Risk				
Impact	Severe (SV)	H	H	C	C	C
	High (H)	M	H	H	C	C
	Significant (sg)	M	M	H	H	C
	Moderate (M)	L	M	M	H	H
	Low (L)	L	L	M	M	M
	Very Low (VL)	L	L	M	M	M
		Very Low (VL)	Low (L)	Moderate (M)	High (H)	Very High (VH)
		Likelihood				

Key	Risk Level
C	Critical
H	High
M	Moderate
L	Low

$$Risk = Likelihood * Impact$$

Risk

A function of the **likelihood** of a given threat source's exercising a particular potential vulnerability, and the resulting **impact** of that adverse event on the organization [1]

MOTIVATION

Key	Risk Level
C	Critical
H	High
M	Moderate
L	Low

Risk	Likelihood	Impact	Risk Score
Risk1	H	H	H
Risk2	L	M	L
Risk3	H	SV	C
Risk4	M	M	M

$$Risk = Likelihood * Impact$$

Risk

A function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [1]

MOTIVATION

Risk	Likelihood										Impact								
	Threat Agent Factors					Vulnerability Factors					Business Impact				Technical				
	Skill Level	Motive	Access	Resources	Size	Discoverability	Exploitability	Awareness	Detectability	Likelihood Average	Financial	Productivity	Reputation	Fines and Legal Penalties	Confidentiality	Integrity	Availability	Impact (Average)	Risk Score
Risk1	6	7	5	7	5	8	8	6	9	6.8	10	7	8	9	8	5	5	7.4	50.3
Risk2	3	3	3	5	4	5	4	4	1	3.6	8	4	8	6	3	7	3	5.6	19.8
Risk3	8	7	8	8	8	9	7	6	6	7.4	9	9	8	10	7	9	6	8.3	61.7
Risk4	5	4	6	4	5	4	5	3	6	4.7	4	6	5	7	6	6	1	5.0	23.3

Source: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

RISK = LIKELIHOOD * IMPACT

MOTIVATION

Risk	Impact			Probability				Risk Score
	Damage Potential (D)	Affected Users (A)	Average	Reproducibility (R)	Exploitability (E)	Discoverability (D)	Average	
Risk1	3	4	4	3	4	3	4	**16.0**
Risk2	3	5	4	2	1	1	2	**8.0**
Risk3	5	4	5	5	5	4	5	**25.0**
Risk4	2	3	3	2	4	3	3	**9.0**

Damage – how bad would an attack be?
Reproducibility – how easy is it to reproduce the attack?
Exploitability – how much work is it to launch the attack?
Affected users – how many people will be impacted?
Discoverability – how easy is it to discover the threat?

MOTIVATION

Risk	Likelihood	Impact	Risk Score
Risk1	H	H	H
Risk2	L	M	L
Risk3	H	SV	C
Risk4	M	M	M

										Li	Impact								
											Business Impact				Technical				
											Financial	Productivity	Reputation	Fines and Legal Penalties	Confidentiality	Integrity	Availability	Impact (Average)	Risk Score
Risk1	6	7	5	7	5	8	8	6	9	6.8	10	7	8	9	8	5	5	7.4	50.3
Risk2	3	3	3	5	4	5	4	4	1	3.6	8	4	8	6	3	7	3	5.6	19.8
Risk3	8	7	8	8	8	9	7	6	6	7.4	9	9	8	10	7	9	6	8.3	61.7
Risk4	5	4	6	4	5	4	5	3	6	4.7	4	6	5	7	6	6	1	5.0	23.3

	Damag	Affec		Repro	Explo	Disco	Average	Risk Score
Risk1	3	4	4	3	4	3	4	**16.0**
Risk2	3	5	4	2	1	1	2	**8.0**
Risk3	5	4	5	5	5	4	5	**25.0**
Risk4	2	3	3	2	4	3	3	**9.0**

Mitigation Costs

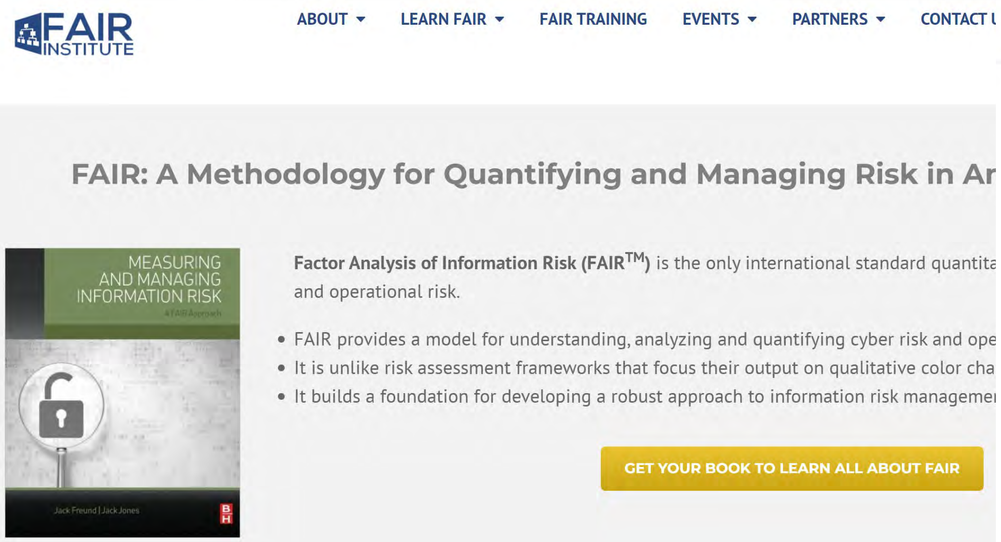
- Risk 1 (H): $700K
- Risk 2 (L): $150K
- Risk 3 (C): $1M
- Risk 4 (M): $350K

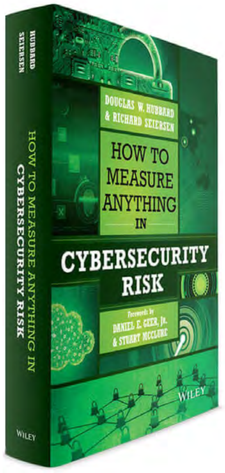
Cybersecurity Budget: $1.25M

What Risk to Prioritize?

MOTIVATION

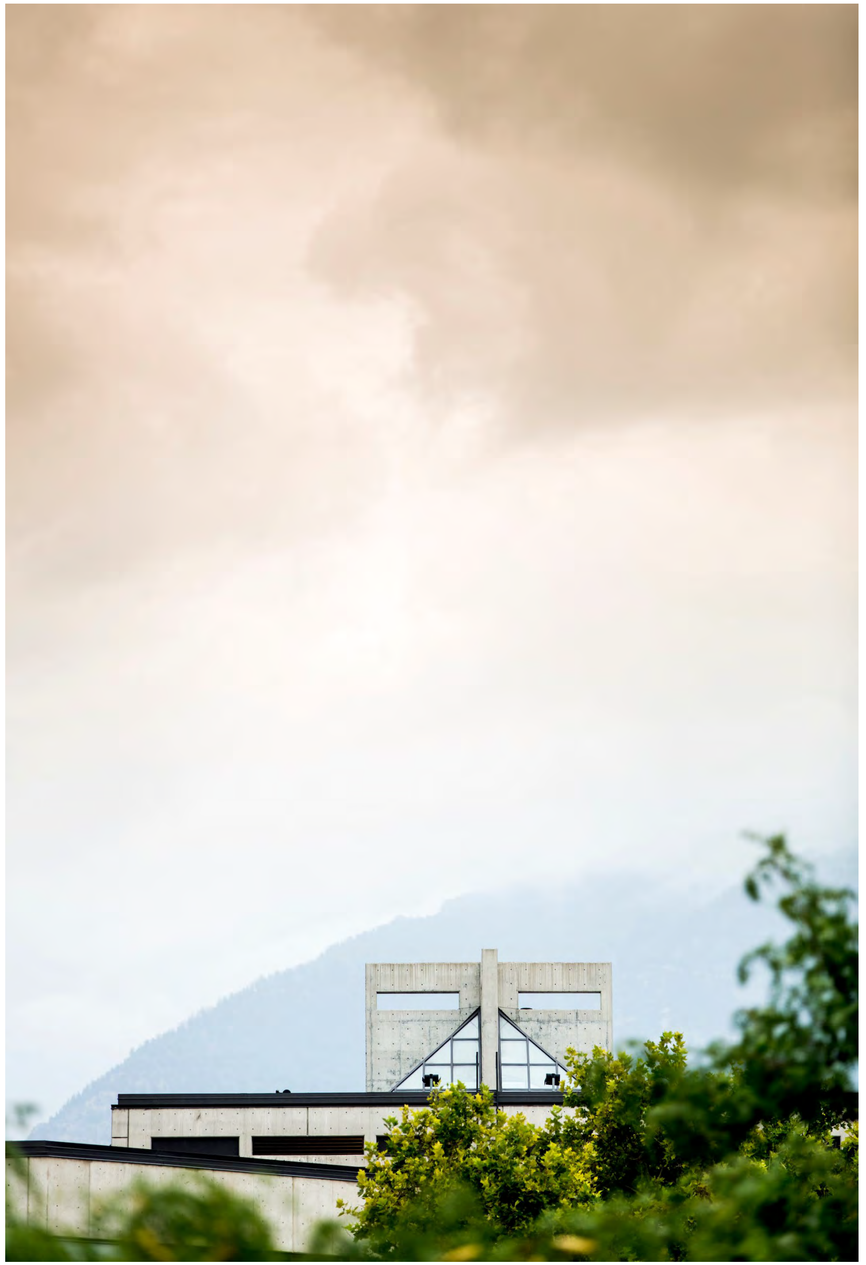
Risk	Likelihood	Impact	Risk Score
Risk1	H	H	H
Risk2	L	M	L
Risk3	H	SV	C
Risk4	M	M	M





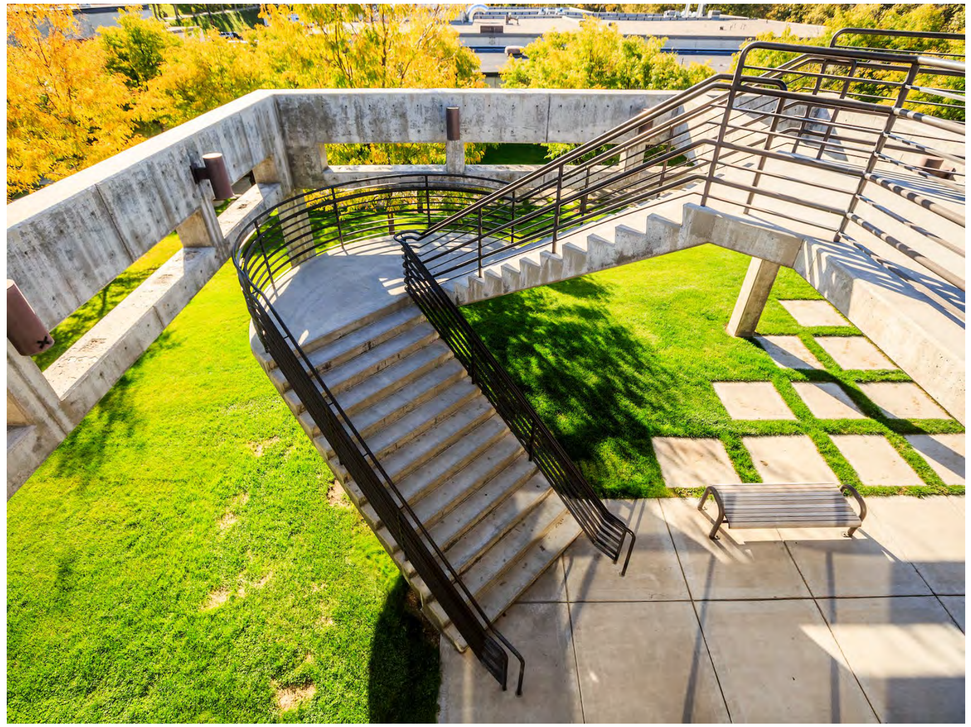
- **Mitigation Costs**
  - **Risk 1 (H): $700K**
  - **Risk 2 (L): $150K**
  - **Risk 3 (C): $1M**
  - **Risk 4 (M): $350K**
- **Cybersecurity Budget: $1.25M**
- **What Risk to Prioritize?**

CASE STUDY



CASE STUDY

The Company



The Company

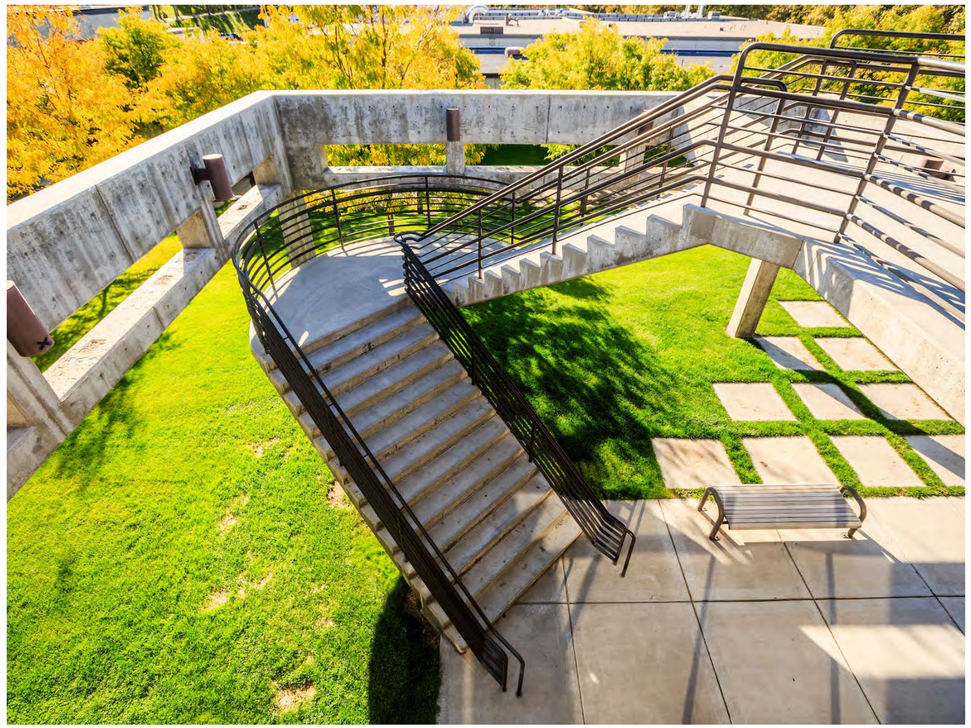
Furniture Essentials is a fast-growing e-Commerce company that sells furniture and home decor items. Despite its relatively short age, having been in business for only 10 years, the company has experienced significant growth and has quickly become one of its industry leaders.

The company employs approximately 1,500 employees and generates approximately $60 million of sales revenue per year.

Most recently, the company saw an exponential growth in its sales. While the increase in revenue was received as welcome news, it also alerted the company to the cybersecurity risk of doing business online.

CASE STUDY

Mission-Critical Assets



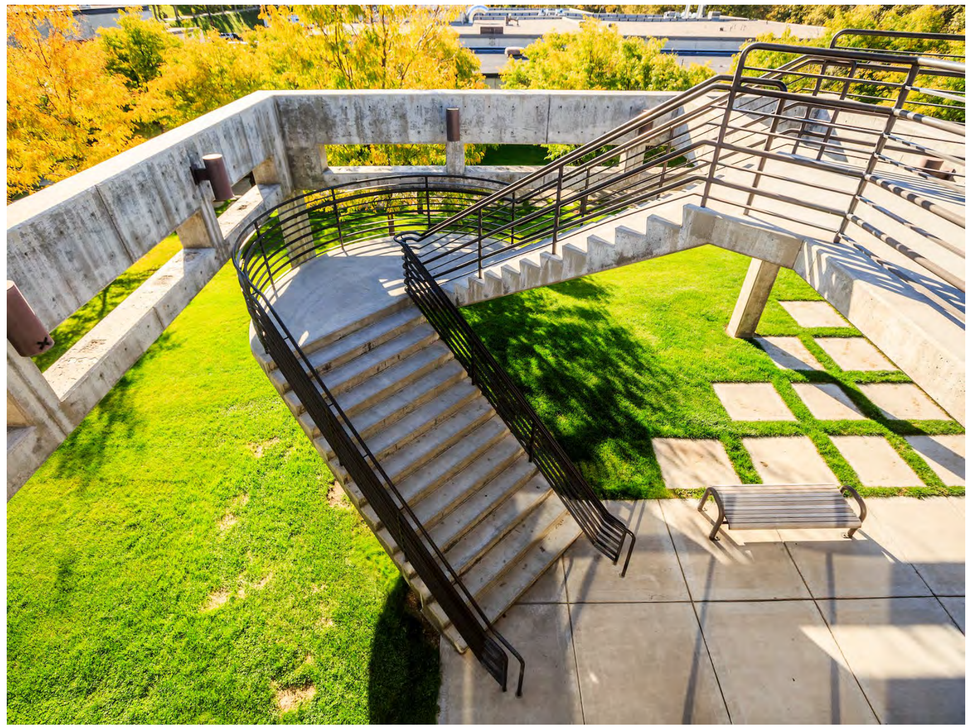
The Assets

The **eCommerce Website** which customers use to order the products that Furniture Essentials sells.

The backend **internal database** that stores customer data and order data.

CASE STUDY

Threat Scenarios



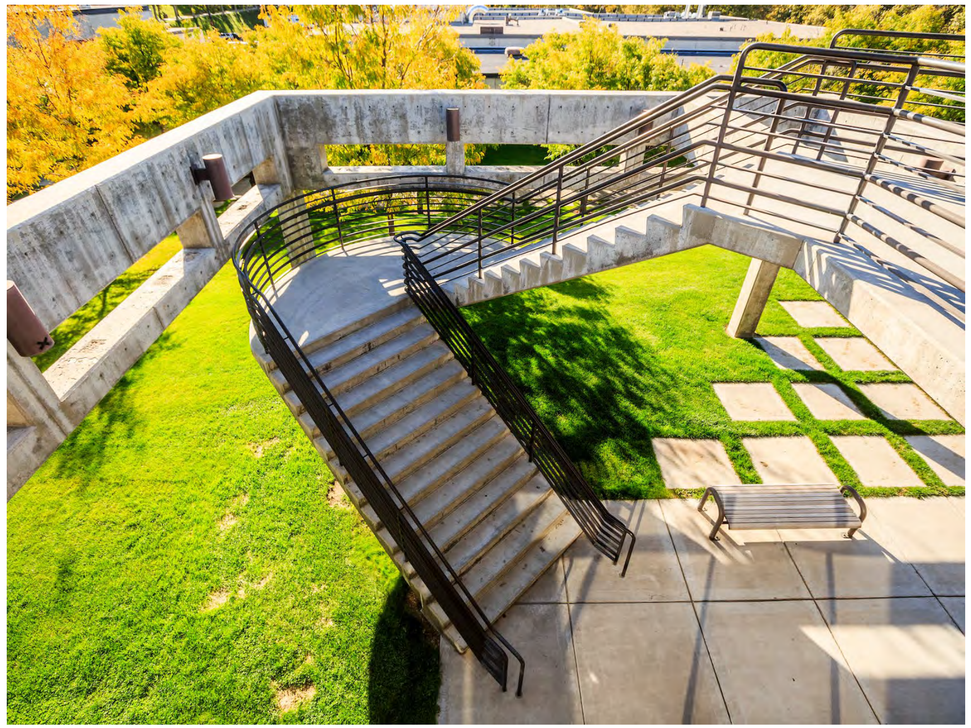
Threat Scenarios

DDoS to be the top attack vector by which malicious hackers could compromise the availability of the **eCommerce Website.**

Phishing as the top attack vector by which malicious hackers could gain unauthorized access to Furniture Essentials' systems and to breach the confidentiality of customer and order data in the **internal database**.

CASE STUDY

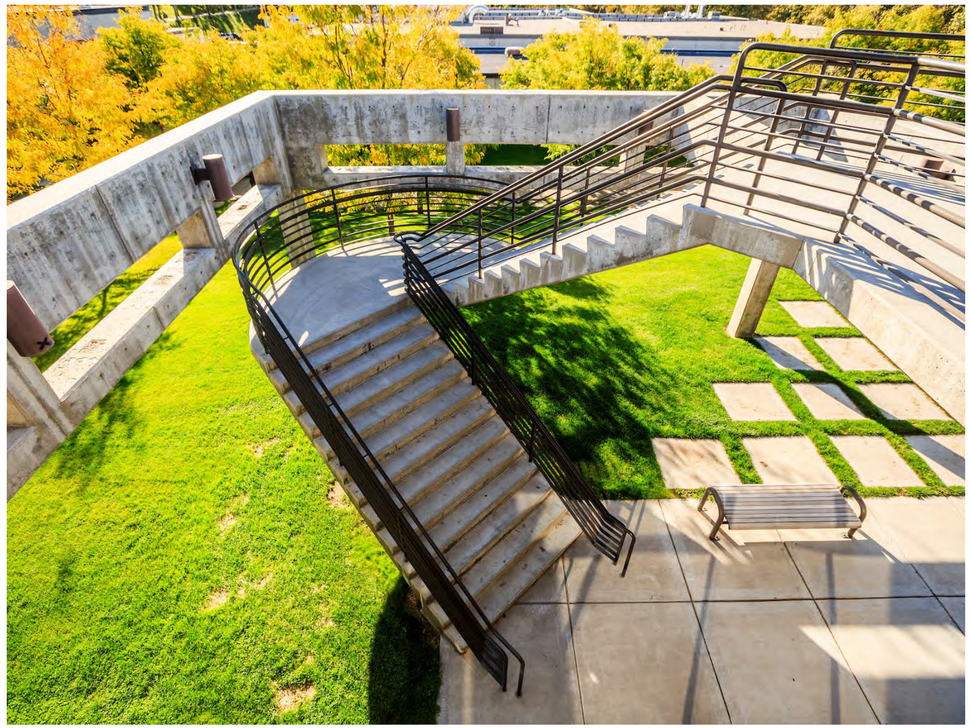
Assessment Approach



Assessment Approach
Up until now, the Cybersecurity Risk Team used both qualitative and semi-quantitative approaches to determine the risk exposure. This time around, the CISO asked the team to perform the risk analysis using a **quantitative methodology for risk assessment**.

CASE STUDY

Assessment Approach



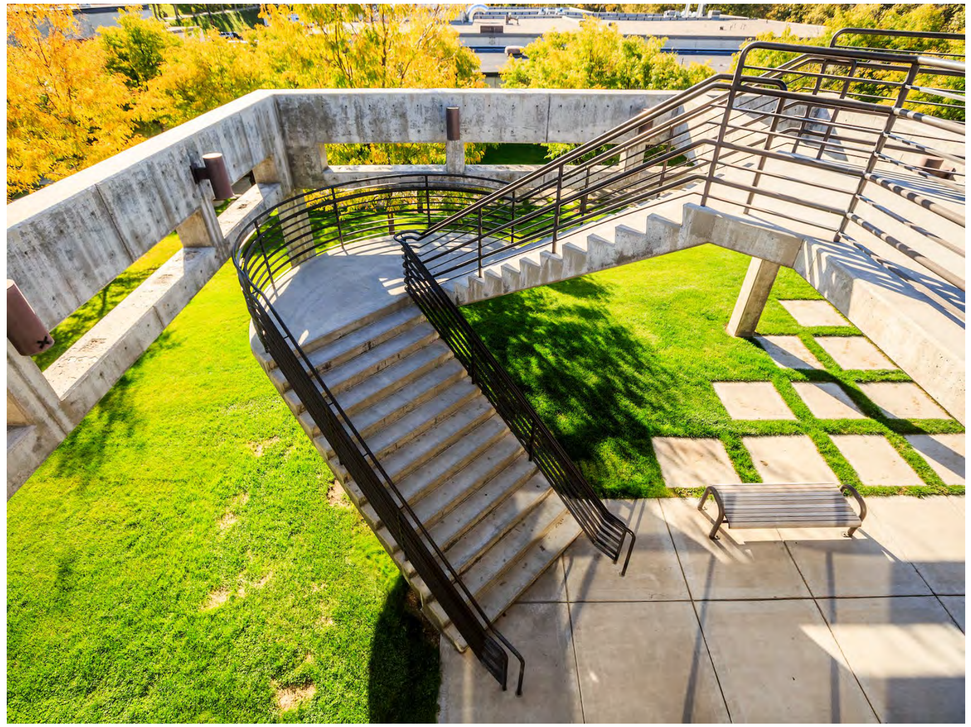
Assessment Approach

Quantitative Approach

- A soft copy of the presentation titled: How To Measure Anything in Cybersecurity Risk [3].
- An e-copy of a book titled: How To Measure Anything in Cybersecurity Risk [2].
- A MS Excel based template for Measuring Cybersecurity Risk [3].
- A soft copy of a document with the Technical Standard for Risk Taxonomy per the FAIR Framework [4].
- A link to a seminar titled: The Future of Cybersecurity Risk Management [5].

CASE STUDY

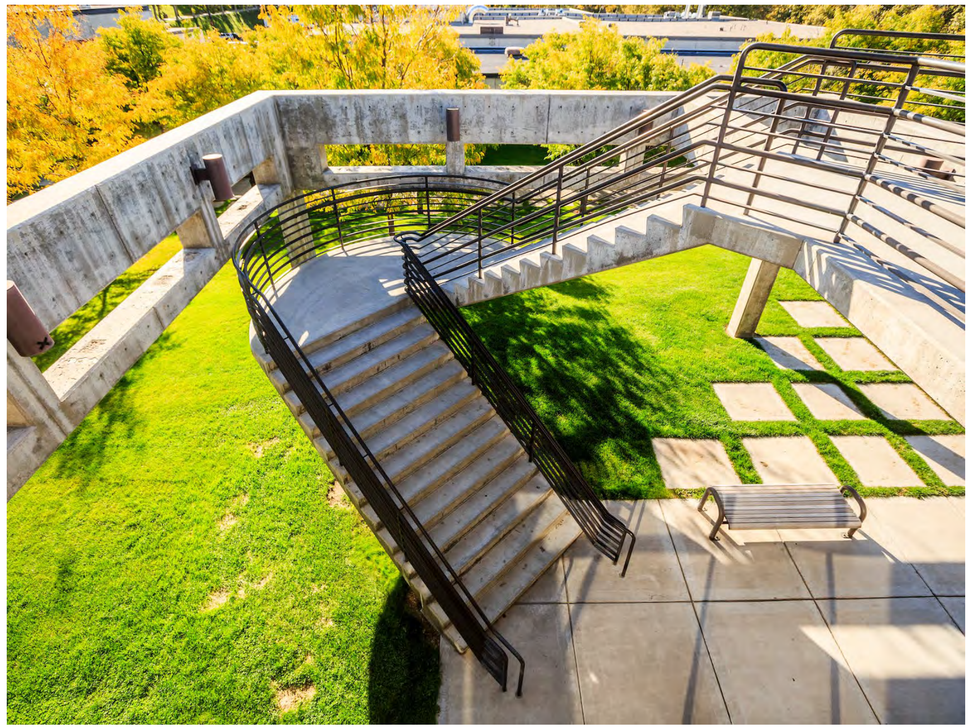
Data Collection



Data Source	Data Summary	Loss Factor
Incident Response	While no data breach has occurred (been detected) within the last 5 years, the likelihood of a data breach occurring at least once a year is 11%.	
	In the event of a data breach, an incident response team of 4-8 members will be assembled and deployed. Depending on the scope of the attack, the team is expected to work overtime for 10-30 hours. The average loaded hourly wage is $100 per hour.	Primary (Internal) Response
	In the event of a data breach, a cybersecurity company would be contracted to assist in the incident response and investigation. The investigation is expected to cost an average of $225,000.	Primary (External) Response
Network Security	An annual cybersecurity awareness training is mandatory for all employees. The training includes extensive modules on malware, phishing, password attacks, and online security. Employees must pass the training, or their credentials will be provoked.	
	An Email spam filtering solution is in place. On average, the solution catches 95% of phishing emails, preventing such emails from reaching employees' inboxes. The annual cost of the solution is $50,000.	

CASE STUDY

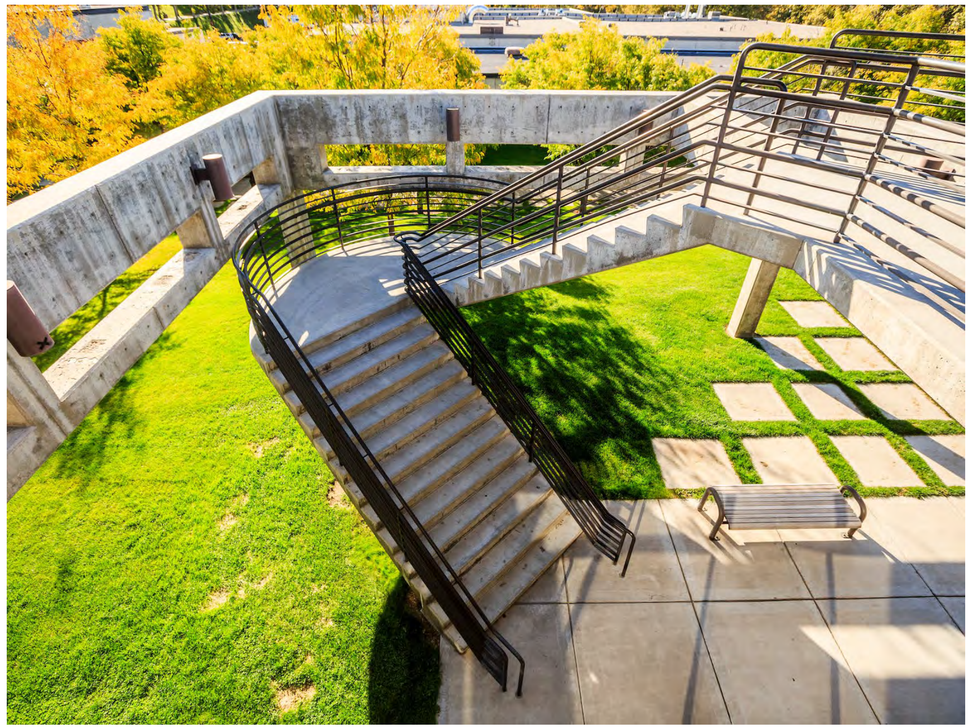
Data Collection



Data Source	Data Summary	Loss Factor
Sales Management	The company's eCommerce website generates approximately $100 million of revenue per year from a customer base **of 50,000 active customers**. The company estimates the customer lifetime value at $300 per customer.	Secondary Reputation
	Approximately, 50% of the customers store their credit card information on the company's website for faster check out.	Secondary Response
	300 employees use the order fulfillment solution for the eCommerce Website. The average loaded hourly wage is $80 per employee.	
Marketing /Public Relations	In the event of a data breach, it is estimated that 10% of impacted customers would stop purchasing products from Furniture Essentials and switch to a competitor going forward.	Secondary Reputation

CASE STUDY

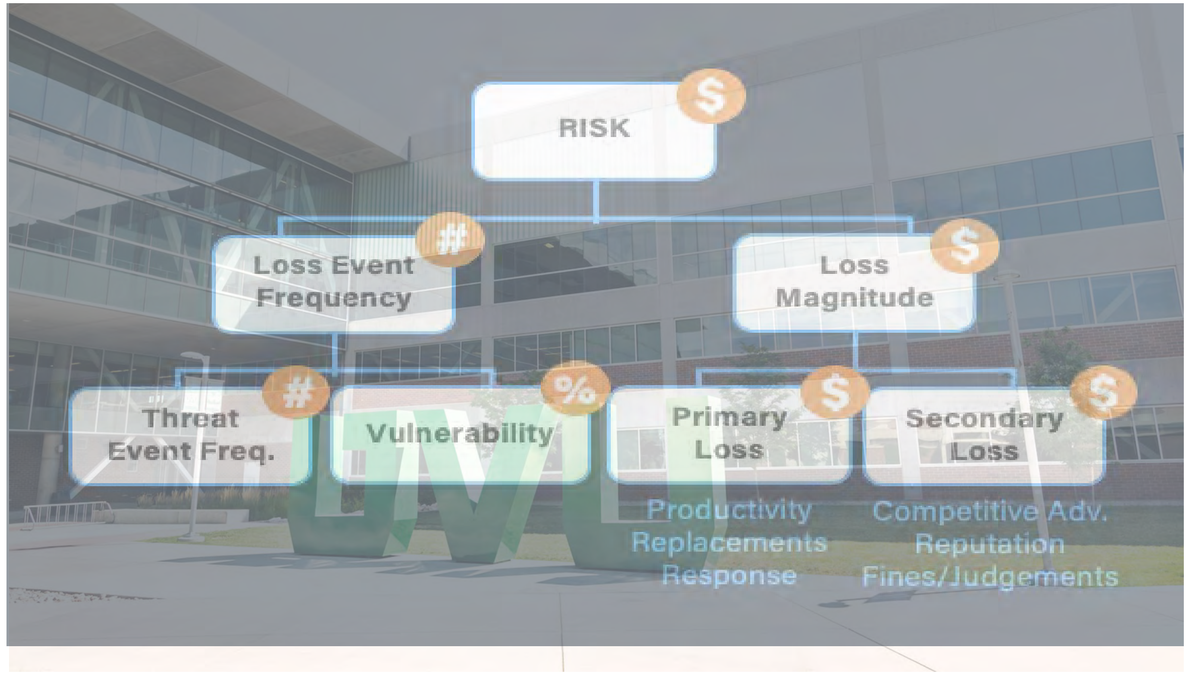
Data Collection



Data Source	Data Summary	Loss Factor
Regulatory Compliance	In the event of a data breach, Furniture Essentials would be required to notify all impacted customers in writing. On average, each notification costs $5.	Secondary Response
	A data breach impacting customer credit cards information is estimated to cost between $100,000 and $500,000 in fines.	Fines/Judgements
	In the event of a data breach impacting customer credit card records, the company would provide free credit monitoring to impacted customers. The average credit monitoring cost is $20 per customer. It is estimated that 10% of the impacted customers would sign up for the credit monitoring service.	Secondary Response

RISK ANALYSIS

Primary Response Costs

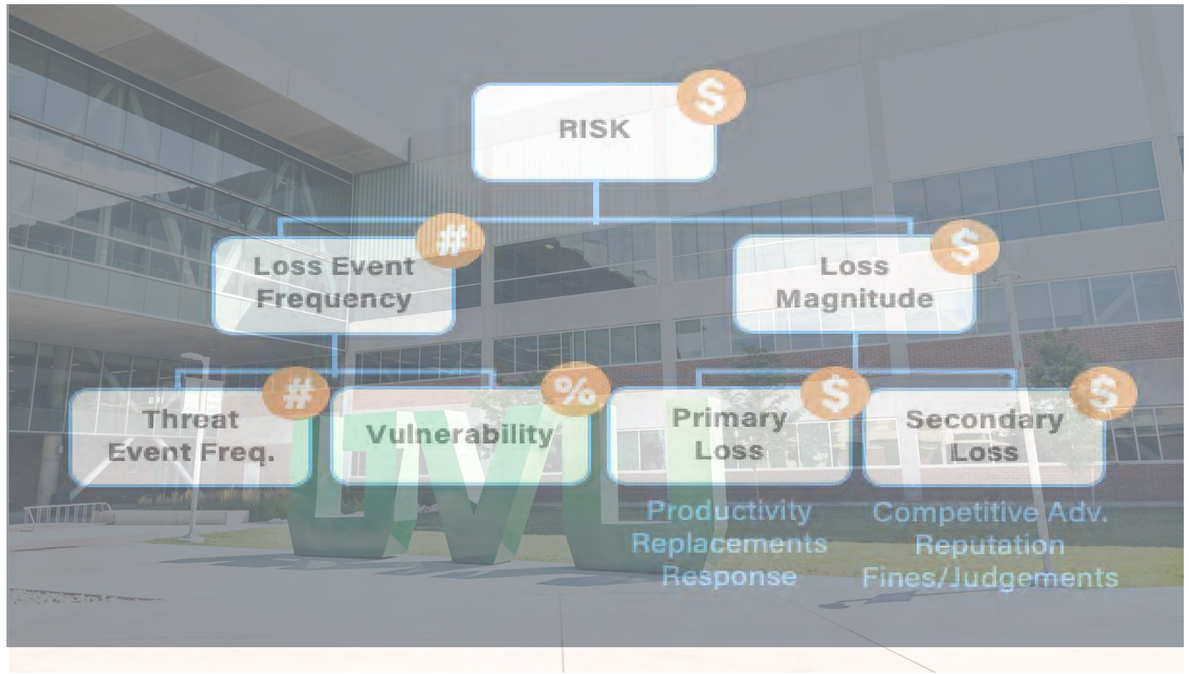


Internal Response	Number of Employees	Number of Hours	Average Hourly Rate	Primary Response
Min	4	10	$100	$4,000
ML	6	20		$12,000
Max	8	30		$24,000

	Minimum	Most Likely	Maximum
External Response	$150,000	$225,000	$300,000

RISK ANALYSIS

Total Primary Loss



Primary Loss	Minimum	Most Likely	Maximum
Internal Response	$4,000	$12,000	$24,000
External Response	$150,000	$225,000	$300,000
Total Primary Loss	$154,000	$237,000	$324,000

RISK ANALYSIS

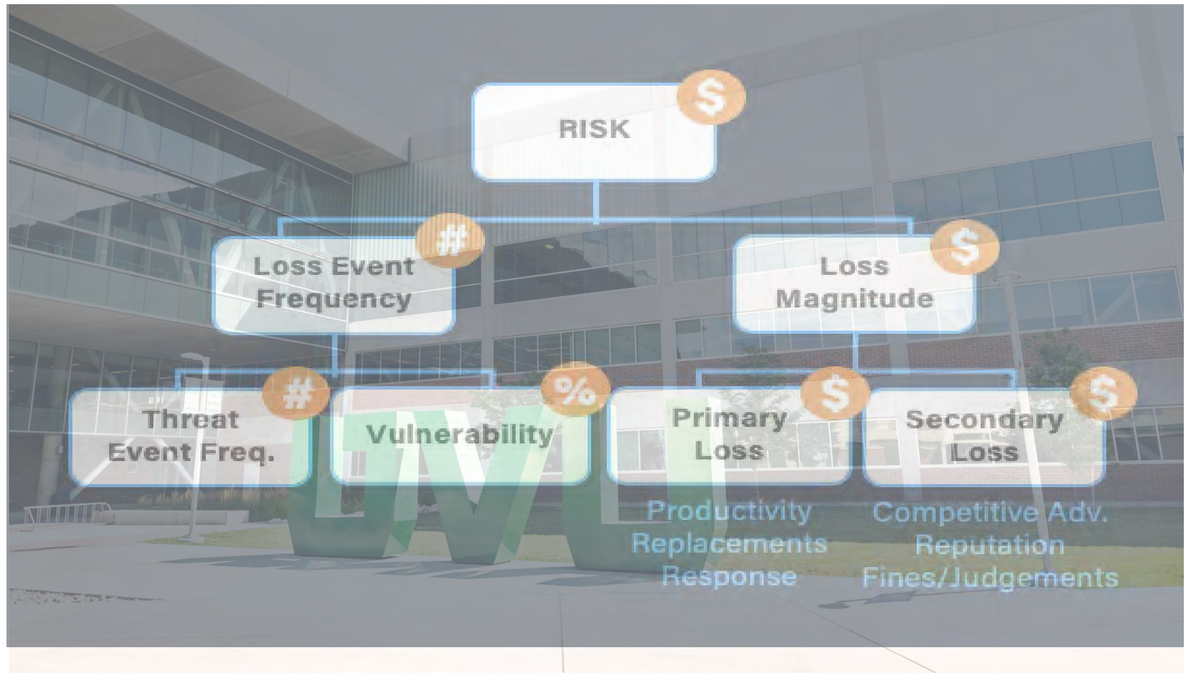
Secondary Response Cost

	% Credit Monitoring	# of Customers	Monitoring Cost/Customer	Monitoring Response Cost
Min	5%	25,000	$20	$275,000
ML	10%			$300,000
Max	15%			$325,000

	Impacted Customers	Cost per Customer	Notification Response Cost
Notification	50,000	5$	$250,000

RISK ANALYSIS

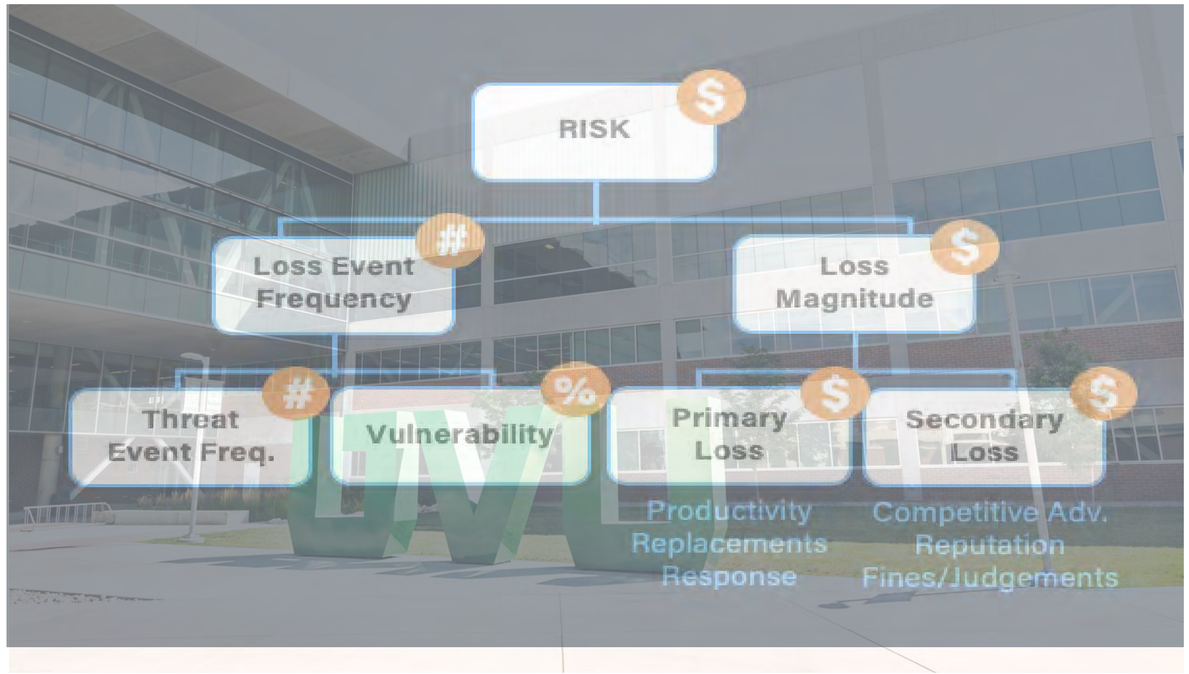
Secondary Fines & Judgments Costs



	Minimum	Most Likely	Maximum
Fines & Judgements	$100,000	$300,000	$500,000

RISK ANALYSIS

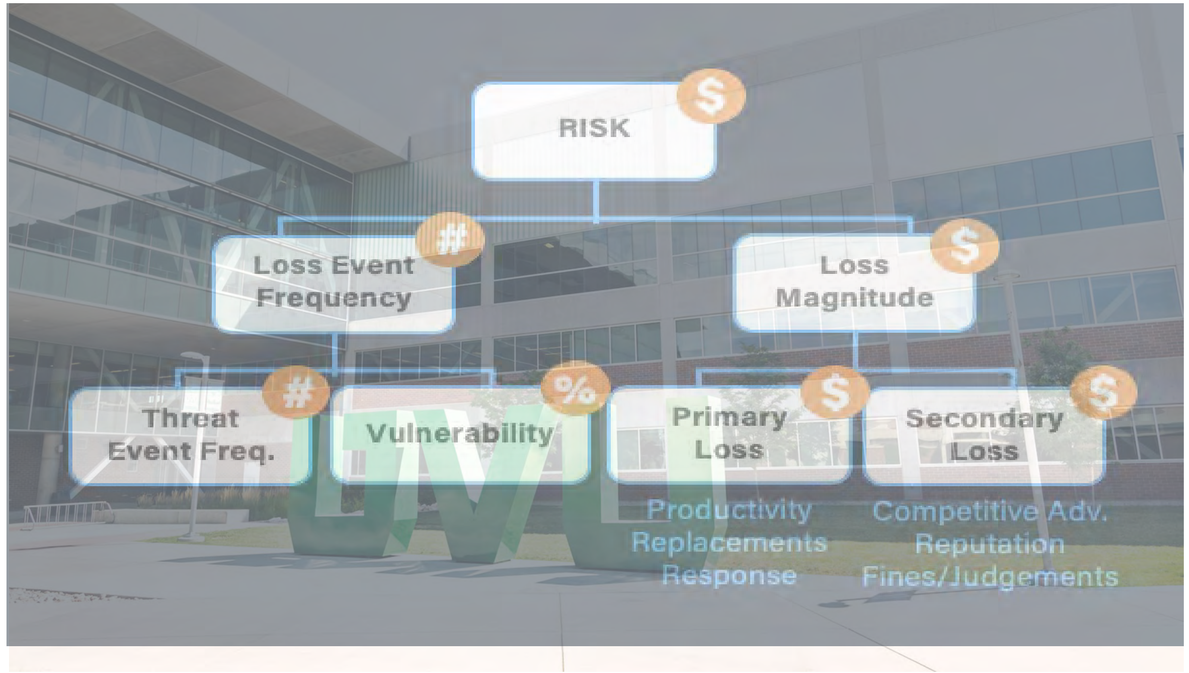
Secondary Reputation Costs



	Market Share Loss	Customer Base	Customer Value	Secondary Reputation
Min	5%	50,000	$300	$750,000
ML	10%			$$1,500,000
Max	15%			$2,250,000

RISK ANALYSIS

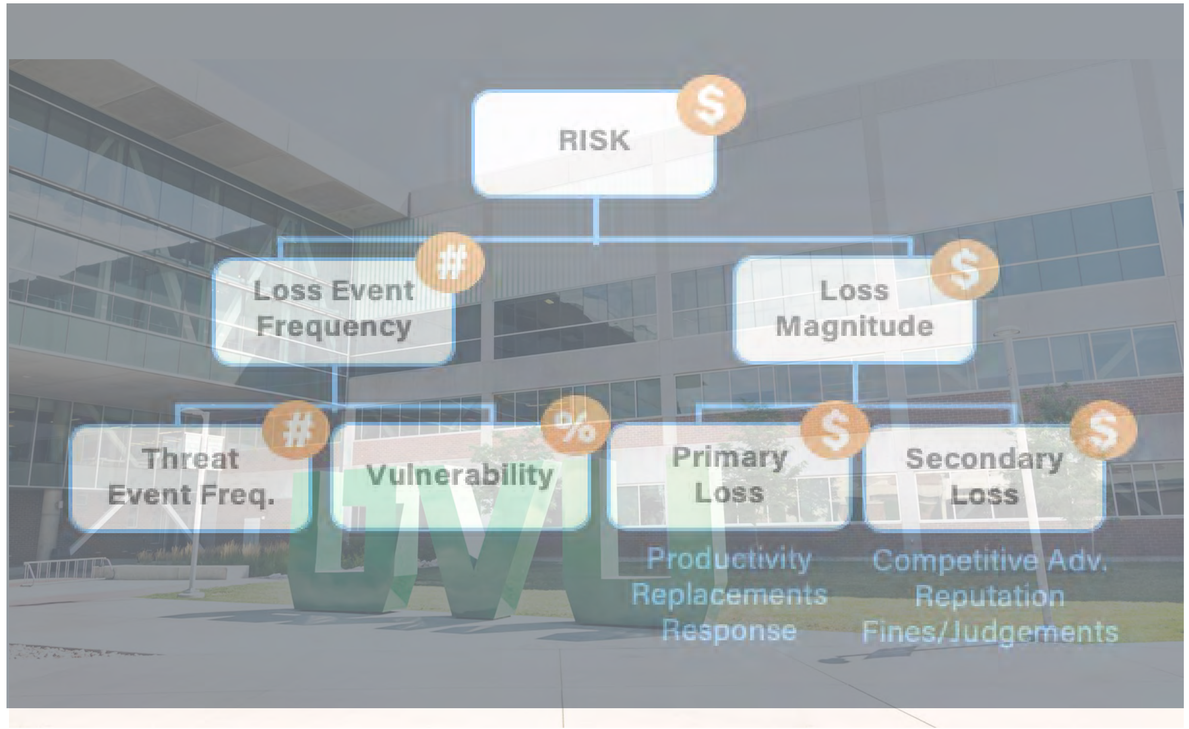
Total Secondary Costs



Secondary Cost	Minimum	Most Likely	Maximum
Response	$275,000	$300,000	$325,000
Fines/Judgements	$100,000	$300,000	$500,000
Reputation	$75,000	$750,000	$1,500,000
Total Secondary	$1,125,000	$2,100,000	$3,075,000

RISK ANALYSIS

Risk Exposure

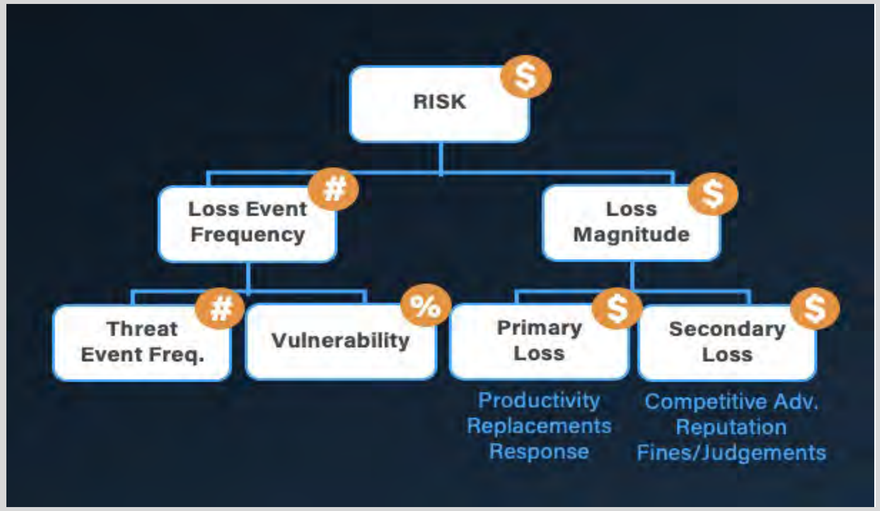


Loss Factor	Minimum	Most Likely	Maximum
Primary Loss	$154,000	$237,000	$324,000
Secondary Loss	$1,125,000	$2,100,000	$3,075,000
Total Loss	**$1,279,000**	**$2,337,000**	**$3,399,000**

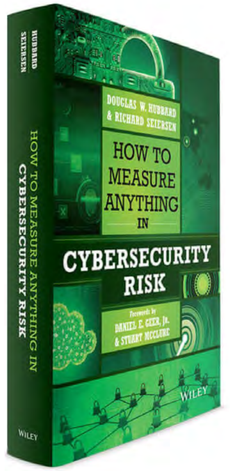
Risk Exposure

Scenario	Probability	Impact	Risk
Phishing	11%	$2,179,111*	$239,702
DDoS	25%	$976,712	$244,178

The lower/upper range of the total loss was turned into a lognormal distribution which was used with the inverse lognormal probability function to return a lognormally distributed impact value for the 11% probability. The value was then turned into a normally distributed impact value. Hence, the $2,179,111.



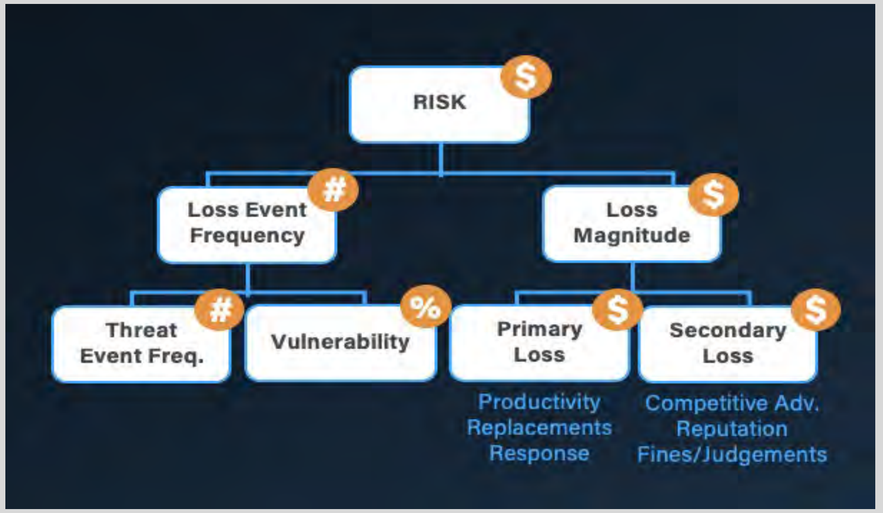
Hubbard Decision Research



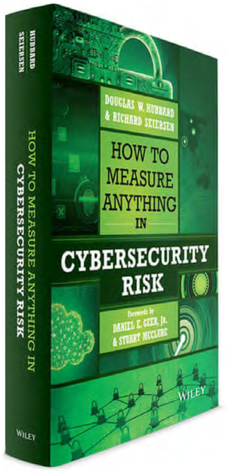
Return on Investment (Control)

Scenario	Probability	Impact	Risk
Phishing	11%	$2,179,111*	$239,702
DDoS	25%	$976,712	$244,178

Control	Cost	Effectiveness	ROI
Spam Filter	$50,000	95%	355%
DDoS Solution	$75,000	90%	193%



Hubbard Decision Research



Thank You!

Questions