BEST PAPER AWARD

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

Basil Hamdan
Department of Information Systems & Technology
Utah Valley University
Orem, USA
basil.hamdan@uvu.edu
0000-0003-0702-4200

***Abstract*—This paper; a scenario-based teaching case study, aims to introduce students in a Cybersecurity Risk Management course to advanced quantitative risk assessment techniques. The case study utilizes a fictitious company for which a risk assessment is underway. Assuming the role of the Cybersecurity Risk Team of the company, students are tasked with determining the risk exposure the company faces from a threat scenario against one of its mission-critical information resources. Specifically, the students are required to (1) quantify the monetary losses that could result from a threat scenario, (2) compute the inherited risk exposure from the threat scenario, (3) compute the residual risk given the implantation of certain security controls, and (4) compute the rate of return on the security controls. The case study holds the promise of enhancing the overall learning of the students and boosting their marketability as future cybersecurity professionals.**

Keywords—Cybersecurity Risk, Risk Assessment, Risk Analysis, Likelihood, Impact

I. INTRODUCTION

Cybersecurity risk is “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]. Here, risk is assessed at the intersection of the likelihood and the impact. Mathematically, risk is computed by the following equation:

$$Risk = Likelihood * Impact$$

At face value, the risk equation is very simple but the real challenge lies in qualifying or quantifying the likelihood and the impact. NIST SP 800-30 describes three approaches for assessing risk. Table I provides short descriptions of each approach.

In academia, much of the focus has been on teaching qualitative and semi-quantitative approaches to risk assessment. This is largely due to the lack of pedagogical materials on measuring cybersecurity risk using quantitative techniques. This paper aims to fill this gap by introducing students in a Cybersecurity Risk Management course to an advanced quantitative risk assessment approach based on the techniques presented in “How To Measure Anything in Cybersecurity Risk” [2]. This goal will be achieved through a scenario-based teaching case study which utilizes a fictitious company and requires students to assume the role of a cybersecurity risk team to compute the risk exposure that the company faces from a threat scenario against one of its mission-critical information resources.

TABLE I. ASSESSMENT APPROACHES

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

II. CASE STUDY

A. Case Scenario

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.

To manage the information security risk to Furniture Essentials, the Cybersecurity Department, with the blessing and support of the top management team, instituted a formal Cybersecurity Risk Management Program. Consistent with industry standards, the program encompasses the supporting processes to manage information security risk to Furniture Essentials' organizational operation. This includes establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time.

The company's Cybersecurity Risk Team has just embarked on a new round of assessing its cybersecurity risk exposure. So far, the team completed two major activities; asset identification and threat assessment.

For **asset identification**, the Cybersecurity Risk Team, led by the Chief Information Security Officer (CISO) met with C-Level executives to identify the information assets that are most critical to the company's operations and whose protection from cyber-attacks should receive high priority.

Both the Chief Financial Officer (CFO) and the Chief Operations Officer (COO) were particularly worried about the eCommerce Website which customers use to order the products that Furniture Essentials sells. They were also concerned about the backend internal database that stores customer data and order data. Not surprisingly, these two assets ranked top two mission-critical assets in a subsequent asset scoping workshop that was attended by C-Level executives and department heads.

During the **threat assessment**, the Cybersecurity Risk Team identified several threat actors that could launch cyber attacks against Furniture Essentials. Given that Furniture Essentials has not been targeted by nation-state actors or advanced cybercriminals, the team elected to mainly focus on external malicious hackers. Subsequently, the team identified several threat actions that these hackers can potentially carry out against Furniture Essentials.

After careful analysis of the threat scenarios, the Cybersecurity Risk Team found DDoS to be the top attack vector by which malicious hackers could compromise the availability of the eCommerce Website. Additionally, they found 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 data in the internal database.

Having identified the top threat scenarios, the team is now ready to conduct a risk analysis in order to determine the probability of occurrence and the impact for each scenario. However, a key determination that the team must make is deciding on the assessment approach to use going forward.

Over the 10 years that Furniture Essentials has been in business and up until now, the Cybersecurity Risk Team used both qualitative and semi-quantitative approaches to determine the risk exposure. This time around, however, the CISO who was under continuous pressure from the CEO and CFO to justify the cybersecurity budget, asked the Cybersecurity Risk Team to adopt a quantitative methodology for risk assessment; one that would allow for computing the risk exposure in terms of dollar amounts. In fact, the CISO had just returned from a Cybersecurity Conference in San Francisco where he attended several presentations and seminars including a presentation titled: "How To Measure Anything in Cybersecurity Risk" and a seminar titled "The Future of Cybersecurity Risk Management" which introduced the attendees to Risk Quantification with FAIR[1] (short for Factor Analysis of Information Risk). The CISO instructed the team to perform the risk analysis utilizing both approaches, to the extent possible. To help the team get familiar with both approaches, the CISO shared the following resources:

- 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[2].
- 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].

After reviewing the materials that the CISO shared and studying up on both approaches, the team made a collective decision to use the forms of loss per the FAIR framework to quantity the loss magnitude and to use the computational approach advocated per the book titled "How To Measure Anything in Cybersecurity Risk" and the accompanying template to compute the risk exposure. Since the team had no previous experience working with quantitative assessment approaches, a decision was made to limit the analysis to the phishing threat scenario, for the time being.

[1] https://www.fairinstitute.org/fair-risk-management

[2] The template can be downloaded from the book's companion website.

B. Case Data

The Cybersecurity Risk Team had several communications (phone calls, meetings, emails, document requests, etc.) with various teams across the company. Table II presents the information that the team obtained. While the team obtained a wide range of information, the table presents a summary of the data deemed relevant to deriving the risk exposure from the phishing attack.

C. Suggested Guided Questions

Assuming the role of the Cybersecurity Risk Team at Furniture Essentials and considering the case scenario and the case data from Table II, compute the cybersecurity risk associated with the phishing threat scenario. Specifically,

1. Read "Chapter 3 An Introduction to Practical Quantitative Methods for Cybersecurity" from "How To Measure Anything in Cybersecurity Risk" [2]. List and describe the one-for-one substitutions per the model presented in the chapter.
2. Read the "Technical Standard for Risk Taxonomy" [4]. What are the six forms of loss that are adopted by the FAIR Framework and Which of these forms is applicable to the phishing threat scenario?
3. For each applicable form of loss, and considering the data in Table II, compute and/or estimate lower bound and upper bound values such that there is a 90% chance the actual impact will be between the bounds (i.e., at 90% confidence interval).
4. Produce a table summarizing the total lower bound and upper bound values of the primary forms of loss, the secondary forms of loss, and the overall loss (i.e., the primary and secondary forms of loss)
5. Considering a 90% confidence interval and the lower and upper bounds for the overall loss as per your computations, simulate the total loss value that corresponds to a likelihood of 11%; the estimated probability of a phishing attack occurring at least once a year per the case narrative.
6. Use the simulated total loss and the probability to compute the risk exposure (inherited risk) from the phishing attack scenario.
7. Given the following hypothetical about a DDoS attack against Furniture Essentials' eCommerce Website, which threat scenario would you chose to mitigate first, the phishing attack or the DDoS attack?
   - The DDoS attack would result in risk exposure of $244,178.
   - The annual cost of a DDoS mitigation solution is $75,000.
   - It is estimated that 2 in 20 DDoS attacks will overcome the protection offered by the DDoS mitigation solution.

TABLE II. CASE DATA

Source	Data Summary
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. 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.
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.
Sales Management	The company's eCommerce website generates approximately $60 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. Approximately, 50% of the customers store their credit card information on the company's website for faster check out. 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.
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. A data breach impacting customer credit cards information is estimated to cost between $100,000 and $500,000 in fines. 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.

D. *Suggested Answers*

In this section, we present suggested answers to some of the previous questions.

Drawing on the FAIR framework [4] and given the case narrative, only 3 forms of loss are applicable to the phishing threat scenario. Table III lists all forms of loss, their definitions, and applicability to the scenario at hand.

TABLE III. FORMS OF LOSS

Form	**Definition**	**Applicable**
Productivity	The reduction in an organization's ability to generate its primary value proposition (e.g., income, goods, services, etc.).	No
Response	Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, etc.).	Yes
Replacement	The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost / damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop).	No
Fines and Judgments	Legal or regulatory actions levied against an organization. This includes bail for any organization members who are arrested.	Yes
Competitive Advantage	Losses associated with diminished competitive advantage.	No
Reputation	Losses associated with an external perception that an organization's leadership is incompetent, criminal, or unethical.	Yes

Having identified the applicable forms of loss, we can turn to computing the primary loss, the secondary loss, and the total loss. Table IV, Table V, and Table VI present the results[3] of these computations.

TABLE IV. PRIMARY LOSS

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

TABLE V. SECONDARY LOSS

Loss Type	**Minimum**	**Most Likely**	**Maximum**
Secondary Response	$275,000	$300,000	$325,000
Fines and Judgements	$100,000	$300,000	$500,000
Secondary Reputation	$750,000	$1,150,000	$2,250,000
Total Secondary Loss	**$1,125,000**	**$2,100,000**	**$3,075,000**

TABLE VI. TOTAL LOSS

Loss Type	**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**

Based on data from the Incident Response Team, the likelihood of a data breach occurring at least once a year is 11%. Considering this likelihood and the lower and upper bounds for the total loss as per Table VI, we can now simulate the total loss value that corresponds to a likelihood of 11% with a 90% confidence interval. Table VII presents a summary of the risk computation[4] for the phishing scenario and a hypothetical DDoS scenario.

[3] For space limitation and to maintain the sanctity of the case, detailed computations were omitted. Please contact the author for a copy of the paper with detailed computations of the all the risk components.

[4] Per the template accompanying Chapter 3 from "How To Measure Anything in Cybersecurity Risk", the impact value that corresponds to a given probability can be computed using the inverse normal probability function. For example, for an 11% probability and a total loss value between $1,279,000 and $3,399,000, the impact value would be $500,359. However, the inverse normal probability function could have returned a negative impact value given a different probability. For example, for a 5% probability, the impact value would be -$126,745 (i.e., a negative loss which is not logical). To overcome this problem, the lower/upper range of the total loss must be turned into a lognormal distribution which then can be used with the inverse lognormal probability function to return a lognormally distributed impact value for a given probability. The value can then be turned into a normally distributed impact value. Hence, the $2,179,111.

TABLE VII. RISK EXPOSURE

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

Based on the risk analysis, a data breach of the internal database would result in a risk exposure of roughly $240,000. A DDoS attack against the eCommerce Website would result in risk exposure of roughly $244,000. Both the phishing and the DDoS threat scenarios result in virtually the same risk exposure. The decision as to which risk should be mitigated first depends on the effectiveness of the control (the percentage/amount of risk reduction), the cost of the control, and ultimately the rate of return on the control given its cost (i.e., Return on Investment or ROI for short). Table VIII presents the return on the Email spam filtering solution and the DDoS mitigation solution.

TABLE VIII. RATE OF RETURN ON SECURITY CONTROLS

Threat Scenario / Control	Risk
Phishing/Email spam filtering solution	335%
DDoS/DDoS mitigation solution	193%

Based on the risk analysis and ROI, Furniture Essentials should first mitigate the risk from the phishing attack scenario and then, if resources are available, the risk from the DDoS attack scenario.

E. Future Decisions

Going forward, Furniture Essentials should consider using methods like Monte Carlo simulations where the risk exposure for each threat scenario is computed based on hundreds or thousands of trials. Further, Furniture Essentials should consider constructing a Loss Exceedance Curve to compare the probability of exceeding a given loss in one year due to cybersecurity risk against predetermined risk tolerance levels. Given these levels, the company may accept the risk, implement countermeasures to reduce the exposure to an acceptable limit, or transfer the risk by purchasing a cyber insurance.

III. CONCLUSION

The main objective of this paper, a teaching case study, is to introduce students in cybersecurity risk management to advanced quantitative risk assessment approaches. To this end, the FAIR framework was used to quantity the loss magnitude whereas the computational techniques per the book titled “How To Measure Anything in Cybersecurity Risk” were used to compute the risk exposure. The teaching case study presented in this paper is yet to be utilized but the authors hope to introduce it in a Cybersecurity Risk Management course the next time the course is taught. The paper holds the promise of filling the current gap in pedagogical materials on measuring cybersecurity risk using quantitative techniques. It also holds the promise of enhancing the overall learning of the students and increasing their marketability as future cybersecurity professionals.

REFERENCES

[1] National Institute of Standards and Technology, “NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments,” Retrieved June 18, 2022 from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[2] D. Hubbard, R. Seiersen, How to Measure Anything in Cybersecurity Risk (1st edition), Wiley, 2016.

[3] D. Hubbard, R. Seiersen, “How To Measure Anything In Cybersecurity Risk,” In Proceedings of the RSA Conference 2016, San Francisco, CA.

[4] The Open GROUP, “Technical Standard Risk Taxonomy,” Retrieved June 18, 2022 from https://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.

[5] J. Jones. “Introduction to Risk Quantification with FAIR,” In Proceedings of the RSA Conference 2022, San Francisco, CA.