Winter 12-10-2023

Optimization of Investments in Cybersecurity: A Linear Programming Approach

Swati Jain
Indian Institute of Management Lucknow

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow

Optimization of Investments in Cybersecurity: A Linear Programming Approach

Research-in-progress

Swati Jain
Indian Institute of Management Lucknow
phd21020@iiml.ac.in

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow
arunabha@iiml.ac.in

ABSTRACT

Cyber-attacks have globally escalated by 125% after the onset of the pandemic as businesses transitioned to online work setups. These cybercrimes incur significant costs. Consequently, organizations are giving heightened priority to cybersecurity investments, integrating them into their strategic decision-making. However, due to limited resources, a judicious approach is necessary, focusing on selective investment in effective mitigation strategies. This study addresses the challenge of optimally allocating investments among diverse cybersecurity measures to enhance cybersecurity efficacy while minimizing the risk of cyberattacks. Specifically, the study aims to anticipate potential losses based on breach likelihood and determine the optimal investment levels. The study employs a combination of machine learning (ML) and linear programming (LP) to determine suitable mitigation strategies for investment, considering constrained monetary resources. ML techniques, including Naïve Bayes and Decision Tree, assess breach likelihood and consequent losses. Subsequently, LP is employed to ascertain the most effective allocation of investments across different cybersecurity mitigation strategies, considering the constraints of monetary resources.

Keywords: Cybersecurity Investment, Optimization, Cyber-Risk Mitigation, Machine Learning, Linear Programming.

INTRODUCTION

The Global Risk Report (2023) has ranked cyber-attacks as the eighth most significant risk for 2022-23, projecting potential severity over the next 2 to 10 years. This prevalence has become customary across both public and private sectors. Critical sectors have increasingly become prime targets for cyber attackers (The Newyork Times 2022). The Covid-19 pandemic prompted a substantial surge in online operations across nearly all sectors, such as healthcare, finance, manufacturing, transportation, and education (McKinsey & Company 2020). As a consequence, 81% of organizations reported an uptick in cyber risks (Businesswire 2023). These cyber-attacks result in extensive losses, including financial setbacks damage to reputation and trust, reduced profits, increased customer attrition, and decreased employee productivity (Jain et al. 2023). Consequently, managers have begun prioritizing the organization's cybersecurity investments and making them a part of business strategic decision. These investments aim to fortify digital assets, preserve sensitive data, maintain customer trust, and ensure operational continuity (Angst et al. 2017). There are multiple options available to invest in, such as perimeter security, employee training, business continuity and disaster recovery planning, backups, vulnerability assessment and remediation, among others (Madnick 2021). However, time, money, and resources constraints permit firms to selectively invest in mitigation strategies (Gordon et al. 2003; Yoo et al. 2020). Therefore, managers' main challenge is ascertaining which mitigation strategies the organization should invest in and to what extent. Our study addresses this dilemma by looking for the optimal allocation of investments in different cybersecurity measures that will maximize cybersecurity effectiveness and minimize cyberattack risk. Accordingly, the research questions we aim to address are:

RQ1) What potential losses can an organization anticipate based on its likelihood of breach?

RQ2) Based on expected losses, what is the optimal investment level in different mitigation strategies?

This study applies a combination of machine learning (ML) and linear programming (LP). ML techniques such as Naïve Bayes and Decision Tree are used to determine the likelihood of a breach and the consequent losses. While the LP is used to decide the best possible division of the invested amount in different mitigation strategies.

LITERATURE REVIEW

While investigating different factors responsible for determining the risk of a cyberattack, we found that the vulnerabilities in the software, hardware, or network of an organization are a major threat (NIST 2014). However, the level of resiliency of the Information Technology (IT) infrastructure against these vulnerabilities, decides the degree of exposure of any firm to a cyberattack. For instance, an organization with threat intelligence incorporated is less likely to face a cyberattack (Zimba et al. 2018). Exploring further, we have found that the organization's structure – its size, whether it belongs to the critical sector, and the level of digital intensity it possesses - plays a crucial role in determining its exposure to cyberattacks (Fitzgerald 2018). Moreover, implementing the cybersecurity controls as per the COBIT19 and ITIL framework would further reduce the firm's exposure to cyberattacks (COBIT 2007; Meijer et al. 2013). While mitigating the organization's cybersecurity risk, the five-function framework of NIST guides us multiple strategies to do so (NIST 2018). However, deciding the best possible allocation of monetary resources in different mitigation strategies is challenging. To address this, we found that Linear Programming, introduced by George Dantzig in 1947, is precisely crafted

to handle the intricacies of optimization dilemmas (N. P. and I.A. 2016). Within this framework, objectives and the governing constraints, particularly monetary, can be articulated as linear functions (Olakunle Oluwaseyi et al. 2020). It significantly aids in decision-making processes and judiciously apportions the scarce resources.

RESEARCH FRAMEWORK

Our proposed model consists of three modules: Cyber Risk Assessment (CRA), Cyber Risk Quantification (CRQ), and Cyber Risk Mitigation using Optimized Allocation of Investments (CRM-OAI). The model is based on the Protection Motivation Theory (PMT) that consists of threat appraisal (TA) and coping appraisal (CA) (Rogers, 1975; Boss et al., 2015). Based on the threat appraisal and the NIST guidelines, CISOs are required to assess the risk and severity of a cyberattack in their organization (NIST 2014). Similarly, we propose the CRM-OI module based on the coping appraisal and Rational Choice Theory. We assume that a CISO is a rational actor who will minimize the probability and impact of cyberattacks in her organization by investing in perimeter security technologies (such as firewalls, Intrusion Detection Systems, Anti-virus, etc.) and training, cyber-risk insurance products (Mukhopadhyay et al. 2013), among others (Becker 1990; Boss et al. 2015; McCarthy 2002). However, considering the conservation of resources theory (Hobfoll et al. 2000), we understand that the CISO will try to maximize cybersecurity efficiency and minimize the opportunity costs in the form of cybersecurity investments (Hobfoll et al. 2000). Figure 1 illustrates our proposed model.

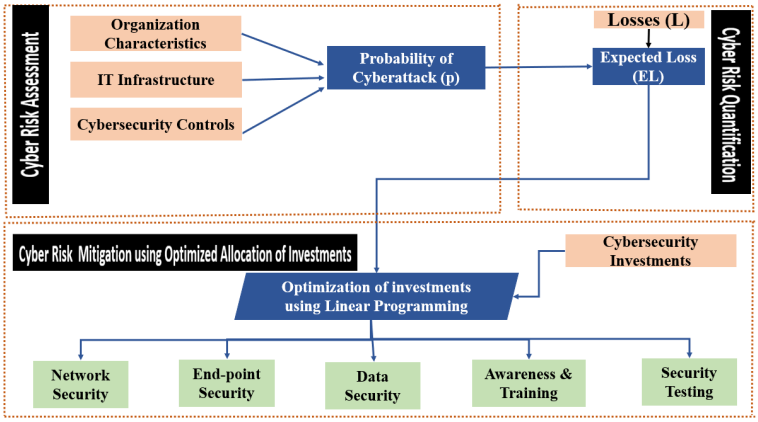

Figure 1. Proposed Model for Optimal Allocation of Investments in Various Cybersecurity Measures

Cybersecurity Risk Assessment (CRA)

According to Threat Intelligence (TI) (Peters 2017) and Cyber-kill chain (CKC) (Lockheed Martin 2011), our CRA module determines the risk of occurrence (p) of the cyberattacks based on the following inputs: the organizational characteristics (Peters 2017), IT Infrastructure (Dargahi et al. 2019; Muckin and Fitch 2019), and cybersecurity controls (FIRST 2019). We assume that an external hacker or an internal disgruntled employee (FIRST 2019) initiates a cyberattack on a significantly large digital platform. The hacker exploits the vulnerability by resorting to attack vectors, such as social engineering, to carry out a Confidentiality-Integrity-Availability breach (FIRST 2019). Using the concepts of TI and CKC, the CISO of an organization needs to identify vulnerable IT assets (NIST 2022) (FIRST 2019) to deter such attacks. However, if implemented, the cybersecurity governance framework and cyber-security controls will bring down the risk of cyberattack (Bodeau et al. 2010; Bowen and Wilson 2006; Fitzgerald 2018).

Cybersecurity Risk Quantification (CRQ)

Next, we quantify the cyberattack risk for organizations to estimate their losses due to cyberattacks. The risk probability (p) computed in the CRA module is used to calculate the severity of the attack in terms of the estimated losses (EL).

Cybersecurity Risk Mitigation using Optimized Allocation of Investments (CRM-OAI)

Lastly, based on the expected losses, we find the optimal allocation of monetary investments in different mitigation strategies. Our model leverages the National Institute of Standards and Technology (NIST) guided cybersecurity mitigation strategies (NIST 2018).

DATA AND METHOD

For this study, we have used the University of Queensland dataset of 1145 organizations to explore their cyber resilience (Tsen et al. 2020). We refer to Statista for the data on average financial losses (Statista 2022).

Cybersecurity Risk Assessment (CRA)

We consider two classifiers, M1 (Naïve Bayes (NB)) and M2 (Decision Tree (DT) to estimate the probability (p) of a cyberattack, as shown in equation 1a and 1b, respectively.

M1 (NB) $p = P(C=R, NR \mid X= CI, size, DI, NS, AV, PR, AC, UI, SC, CIA, CSR)$ 1(a)
Where, $P(C|X) = [P(X|C) * P(C)] / P(X)$

M2 (DT) $(Generate\_decision\_rules, p) = f(C=R, NR \mid X= CI, size, DI, NS, AV, PR, AC, UI, SC, CIA, CSR$ 1(b)

The model's performance is measured by computing Accuracy, F-score, Precision and Recall. We assessed the risk and obtained the posterior probabilities (p) of a cyberattack.

Cybersecurity Risk Quantification (CRQ)

Next, we calculate the severity by computing the expected losses (ELi). The mathematical representation of the expected financial loss (ELi) is illustrated in equation (2).

$$EL_i = q_i * L_j \quad (2)$$

Where qi = misclassification rate = 1 - pi; pi = posterior probabilities; Lj = losses in each year from 2004 to 2022; ELi = estimated loss for each organization; i = organization in the dataset.

Cybersecurity Risk Mitigation using Optimized Allocation of Investments (CRM-OAI)

Lastly, we use the Linear Programming using Solver to compute the optimal distribution of invested amount in different cyber-security strategies.

RESULTS AND DISCUSSION

In CRA module, the performance of the M1 and M2 classifiers is measured and compared in terms of accuracy, precision, recall, and F1-Score, as shown in Table 1.

Table 1. Performance metrics of M1 (NB) and M2 (DT) for classifying a cyberattack

Model	ML-Algorithms	Accuracy(p)	Misclassification rate (q=1-p)	Precision	Recall	F1 score
M1	NB	0.94	0.06	0.63	0.79	0.63
M2	DT	0.93	0.07	0.64	0.50	0.64

ML: Machine Learning; NB: Naïve Bayes; DT: Decision Tree

We consider M1 better than M2 since the accuracy of M1 is more than that of M2. Next, in CRQ, we input the risk (q_i= 1-p_i) obtained using NB and computed the expected losses (EL_i). Lastly, based on expected losses and investments of the firm, we computed the optimal division of the invested amount in different mitigation solutions, as shown in Table 2 and Figure 2.

Table 2. Optimal Allocation of Investment in Cybersecurity Measures

Total Investment (in Million US$)	Expected Loss (in Million US$)	Optimal Allocation of Investment in				
		Network Security	End-point Security	Data Security	Awareness & Training	Security Testing
3	7.5	1.50	1.50	1.50	1.50	1.50
38	55	11.00	11.00	11.00	11.00	11.00
96	120	24.00	24.00	24.00	24.00	24.00
204	260	18.57	18.57	18.57	92.86	111.43
230	295	18.44	18.44	18.44	129.06	110.63
248	320	18.82	18.82	18.82	150.59	112.94
278	375	20.83	62.50	20.83	145.83	125.00
296	385	40.53	40.53	20.26	162.11	121.58
306	445	44.50	89.00	22.25	155.75	133.50
320	440	44.00	66.00	22.00	176.00	132.00
326	455	41.36	103.41	20.68	165.45	124.09
335	490	44.55	111.36	22.27	178.18	133.64
344	490	44.55	111.36	22.27	178.18	133.64
347	497.5	45.23	113.07	22.61	180.91	135.68
350	505.5	45.95	114.89	22.98	183.82	137.86

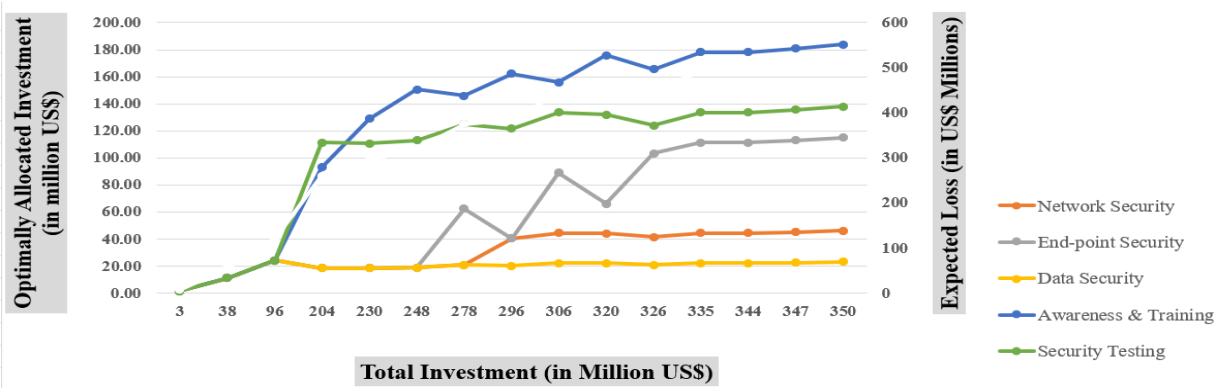

Figure 2. Optimal Allocation of Cybersecurity Investment in Mitigation Strategies

As evident from Table 2 and Figure 2, the highest portion of cybersecurity investments is directed towards the awareness and training of employees. This aligns with existing literature, which emphasizes that employees could be the weak links in an organization's security (McIntosh et al. 2022). Therefore, employees should be trained to identify phishing emails and to refrain from clicking on unknown links. They can be made aware and vigilant by frequent dry runs of incident response procedures to combat cyber-attacks (Samonas et al. 2020). The next substantial allocation of investment should be towards the regular monitoring and testing of cybersecurity within the organization. This approach is consistent with literature that advocates for regular vulnerability assessments through vulnerability scans or penetration testing (Jain and Mukhopadhyay 2023). These assessments analyze vulnerabilities inside the IT assets and network, allowing for timely mitigation. The third highest proportion of investment should be channelled towards endpoint or perimeter security. Literature also advises fortifying digital perimeters using firewalls and antivirus to deter cyber attackers (NIST 2018). The fourth highest investment priority should be to ensure network security by employing intrusion detection/prevention systems. Lastly, securing data, through reliable backups and robust data encryption is a paramount concern (NIST 2014).

CONCLUSION

In this study, we have explored the way to optimally allocate the cyber security investments in different mitigation strategies - network security, end-point security, data security, awareness & training, and security testing. This optimization was done based on the expected losses computed for organizations depending on their exposure to cyber-attack risk. The highest proportion is allocated to educate the employees and create awareness of cyber security attack risks.

REFERENCES

Angst, C. M., Block, E. S., D'Arcy, J., and Kelley, K. 2017. "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* (41:3), pp. 893–916. (https://doi.org/10.25300/MISQ/2017/41.3.10).

Becker, G. 1990. *The Economic Approach to Human Behavior*, University of Chicago Press.

Bodeau, D., Boyle, S., and Fabius-greene, J. 2010. "Cyber Security Governance A Component of MITRE ' s Cyber Prep Methodology."

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864. (https://doi.org/10.25300/MISQ/2015/39.4.5).

Bowen, P., and Wilson, M. 2006. "Information Security Handbook : A Guide for Managers." (http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf).

Businesswire. 2023. "Cyber Threats Have Increased 81% Since Global Pandemic." (https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic).

COBIT. 2007. "Effective IT Governance at Your Fingertips." (https://www.isaca.org/resources/cobit).

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., and Benedetto, L. 2019. "A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features," *Journal of Computer Virology and Hacking Techniques* (15:4), pp. 277–305. (https://doi.org/10.1007/s11416-019-00338-7).

FIRST. 2019. *Common Vulnerability Scoring System Version 3.1 Specification Document*, pp. 1–24. (https://www.first.org/cvss/).

Fitzgerald, T. 2018. "CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers," *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers*, CRC Press. (https://doi.org/10.1201/9780429399015).

Global Risk Report. 2023. *The Global Risks Report 2023 - 18th Edition*, World Economic Forum. (https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf).

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2003. "Information Security Expenditures and Real Options: A Wait-and-See Approach," *Computer Security Journal* (19:2), Computer

Security Institute, pp. 1 – 7.

Hobfoll, S. E., Shirom, A., and Golembiewski, R. 2000. "Conservation of Resources Theory," *Handbook of Organizational Behavior*, Marcel Dekker New York, NY, pp. 57–80.

Jain, S., and Mukhopadhyay, A. 2023. "Vulnerability-Based Cyber-Risk Management : A Text-Mining Approach," in *AMCIS 2023 Proceedings*, p. 17. (https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/17).

Jain, Swati, Mukhopadhyay, A., and Jain, Saloni. 2023. "Can Cyber Risk of Health Care Firms Be Insured? A Multinomial Logistic Regression Model," *Journal of Organizational Computing and Electronic Commerce* (0:0), Taylor & Francis, pp. 1–29. (https://doi.org/10.1080/10919392.2023.2244386).

Lockheed Martin. 2011. "The Cyber Kill Chain." (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html).

Madnick, S. 2021. "The Rest of the Cybersecurity Story," *MIT Sloan Management Review*. (https://sloanreview.mit.edu/article/the-rest-of-the-cybersecurity-story/).

McCarthy, B. 2002. "New Economics of Sociological Criminology," *Annual Review of Sociology*, JSTOR, pp. 417–442.

McIntosh, T., Kayes, A. S. M., Chen, Y.-P. P., Ng, A., and Watters, P. 2022. "Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions," *ACM Computing Surveys* (54:9), pp. 1–36. (https://doi.org/10.1145/3479393).

McKinsey & Company. 2020. "COVID-19 Digital Transformation & Technology." (https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever, accessed September 30, 2022).

Meijer, M., Smalley, M., Taylor, S., and Dunwoodie, C. 2013. "ITIL® and BiSL®: Sound Guidance for Business-IT Alignment from a Business Perspective," *The Stationary Office AXELOS Whitepaper*, pp. 1–8.

Muckin, M., and Fitch, S. C. 2019. "A Threat-Driven Approach to Cyber Security," *Lockheed Martin Corporation*, pp. 1–45.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. 2013. "Cyber-Risk Decision Models: To Insure IT or Not?," *Decision Support Systems* (56:1), Elsevier B.V., pp. 11–26. (https://doi.org/10.1016/j.dss.2013.04.004).

N. P., A., and I.A., I. 2016. "Application of Linear Programming for Optimal Use of Raw Materials in Bakery," *International Journal of Mathematics and Statistics Invention (IJMSI)* (4:8), pp. 51–57.

NIST. 2014. "Framework for Improving Critical Infrastructure Cybersecurity," , February. (https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf).

NIST. 2018. "The Five Functions," *NIST*, Gaithersburg, MD, April 16. (https://doi.org/10.6028/NIST.CSWP.04162018).

NIST. 2022. "Getting Started with Cybersecurity Risk Management: Ransomware."

Olakunle Oluwaseyi, K., Elizabeth, A., and Ezekiel Olaoluwa, O. 2020. "Profit Maximization in a Product Mix Bakery Using Linear Programming Technique," *Journal of Investment and Management* (9:1), p. 27. (https://doi.org/10.11648/j.jim.20200901.14).

Peters, J. 2017. "How to Organize and Classify Different Aspects of Cyber Threat Intelligence," *SurfWatch Labs Inc*. (https://blog.surfwatchlabs.com/2017/10/02/how-a-mind-map-can-

help-organizations-better-understand-threat-intelligence/).

Samonas, S., Dhillon, G., and Almusharraf, A. 2020. "Stakeholder Perceptions of Information Security Policy: Analyzing Personal Constructs," *International Journal of Information Management* (50), pp. 144–154. (https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.04.011).

Statista. 2022. "Amount of Monetary Damage Caused by Reported Cyber Crime to the IC3 from 2001 to 2021 (in Million U.S. Dollars)," *Statista 2022*. (https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/).

The Newyork Times. 2022. "Estonia Says It Repelled a Major Cyberattack Claimed by Russian Hackers." (https://www.nytimes.com/2022/08/18/world/europe/estonia-cyber-attack-russia.html).

Tsen, E., Ko, R. K. L., and Slapnicar, S. 2020. *Dataset of Data Breaches and Ransomware Attacks over 15 Years from 2004*, University of Queensland.

Yoo, C., Goo, J., and Rao, R. 2020. "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness," *MIS Quarterly* (44), pp. 907–931. (https://doi.org/10.25300/MISQ/2020/15477).

Zimba, A., Wang, Z., and Chen, H. 2018. "Multi-Stage Crypto Ransomware Attacks: A New Emerging Cyber Threat to Critical Infrastructure and Industrial Control Systems," *ICT Express* (4:1), Korean Institute of Communication Sciences, pp. 14 – 18. (https://doi.org/10.1016/j.icte.2017.12.007).