An Interdisciplinary Study of Cybersecurity Investment in the Nonprofit Sector

Natalia Ermicioi
Marymount University

Xiang Michelle Liu
Marymount University

Cybersecurity is becoming a worldwide priority. It is critical for organizations to quantify losses from cybercrimes and make informed decisions on cybersecurity investments. This paper expands the body of knowledge in cybersecurity of nonprofit organizations (NPOs)—a less-researched area—by examining investment in NPOs' cybersecurity from the business and economics perspectives. The authors combine two economics and risk management models to quantify the potential loss caused by a cyberattack. The paper provides a hypothetical example of applying the insights from the GL and FAIR risk models to assess the information assets of an NPO and calculating the optimal level of cybersecurity investment. Developing cybersecurity measures for NPOs is equally important as developing cybersecurity strategies, tools, and policies for large corporations or small businesses. Therefore, the findings of this paper can serve as decision-making tools for NPOs to evaluate information security assets, estimate the potential loss caused by cyberattacks, and determine the optimal investment value in cybersecurity measures.

Keywords: cybersecurity, nonprofit, risk management, investment

BACKGROUND

One of the latest McAfee reports revealed that the annual monetary loss from cybercrime would create a $1 trillion drag on the global economy in 2020 (Malekos & Lostri, 2020). As ransomware and phishing campaigns are skyrocketing (Verizon, 2021), the cost of global cybercrime is expected to continue increasing and to reach $10.5 trillion annually by 2025 (Morgan, 2020). To achieve such a level of growth, cybercrime has been organized like a business, spread and delivered through supply chains, services, and distribution channels. As cyber threats have evolved from targeting and harming computers, networks, and smartphones to affecting people, cars, gas pipelines, and medical devices, businesses of all sizes and in all sectors including healthcare organizations, schools, and local governments, could be cybercriminal group targets. The recent President Executive Order (EO) on "Improving the Nation's Cybersecurity" reflects the national security implications of cybersecurity attacks on everyday life (Executive Office of the President, 2021). Therefore, it is critical for organizations to understand the factors involved in quantifying losses from cybercrime as well as costs of cybersecurity investment in order to make informed decisions on cybersecurity spending and reduce risks from cyberattacks (AT&T, 2017; Gordon et al., 2015).

The EO further signals the pressing need for companies of all sizes, industries, and locations to conduct due diligence to mitigate the risk of cyberattacks as they arise (Boggs, 2021). However, due to the limited financial resources and skillsets, sufficiency of cybersecurity spending and effectiveness of security policy are usually afterthoughts in small businesses and nonprofit organizations (NPOs). Unfortunately, more than half of all cyberattacks are committed against small-to-mid-sized businesses (SMB), and 60 percent of them go out of business within six months of falling victim to a data breach or hack (Johnson, 2019). Like for-profit businesses, the bulk of NPOs are small; small NPOs employ about half of all nonprofit workers (Headd, 2019). When taking a closer look at NPOs, their cybersecurity readiness raises an even more alarming sign. NPOs are frequently "understaffed," engage volunteers instead of paid professional staff, and lack talents and infrastructure for security best practices (Haight, 2015; Suykens, Verschuere, & De Rynck, 2017). Ermicioi (2020) found that the number of employees and the size of the annual budget of a nonprofit organization significantly affect cybersecurity readiness, especially during disasters. The limited resources (such as budget and people) pose big challenges, making NPOs more vulnerable to cyber threats compared with their for-profit sector counterparts.

The subject of cybersecurity applied in large corporations has been widely explored due to the numerous data breaches that have implicated millions of people. However, much uncertainty remains in nonprofit counterparts due to underreported cybersecurity threats in NPOs compared with for-profit businesses. This study aims to address this gap by using a quantitative research method to examine cybersecurity risk and investment in NPOs.

CYBERSECURITY APPLIED TO NONPROFITS: ISSUES AND CHALLENGES

Contrary to common perceptions, nonprofit organizations, much the same as for-profit businesses, engage in a variety of activities involving data collection (National Council of Nonprofits, 2019), including:

- Conduct e-commerce on its websites, such as processing donations or event registrations;
- Store and transfer personally identifiable information such as donors' personal information, donors' financial information (credit card numbers, account information), clients' personal and medical information, and employee records including drivers' licenses, addresses, and social security numbers;
- Collect information on the preferences and habits of donors and patrons; and
- Collect newsletter subscribers' information, etc.

Moreover, the *Nonprofit Guidelines for Cybersecurity and Privacy* highlighted the fact that NPOs regularly assume significant financial and social responsibilities entrusted by governments (Microsoft Corporation, 2017). For example, the city of New York awarded contracts worth 404 million dollars to four NPOs of the top 15 contractors in 2016. Further, the same report emphasized the weaknesses that nonprofits are facing:

> In the past, cybersecurity and privacy were often low on the list of nonprofit priorities—but times are changing. The stakes for nonprofits are increasingly high. They often do not know how best to develop cybersecurity or data protection strategies that meet the evolving needs and challenges of today's online environment. (p. 1)

An example of cyberattacks targeting NPOs is Little Red Door, a small Indiana nonprofit that works with terminal cancer patients. The nonprofit experienced a Ransomware attack in January 2017, which is an example of the devastating impact that an attack could have on a nonprofit. Hackers accessed the nonprofit's server after "a staffer inadvertently downloaded malware from an email" (Ropeik, 2017).

Budget limitations are among the biggest challenges that NPOs face when considering investment in cybersecurity programs (Ermicioi, 2020; Nexia International, 2017). This stands in contrast to industries that exhibit greater technology adoption and maturity, such as banking and financial services and healthcare and life sciences, where time constraints are cited as the primary challenge to implementation of cybersecurity programs (Nexia International, 2017). Developing cybersecurity measures for NPOs is equally important as developing cybersecurity strategies, tools, and policies for large corporations or small businesses. However, limited field and industry research has been conducted to provide data, knowledge, and guidance for NPOs. The privacy and security of the data they collect have rarely been discussed and investigated in the specialized literature, which opens a range of research opportunities. Further, little discussion and attention has been paid to what the optimal amount of investment in cybersecurity for NPOs would be as well as how such a number can be obtained in a systematic, quantitative manner.

The authors utilized two quantitative models in this paper as vehicles to demonstrate a quantitative approach to help the management in NPOs make more informed and effective decisions in terms of cybersecurity investment. First, the Gordon–Loeb (GL) model (Gordon & Loeb, 2002) is a single-period economic model to analyze the optimal amount of investment in cybersecurity to protect the information assets of an organization. However, no previous study has investigated the applicability of the model on NPOs. This research intends to assess the extent to which the GL model applies to NPOs and whether the model fits their particularities. The study will also determine whether the 37% rule of the GL model is a valid option for NPOs and what the rationales are. To the best of our knowledge, this would be the first study to test the applicability of one of the well-accepted analytical models in the economics of information security investment literature to a less-researched field. Another model applied in this paper is the Factor Analysis of Information Risk (FAIR) model, which defines "the necessary building blocks for implementing effective cyber risk management program" (FAIR Institute, 2021). The FAIR model is the only international standard quantitative model for cybersecurity and operational risk. We selected this model based on the fact that it "specializes in financially derived results tailored for enterprise risk management" (FAIR Institute, 2021).

In summary, the purpose of this paper is to enlarge the limited body of knowledge of investment in the NPOs' security measures by combining two well-known quantitative models (GL and FAIR) and applying their principles to an under-researched sector—the nonprofits. The current paper does not seek to provide an optimal amount of investment. Instead, it focuses on evaluating the applicability of the two models that have been previously developed mainly for the private sector's particularities to the nonprofit sector, a less-researched field.

The rest of this paper is structured as follows. The next section provides a review of the GL model followed by an overview of the FAIR model. The rest of the paper proposes a hypothetical scenario and applies the principles of the above-mentioned models.

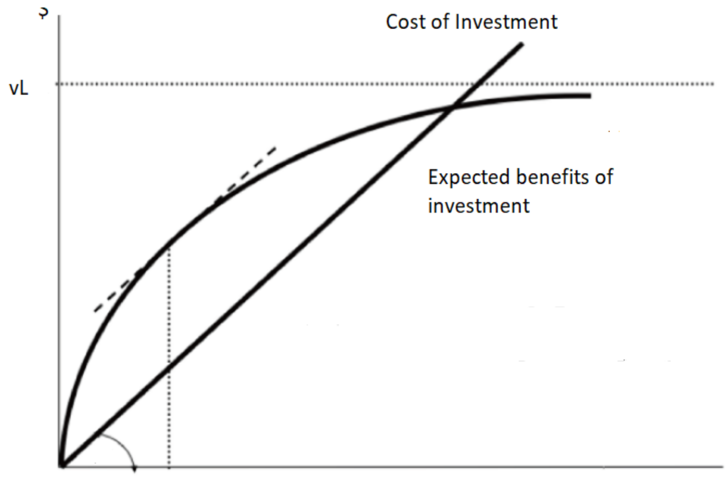
RESEARCH MODELS

This section provides a general overview of the two models used in this paper: the GL and FAIR models.

Overview of the Gordon–Loeb (GL) Model

The GL model has been widely referenced in the academic and industry literature (e.g., Gao & Zhong, 2015; Gordon & Loeb, 2011; Hausken, 2014; Palin, 2013; Pfleeger & Rue, 2008). The optimal level of cybersecurity investment is accurate at the investment level of z* (Gordon & Loeb, 2002). Gordon and Loeb, in their original paper (Gordon & Loeb, 2002), concluded that "for two broad classes of security breach probability functions, the optimal level would not exceed vL/e, or roughly 37% of the expected loss from a security breach, vL". Figure 1 is a replicated representation of the original Gordon–Loeb model.

FIGURE 1
GORDON–LOEB MODEL



Adapted from Gordon & Loeb, 2002

Two findings from the GL model are summarized below (Gordon, Loeb, & Zhou, 2016):

1. *Firms should generally invest an amount that is less than or at most equal to roughly 37% of the expected loss that could result from a cybersecurity breach to an information set is directly related to the assumption that the benefits of cybersecurity investments increase at a decreasing rate;*
2. *The optimal level of cybersecurity investment does not always increase with the level of vulnerability.*

The FAIR Model

The FAIR model codifies and monetizes the risk. It deconstructs risk by explaining the components that constitute the risk as well as their interdependencies. The numerical connections between each building block or aspect of risk have been assessed and attributed dollar values, allowing risk to be evaluated as financial loss. The FAIR model is widely explored on the FAIR Institute web page https://www.fairinstitute.org/ and the book titled *Measuring and Managing Information Risk* (Freund & Jones, 2014).

A HYPOTHETICAL CASE STUDY

This section will provide a hypothetical example of how to apply the insights from the GL and FAIR risk models to assess the information assets of an NPO and calculate the optimal level of cybersecurity investment. We will use the same steps used in Gordon, Loeb, and Zhou (2016) in addition to the FAIR risk model concepts.

Profile of the Subject

The LE nonprofit, referred to as LE NPO, is a small nonprofit organization located in the DMV area (District of Columbia, Maryland, and Northern Virginia). It has fewer than 50 employees and fewer than 100 passive and active volunteers, and an annual budget less than $3 million.

LE NPO's beneficiaries are adults aged 18 years and older. LE NPO provides free education (various topics) services, monetary support, as well as first-necessity goods (food, clothes, toiletries).

LE NPO's activities rely on five streams of income: individual donations; grants coming from the federal government; grants coming from the state and the county; grants coming from other big donor organizations; and donations from commercial companies.

In order to maintain a constant level of annual income to fulfil its mission, the LE NPO must report to the donors who the beneficiaries are and what types of services are provided to the beneficiaries. In order to provide a comprehensive report to the donors, the LE NPO uses a database system and through electronic means collects personal identifiable information (PII) from the beneficiaries. The information is gathered centrally in the database and the integrated reporting functions help LE NPO to describe its beneficiaries. The collection of PII is particularly important for LE NPO when the donors request the funds to be distributed in forms of monetary donation, services, or goods specifically to vulnerable populations. So as to achieve this request, LE NPO collects five types of information:

1. General Information (First Name, Last Name and Contact Information: Phone number, Email Address and Physical Address, Social Security Number);
2. Demographics (Age, Gender, Race, Ethnicity);
3. Other (Marital Status, Children);
4. Employment and Annual/Monthly Income; and
5. Assets and Liabilities

No banking, credit, or other financial information is collected.

Estimation of the Monetary Value of the Information Set Using the FAIR Model

For the current project, we will consider the basic estimation of the monetary value of the information set: a dataset of 3,000 records containing beneficiary name, address, date of birth, and social security number (as per FAIR model example).

We used the FAIR model to estimate the value of the information set as the maximum potential loss (L) that LE NPO would suffer if the NPO would experience a data breach. According to FAIR model, such an information set is evaluated as follows.

I. The Scope Table for Level of Risks

The scope table (Table 1) provides a general overview of the assets of risks (Sensitive information), the primary threat – malicious in nature, and the confidentiality as the threat effect of interest.

TABLE 1
SCOPE TABLE FOR LEVEL OF RISKS

Asset at Risk	Threat Community	Threat Type	Effect
Customer PII	Cyber criminals	Malicious	Confidentiality

II. Primary Loss and Secondary Loss

According to the FAIR model, there are three loss forms likely to materialize from a data breach as *Primary Loss* (Productivity Loss, Response Costs, and Replacement Costs), and three forms as *Secondary Loss* (Response, Fines and Judgments, and Reputation).

Primary Loss

1. Primary Loss calculation – Productivity Loss is considered to be the loss caused by the interruption of the production/operations of a company; however, due to the nature of NPOs, no productivity loss is foreseen in the case of a data breach.
2. Primary Loss calculation – Response Cost is the time spent investigating and dealing with the event. According to the FAIR model, the primary response costs for an incident like this tends to fall into one of three categories: (1) person-hours spent in meetings regarding the incident, (2) investigation into what transpired, and (3) dealing with law enforcement. The FAIR model considers a minimum of 50 hours, a maximum of 400 hours, and a most likely value of 150 hours times the organization's average loaded employee hourly rate of $55 to come up with the following primary response cost estimates:

TABLE 2
PRIMARY LOSS ESTIMATES

Loss Type	Minimum	Most Likely	Maximum	Confidence
Primary Response	$2,750	$8,250	$22,000	Moderate

Note: For the purpose of this evaluation, the Primary Response can be considered as a general loss category and not strictly associated with the information set.

3. Primary Loss calculation – Replacement Costs are associated with terminated employees and considered not to be relevant for the current study.

Secondary Loss

4. Secondary Loss calculation – According to FAIR, response costs almost always include:
    - The cost of notifying customers and perhaps regulators.
    - The cost associated with increased volumes of customer support calls.
    - The cost of credit monitoring.
    - The cost of having people in meetings to strategize how to handle customers and regulators.
    - Legal and PR costs if the number of records is large enough.

Calculations: Compromised records – total number of records = 3,000

a. Customer notification costs – FAIR model considers notification costs were pretty well established for customers at $3 each. Therefore:
    - Customer notification cost maximum: $3 × 3,000 = $9,000
    - Confidence level: Low

b. Customer support calls resulting from an incident are also sometimes included as a response cost. FAIR considers 10% of the customers would call on an average at $10 per call. Therefore:
    - Customer support costs maximum: 10% × $10 × 3,000 = $3,000
    - Confidence level: Low

c. Credit monitoring costs – FAIR considers —the percentage of customers who would use the offer of credit monitoring and the cost each of those would represent. Those numbers were 10% and $25, respectively. Therefore:
    - Credit monitoring costs maximum: 10% × $25 × 3,000 = $7,500
    - Confidence level: Low

d. The person-hours involved in meetings, according to FAIR, also can be pretty sensitive to the number of compromised records. The estimated ranges were established as a minimum of 20 hours, maximum of 400 hours, and most likely 50 hours, and set at $125 per hour. Therefore:
    - Person-hours minimum: 20 × $125 = $2,500
    - Person-hours most likely: 50 × $125 = $6,250
    - Person-hours maximum: 400 × $125 = $50,000
    - Confidence level: Low

e. The legal cost estimates by FAIR are based on the number of compromised records. Therefore:
    - Legal costs minimum: $0
    - Legal costs maximum: 3,000 × $100 = $300,000
    - Confidence level: Low

f. PR costs according to FAIR are also highly sensitive to the number of affected customers. The number provided by business management and marketing for a worst-case event of this sort was $3,000,000. The most likely value was $0 based on an expectation that a compromise of 500 records would not result in any PR costs. For the current project, the PR costs will be considered as unknown.

g. Estimated fines and judgments according to FAIR would be $20 per record. Therefore:

- Legal costs minimum: $0
- Legal costs maximum: 3,000 × $20 = $60,000
- Confidence level: Low

TABLE 3
COMBINED SECONDARY LOSS ESTIMATES

	Maximum	Confidence
Notification	$9,000	Low
Customer support	$3,000	Low
Credit monitoring	$7,500	Low
Meetings	$6,250	Low
Legal	$300,000	Low
Fines and Judgments	$60,000	Low
PR	Unknown	Unknown

For the current project, we will consider just the values associated with the information set: the database with 3,000 records.

TABLE 4
COMBINED SECONDARY LOSS ESTIMATES – SCENARIO-BASED

	Maximum	Confidence
Notification	$9,000	Low
Customer support	$3,000	Low
Credit monitoring	$7,500	Low
Legal	$300,000	Low
Fines and Judgments	$60,000	Low
Total	$379,500	Low

Identify the Optimal Level of Cybersecurity Investment Using the GL Model

Step 1: For each information set, a rough estimate of the total monetary value will be provided. The estimated amount is considered to be the maximum potential loss (L) that LE NPO would suffer if the NPO would experience a data breach caused by unencrypted internal network traffic.

For the purpose of the current project, we considered four hypothetical information sets; however, we created the exact estimates just for one—the database with 3,000 records with beneficiaries' information. The reason for choosing just one information set is because we do not have information about the monetary value of other information sets (applicable to nonprofits) in the FAIR Model. Based on FAIR estimates, we can recreate the monetary value of the beneficiaries' information (3,000 records).

TABLE 5
INFORMATION SETS AND THEIR CORRESPONDING VALUE

	Information Sets	Monetary Value of Information Sets	Value
1	Database – 3,000 records	$379,500	High
2	Donors' information (PII & financial information)	n/a	High
3	Employees' information (PII)	n/a	Medium
4	Volunteers' information (PII)	n/a	Medium
5	Other internal documents	n/a	Low

Note: The n/a monetary value was provided to the other hypothetical information sets because no estimation is necessary as per the research methodology.

Step 2: Assign a vulnerability (V) score of 0.2, 0.4, 0.6, or 0.8 for each information set to indicate, respectively, a 20%, 40%, 60%, or 80% probability that the information set will suffer a data breach.

TABLE 6
VULNERABILITY SCORE & LEVEL

	Information Sets	Vulnerability Score (V)	Vulnerability Level
1	Database – 3,000 records	80%	High
2	Donors' information (PII & financial information)	60%	High-Medium
3	Employees' information (PII)	40%	Medium
4	Volunteers' information (PII)	40%	Medium
5	Other internal documents	20%	Low

Step 3: Combine Step 1 & Step 2 in a grid.

TABLE 7
COMBINED VULNERABILITY SCORE AND CORRESPONDING MAXIMUM LOSS PER INFORMATION SET

	Information Set V	Information Set IV	Information Set III	Information Set II	Information Set I – Database of 3,000 records $379,500 (Maximum Loss)
Vulnerability Score (V)	Donors' information (PII & financial information)	Employees' information (PII)	Volunteers' information (PII)	Other internal documents	Database – 3,000 records

20%	n/a	n/a	n/a	n/a	$75,900
40%	n/a	n/a	n/a	n/a	$151,800
60%	n/a	n/a	n/a	n/a	$227,700
80%	n/a	n/a	n/a	n/a	$303,600

Note: The n/a monetary value was provided to the other hypothetical information sets because no estimation is necessary as per the research methodology.

Step 4: The final step in the process is to decide the optimal level of investment in cybersecurity while considering the cost–benefit aspects of investing additional funds on each information set.

Note: Considering that the current project focuses on the value of just one information set—the database with 3,000 records—we will be consistent with the GL rule that the optimum investment is less than 37% of the expected loss. The GL model suggests that the optimal level of cybersecurity investment does not always increase with the level of vulnerability; however, for the hypothetical purpose of the current paper, we will apply the incremental levels of vulnerability to the Maximum Potential Loss calculated based on the FAIR model estimates.

TABLE 8
MAXIMUM POTENTIAL LOSS BY PROBABILITY SCALE & 37% RULE

Probability of a Breach	Probability x Maximum Potential Loss	Max 37% of Investment (as per GL model)
20%	$75,900	$28,083
40%	$151,800	$60,720
60%	$227,700	$84,249
80%	$303,600	$112,332
100%	$379,500	$140,415

As reported in Table 8, the Maximum Potential Loss of a dataset can range from $379,500 (at a 100% probability) to $75,900 (at a 20% probability). Therefore, by applying the 37% GL model rule of investment of the total potential loss, the investment in cybersecurity would range from $140,415 to $28,083. Considering the hypothetical scenario in which the organization is an NPO with an annual budget of $3 million, investment in the protection of only one dataset would range from 4% to 0.9% of the NPO's annual budget. This amount would be considered "operational costs" and would be considerably high for a NPO whose primary mission is positive social impact.

DISCUSSIONS

A maximum of $140,415 investment amount in cybersecurity for one basic information set of a nonprofit organization with an annual budget of less than $3 million would represent roughly 4% of the total annual income of the NPO. Considering the budget limitations of NPOs explained in a previous section, a 4% of the annual budget invested in the security of one basic information set (in this case a database of 3,000 records) would considerably harm the NPO's financial possibility to fully satisfy its social mission. Furthermore, NPOs tend to prioritize social mission over operational costs (Carey-Smith, Nelson, & May, 2007), which in this case is investment in cybersecurity. Therefore, a widely accepted model like GL in its original form may not represent a realistic solution for NPOs, considering their budget limitations. For example, the authors of the GL model have modified the original model to reflect the particularities of a specific sector to better fit the sector's needs (Gordon et al., 2015). Therefore, one future research direction would be to modify the GL model to incorporate the particularities of the NPOs.

Similarly, the FAIR model considers only "primary" and "secondary" costs. However, it does not consider potential "indirect economic costs" of business data breaches such as profit decline, productivity decline, loss of customers, reduced growth, loss of investments, system downtime, loss of competitiveness, loss of talent, loss of consumer confidence, reduced credit rating, insurance cost, and reputational costs (Wang, D'Cruze, & Wood, 2019). Despite that, not all those indirect costs are applicable to the nonprofit sector; some are indispensable parameters in a NPO's functional departments. For instance, NPOs heavily rely on their good reputation, trust, and confidence from individual donors, funding organizations, commercial donors, the public sector, and beneficiaries (Campbell, 2019). For NPOs, especially small NPOs, a data breach can result in detrimental consequences and even going out of business (Campbell, 2019; Johnson, 2019). Therefore, another future research direction is to take the indirect costs into consideration in order to fine-tune the FAIR model to a higher degree of precision.

Another significant difference between NPOs and for-profit organizations is the engagement of "volunteer work." The FAIR model considers an "average loaded employee hourly rate of $55"; however, NPOs often engage unpaid volunteers to perform daily activities, including data-related activities, instead of paid professional staff (Haight, 2015). From this perspective, the costs associated with human labor might be lower in case of the NPOs, which also requires a slight modification of the model to fit the NPO's particularities.

The National Council for Nonprofits recommends cyber liability insurance for nonprofits that would cover the costs resulted from notifying the entities whose information may have been compromised; to content repair, such as repair to a hacked website; and to hiring a PR firm for reputation recovery after a data breach (National Council of Nonprofits, 2019). However, while an annual insurance premium ranges between $5,000 and $10,000 per $1 million in primary or excess coverage (Gallagher, 2021), a recent report by the Cybersecurity and Infrastructure Security Agency (CISA) estimated potential losses for two cyber incident scenarios and found that only 13–17% of losses were actually covered by the insurance (CISA, 2020). Therefore, cyber insurance as a risk transfer strategy may or may not be an optimal choice for an NPO, depending on various factors such as the annual budget, the insurance policy, preemptions, and exemptions.

CONCLUSIONS

The use of technology in various sectors and fields contributes also to the rise of threats and security issues. These new risks necessitate greater research into the social, technical, and economic components of the cyberworld. Expenditure on cybersecurity has continually increased in response to increasing cybersecurity threats and it may soon reach an "inefficient and unaffordable" level (Felici et al., 2015). Felici et al. (2015) further emphasized that it is critical to have a deeper knowledge of these new socio-technical-economic complexities, which will imply both rethinking old cybersecurity challenges and finding new and unexplored areas of research. These new complexities make cybersecurity a multi- and interdisciplinary field rather than a unidirectional one.

The current paper is a great example of an interdisciplinary study that examines cybersecurity expenditure through the lens of economics and business aspects. This paper sheds light on a less-researched area in the cybersecurity field—NPOs—and demonstrates a hypothetical case study on how to calculate an optimal investment level in cybersecurity based on the GL and FAIR models. As a future work, the authors consider extending and modifying the two models to provide a realistic option for investment in cybersecurity for NPOs, considering their budget and workforce limitations. Providing an optimal amount of cybersecurity investment in the nonprofit sector would not only enlarge the limited body of academic knowledge, but would also significantly contribute to the industry.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of Marymount University Discover Research Center toward completing the current research project.

REFERENCES

AT&T. (2017). *The CEO's Guide to Data Security*. Retrieved from https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/attceocyberreport_compressed.pdf

Boggs, S.P. (2021). Key Takeaways from President Biden's Cybersecurity Executive Order. *The National Law Review*, *XI*(138). Retrieved from https://www.natlawreview.com/article/key-takeaways-president-biden-s-cybersecurity-executive-order

Campbell, J. (2019). *Marketing for the Modern Nonprofit*. Retrieved from https://jcsocialmarketing.com/nonprofits/

Carey-Smith, M., Nelson, K., & May, L. (2007). Improving Information Security Management in Nonprofit Organisations with Action. *5th Australian Information Security Management Conference*. Perth Western: Security Research Institute.

CISA. (2020). *Cost of a Cyber Incident: Systematic Review and Cross-Validation*. Retrieved from https://www.cisa.gov/publication/cost-cyber-incident-systematic-review-and-cross-validation

Ermicioi, N. (2020). *Factors affecting nonprofits' information security readiness during crises: A study of COVID-19's impact on small and medium nonprofit organizations (NPOS) in the DMV area (Order No. 28414637)*. Marymount University. Available from ProQuest Dissertations & Theses Global. (2524374134). Retrieved from https://www.proquest.com/docview/2524374134?pq-origsite=gscholar&fromopenview=true

Executive Office of the President. (2021). Executive Order 14028: Improving the Nation's Cybersecurity. In *Federal Registrar 86 FR 26633* (pp. 26633–26647).

FAIR Institute. (2021). *What is FAIR?* Retrieved May 26, from https://www.fairinstitute.org/frequently-asked-questions

Felici, M., Wainwright, N., Bisogni, F., & Cavallini, S. (2015). What's New in the Economics of Cybersecurity?: Observational and Empirical Studies. *IEEE Security & Privacy*, *13*(05), 12–15. https://doi.org/10.1109/MSP.2015.105

Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann.

Gallagher. (2021). *2020 Market Conditions Report: Cyber Liability*. Retrieved from https://www.ajg.com/us/news-and-insights/2020/feb/2020-market-conditions-report-cyber-liability/

Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, *235*(1), 277–300.

Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L.A., & Loeb, M.P. (2011). You May Be Fighting the Wrong Security Battles. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB10001424053111904900904576554762089179984

Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, *6*(1), 24–30. https://doi.org/10.4236/jis.2015.61003

Gordon, L.A., Loeb, M.P., & Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, *7*(2), 49–59.

Haight, L. (2015). *Is Your NonProfit Too Small to Be Hacked? Don't Believe It.* Retrieved from https://www.linkedin.com/pulse/too-small-hacked-dont-believe-laura-haight/

Hausken, K. (2014). Returns to information security investment: Endogenizing the expected loss. *Information Systems Frontiers*, *16*(2), 329–336.

Headd, B. (2019). *Small Business Facts: SPOTLIGHT ON NONPROFITS*. The Office of Economic Research of the SBA Office of Advocacy.

Johnson, R. (2019). 60 Percent of Small Companies Close Within 6 Months of Being Hacked. *Cybercrime Magazine*. Retrieved from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Malekos, Z., & Lostri, E. (2020). *The Hidden Costs of Cybercrime*. The Center for Strategic and International Studies (CSIS) of McAfee. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Microsoft Corporation. (2017). *Nonprofit Guidelines for Cybersecurity and Privacy*. Retrieved from https://download.microsoft.com/download/1/D/4/1D494A7D-D153-40FC-BC18-F4C2F800E752/Nonprofit_Guidelines_for_Cybersecurity_and_Privacy.pdf

Morgan, S. (2020). Cybercrime to Cost the World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

National Council of Nonprofits. (2019). *Cybersecurity for Nonprofits*. Retrieved from https://www.councilofnonprofits.org/tools-resources/cybersecurity-nonprofits

Nexia International. (2017). *Global Cybersecurity Report*. Retrieved from https://nexia.com/assets/files/Global_Cybersecurity_Report_2017.pdf

Palin, A. (2013). Maryland professors weigh up cyber risks. *Financial Times*. Retrieved from https://www.ft.com/content/606e0e5a-b345-11e2-b5a5-00144feabdc0

Pfleeger, S.L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software*, *25*(1), 35–42.

Ropeik, A. (2017). Small Indiana Nonprofit Falls Victim to Ransom Cyberattack. *NPR*. Retrieved from https://www.npr.org/2017/05/20/529257365/small-indiana-nonprofit-falls-victim-to-ransom-cyberattack

Suykens, B., Verschuere, B., & De Rynck, F. (2017). *Organizational Hybridity in Flemish Civil Society Organizations: Past Developments, Present Trends and Future Research Possibilities*. In CSI Flanders Working Paper 3. Ghent: Ghent University.

Verizon. (2021). *2021 Data Breach Investigations Report*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Wang, P., D’Cruze, H., & Wood, D. (2019). ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES. *Issues in Information Systems*, *20*(2), 162–171. https://doi.org/10.48009/2_iis_2019_162-171