



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**CYBERSECURITY COST EFFECTS ON THE
UNITED STATES MARINE CORPS' BUYING POWER**

by

Ian J. Cunningham

March 2021

Thesis Advisor:

Kenneth H. Doerr

Co-Advisor:

Simona L. Tick

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2021	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE CYBERSECURITY COST EFFECTS ON THE UNITED STATES MARINE CORPS' BUYING POWER			5. FUNDING NUMBERS	
6. AUTHOR(S) Ian J. Cunningham				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) This thesis conducted a systematic literature review to synthesize and analyze current research on cybersecurity investment risk that may inform the Marine Corps' future cybersecurity investment decisions. Using both public and private sector research on cybersecurity investment risk allowed for a broad look at academic studies that approached similar issues. This thesis makes recommendations on framework and two models that may be adopted by the Marine Corps as effective decision-making tools to help leadership. This research is important because the Marine Corps could benefit from an investment decision-making tool that is robust, works in a constrained budget environment, and allows for leaders to understand the risks of their decisions.				
14. SUBJECT TERMS cybersecurity investment, risk, discretionary spending, non-discretionary spending, military buying power			15. NUMBER OF PAGES 79	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**CYBERSECURITY COST EFFECTS ON THE
UNITED STATES MARINE CORPS' BUYING POWER**

Ian J. Cunningham
Captain, United States Marine Corps
BS, Colorado State University, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
March 2021**

Approved by: Kenneth H. Doerr
Advisor

Simona L. Tick
Co-Advisor

Chad W. Seagren
Academic Associate, Graduate School of Defense Management

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis conducted a systematic literature review to synthesize and analyze current research on cybersecurity investment risk that may inform the Marine Corps' future cybersecurity investment decisions. Using both public and private sector research on cybersecurity investment risk allowed for a broad look at academic studies that approached similar issues. This thesis makes recommendations on framework and two models that may be adopted by the Marine Corps as effective decision-making tools to help leadership. This research is important because the Marine Corps could benefit from an investment decision-making tool that is robust, works in a constrained budget environment, and allows for leaders to understand the risks of their decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	INTRODUCTION.....	1
B.	RESEARCH QUESTIONS.....	3
1.	What Research on Cybersecurity Spending Informs the Current Marine Corps' Buying Power Position?	4
2.	Given Data, Which Methods/Models Can Be Applied toward Marine Corps programs? Which Models are Most Likely to Address Cost Overruns Assuming Budget Constraints?.....	4
C.	SCOPE AND LIMITATIONS	4
D.	ORGANIZATION OF STUDY	5
E.	SUMMARY	5
II.	BACKGROUND	7
A.	CYBERSECURITY STUDIES.....	7
B.	SYSTEMATIC LITERATURE REVIEWS.....	11
C.	CONCLUSION	12
III.	METHODOLOGY AND RESEARCH APPROACH.....	13
A.	IDENTIFICATION PHASE	14
B.	SEARCHING PHASE	15
C.	SELECTION PHASE.....	17
D.	ASSESSMENT PHASE.....	19
E.	SYNTHESIS PHASE.....	20
IV.	SOURCE ANALYSIS.....	25
A.	IMPORTANT THEMES	25
1.	Robustness	25
2.	Constrained Budget	27
3.	Risk Appetite	29
B.	ADDRESSING THE RESEARCH QUESTIONS	30
1.	Informing the Marine Corps Situation	30
2.	Suggested Models	32
V.	CONCLUSION	35
A.	SUMMARY	35
B.	LIMITATIONS.....	36

C.	FUTURE RESEARCH.....	36
D.	RECOMMENDATIONS.....	37
APPENDIX A. SEARCH RESULTS		39
APPENDIX B. DEFINITIONS.....		43
APPENDIX C. BIBLIOGRAPHIC INFORMATION		47
APPENDIX D. RESEARCH CHARACTERISTICS.....		51
LIST OF REFERENCES.....		53
INITIAL DISTRIBUTION LIST		57

LIST OF FIGURES

Figure 1.	Decreasing benefits. Source Gordon et al. (2016).	9
Figure 2.	Game theory example. Source: Fielder et al. (2017).	10
Figure 3.	Search iterations flowchart	17

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Systematic Literature Review Comparison	14
Table 2.	Source Quality	20
Table 3.	Results by Research Approach	22
Table 4.	Results by Sector.....	22
Table 5.	Results by Model Used	23
Table 6.	Results by Output Measure.....	23
Table 7.	Results by Data Type	23
Table 8.	Model Comparison Table	33

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AHP	analytic hierarchy process
C&A	certification and assurance
DIACAP	DOD Information Assurance Certification and Accreditation Process
DOD	Department of Defense
DoDI	Department of Defense Instruction
FHAP	fuzzy analytic hierarchy process
FIS	fuzzy inference system
HQMC	Headquarters Marine Corps
IA	information assurance
IS	information systems
IT	information technology
MCDM	multi-criteria decision making
P&R	programs and resources
PPBE	Planning, Programming, Budgeting, and Execution
RMF	risk management framework

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis researches a possible gap in how the Marine Corps invests cybersecurity funds: unknown or incorrect forecasting models may cause budget overruns in future spending. I am using a systematic literature review to determine what current research on cybersecurity investing could best inform the future budgets of the Marine Corps. This systematic literature review identifies and catalogs the approaches used to determine cybersecurity investment risk currently reported in academic papers and establishes which models are applicable to the Marine Corps moving forward. Knowing how cybersecurity investment risk could affect future budgets will advise decision makers on the best courses of action moving forward in acquisition and fiscal decision making.

The importance of cybersecurity continues to increase due to information system requirements becoming more robust. Keeping up with peer competitors in relation to cybersecurity while keeping spending under control is important for the Department of Defense (DOD) to maintain competitive advantage in future fights and deterrence operations. The importance of a quality cybersecurity investment strategy is apparent when reading current strategic documents. The 2018 DOD Cyber Strategy document envisions the need for strong and prudent investments to help mitigate the risk to its cyber networks and infrastructure. “Defense Department faces a risk from the U.S. government’s continued budgetary uncertainty... continued fiscal uncertainty requires that DOD plan to build its cyber capabilities under a declining overall defense budget” (Secretary of Defense, 2018, p. 10).

This systematic literature review of current cybersecurity investment and budgeting risk research helps answer the following research questions.

1. What research on cybersecurity spending informs the current Marine Corps buying power position?
2. Given data which methods/models can be applied toward Marine Corps programs? Which models are most likely to address cost overruns assuming budget constraints?

This research uses the technical report *Guidelines for Performing Systematic Literature Reviews in Software Engineering* as the standard to conduct this systematic literature review. Systematic literature reviews can be used for multiple reasons, defined in the source as “a form of secondary study that uses a well-defined methodology to identify, analyse and interpret all available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable” (Kitchenham, 2007, p. vi). For this study, the systematic literature review is for finding an unbiased gap in current methods to suggest future studies and provide framework for new research through a well-defined methodology (Kitchenham, 2007).

This thesis used the following phases to conduct the systematic literature review: identification, searching, selection, assessment, and synthesis. These phases are derived from Kitchenham (2007). As Kitchenham states the best search strategies are iterative and benefit from examining other systematic literature reviews. This research used multiple other systematic literature reviews to help inform of different techniques to conduct the phases of a systematic literature review. The identification phase explains how this thesis took multiple iterations of research and contact to recognize there is a possible gap in knowledge to focus the research questions. The search process is explained throughout the identification and searching phases and consisted of five iterations of refining search terms. The selection of sources occurred during the searching and selection phases. Assessment of sources occurred during the selection, assessment, and synthesis phases. Synthesis was conducted solely in the synthesis phase.

The original search term of cybersecurity investment risk had 3972 results across five search engines. These results were paired down to 129 through five different search iterations. Once the 129 results were assessed and checked against inclusion criteria only 27 sources met the standard for the synthesis phase. These 27 sources were then assessed by the sources’ research approach, sector, model used, and data used.

The models that best fit the Marine Corps should incorporate robustness, constrained budget, and risk appetite. A robust model helps deal with the uncertainty of cybersecurity investing and responses of internal and external factors. Models that incorporate constrained budgets or constrained spending match the public domain and the

Marine Corps funding process that deals with a limited discretionary budget. Risk appetite of models are considered because the Marine Corps should view the risk of different options when considering cybersecurity spending.

The first research question posed in this thesis was what research on cybersecurity spending informs the current Marine Corps buying power position? The sources found in this systematic literature review had varying results that spoke to frameworks, game theory methods, and quantitative models in attempts to explain the most efficient ways to invest in cybersecurity. Three sources inform the Marine Corps' position by providing the framework and structure for potential models, though they may not have ideal quantitative models as part of the source. The first source that informs the Marine Corps (Paul & Wang, 2019) shows that entities should recognize the different aspects of cybersecurity investments and have a framework and model that manages risk across separate functions of cybersecurity. Garvey et al. (2013) show that spending to reduce cybersecurity events is not linear and timing of the investments is important. Another way this source can inform the Marine Corps situation is through their conclusion that decisions are made with uncertainties, informed assessment is crucial, and "Cybersecurity economic analyses must inform countermeasure investment decisions" (Garvey et al., 2013, p. 325). Ganin et al. used a multi-criteria decision framework to consider threats, vulnerabilities, and consequences. Their research is distinctive because it understands that social and physical domains must be considered along with the information domain (Ganin et al., 2020). The Marine Corps must understand the importance of protecting social and physical domains along with information to remain mission ready.

The second research question looks for a model that the Marine Corps could use when making cybersecurity investment decisions. The two recommended quantitative models come from Tavana et al. (2019) and Miaoui and Boudriga (2019). Tavana et al. (2019) presented a two-part model that uses FAHP to create informed qualitative inputs utilized by a FIS quantitative model to determine maximum benefit and minimal risks. The model is focused on robustness, understanding risks, and working with constraints. Miaoui and Boudriga's model is based off utility theory and implements the risk appetite of the decision makers when deciding the optimal investments (2019). Miaoui and Boudriga

conducted analysis of existing cybersecurity investment models and compared them across eleven aspects of cybersecurity. Their proposed model covers six aspects of cybersecurity investment models including budget constraints, investment tranches planning, and vulnerabilities and threats (Miaoui & Boudriga, 2019).

The purpose of the present study was to look at how the Marine Corps could approach the issue of cybersecurity investing under current strategic guidance. This systematic literature review used commonly accepted terms among the DOD to gather 129 filtered sources and through Kitchenham's best practices narrow to 27 final sources for synthesis and analysis. Sources were assessed by how their models approached the topic, examined the data, the outputs of models, and how they best fit themes that could benefit the Marine Corps. Themes identified in the research were robustness, budgetary constraints, and risk appetite. Three sources were noted for their way to inform the Marine Corps situation and provide possible framework structure. Ultimately, the models from Tavana et al. (2019) and Miaoui and Boudriga (2019) were suggested as possible solutions due to their ability to combine qualitative and quantitative inputs that can be robust, work with budget constraints, and incorporate risk.

References

- Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 40(1), 183–199. <https://doi.org/10.1111/risa.12891>
- Garvey, P. R., Moynihan, R. A., & Servi, L. (2013). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering*, 16(3), 313–328. <https://doi.org/10.1002/sys.21236>
- Kitchenham, B. (2007). *Guidelines for performing systematic literature reviews in software engineering*. https://www.elsevier.com/_data/promis_misc/525444systematicreviewsguide.pdf
- Miaoui, Y., & Boudriga, N. (2019). Enterprise security investment through time when facing different types of vulnerabilities. *Information Systems Frontiers*, 21(2), 261–300. <https://doi.org/10.1007/s10796-017-9745-3>

- Paul, J. A., & Wang, X. (Jocelyn). (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, 122, 113069. <https://doi.org/10.1016/j.dss.2019.05.009>
- Secretary of Defense. (2018). *The DOD cyber strategy*. Department of Defense. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
- Tavana, M., Khosrojerdi, G., Mina, H., & Rahman, A. (2019). A hybrid mathematical programming model for optimal project portfolio selection using fuzzy inference system and analytic hierarchy process. *Evaluation and Program Planning*, 77, 101703. <https://doi.org/10.1016/j.evalprogplan.2019.101703>

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. INTRODUCTION

Cybersecurity threats are increasing as the world continues to unite via networks. Defense systems continue to utilize information systems (IS) and networks to maximize effectiveness. Across the world other nations and non-state actors employ cyber attacks to weaken and compromise the United States defense industry. The costs of protecting and attacking in the cyber realm increases acquisition spending related to cybersecurity for the Department of Defense (DOD). The opportunity cost of spending on cybersecurity instead of funding other defense projects may have impacts on readiness. Increasing costs driven by growing cybersecurity requirements could cause future budgeting issues for the United States Marine Corps. We need to understand how cybersecurity cost growth will affect the future buying power to allow for better acquisition decisions. The threats to buying power must be identified and mitigated to the maximum extent possible to allow for budgetary freedom in the future.

This thesis researches a possible gap in how the Marine Corps invests cybersecurity funds: unknown or incorrect forecasting models may cause budget overruns in future spending. I am using a systematic literature review to determine what current research on cybersecurity investing could best inform the future budgets of the Marine Corps. A systematic literature review is a research method that allows for identification, evaluation, and interpretation of available research focused on a particular question (Kitchenham, 2007). This systematic literature review identifies and catalogs the approaches used to determine investment risk currently reported in academic papers and establishes which models are applicable to the Marine Corps moving forward. Knowing how cybersecurity investment risk could affect future budgets will advise decision makers on the best courses of action moving forward in acquisition and fiscal decision making.

To get a starting base for cybersecurity I use the DOD definition of cyberspace security from Joint Publication 3-12.

Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (2015).

The National Security Strategy of 2017 states the growing importance of cybersecurity.

America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security. For most of our history, the United States has been able to protect the homeland by controlling its land, air, space, and maritime domains. Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders. Cyber attacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business. (President of the United States, 2017).

The 2018 DOD Cyber Strategy outlines the need for action in cyberspace to preserve and enhance U.S. military advantages on a day-to-day basis. The focus on winning the cyber domain includes protecting critical infrastructure, military, and non-DOD defense critical infrastructure. The strategy document also mentions the importance of increasing cooperation between the U.S., allies, and industry to support cyber operations (Secretary of Defense, 2018).

"Department of Defense systems and networks are constantly under cyber attack. Nearly all defense systems incorporate information technology (IT) in some form and must be resilient from cyber adversaries" (Department of Defense, 2015, p. iii). The DOD has begun to understand the importance of cybersecurity and has implemented policies guiding the acquisition of IT with emphasis on cybersecurity. The DOD prior policy was the DOD Information Assurance (IA) Certification and Accreditation (C&A) Process (DIACAP) from 2007. The DIACAP was a set of DOD instructions that integrated activities across the DOD by using a three-part DIACAP enterprise governance. The three steps were accreditation, configuration control and management, and certification & accreditation

process. The DIACAP process was designed to manage employment of IS and enhance visibility of accreditation (Department of Defense Chief Information Officer, 2007). All programs were instructed to follow the DIACAP activities which were five steps intending to mirror the system life cycle. The five steps were initiate and plan information assurance IA C&A, implement and validate assigned IA controls, make certification determination & accreditation decision, maintain authorization to operate and conduct reviews, and decommission (Department of Defense Chief Information Officer, 2007).

Since DIACAP, the DOD has issued Department of Defense Instruction (DoDI) 8510.01 Risk Management Framework (RMF) for DOD IT, DoDI 8500.01 Cybersecurity, DOD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Life cycle, and DoDI 5000.02 Operation of the Defense Acquisition System which updated cybersecurity requirements in the DOD with focus on the acquisition process. DoDI 8500.01 Cybersecurity has mandated "cybersecurity must be fully integrated into the system life cycle and will be a visible element of organizational, joint, and DOD Component IT portfolios." The DOD evolved from DIACAP into a model of multi-tiered risk management method to help protect the interests of the United States (Department of Defense Chief Information Officer, 2019). Cybersecurity and overall IT risks will be assessed throughout the acquisition process and shall revise as the threats to system and the cybersecurity environment change (Department of Defense, 2015). The creation and dissemination of these recent DoDIs and guidebook demonstrates the DOD recognizing how important the future competitive environment of IS and cybersecurity is to the national strategies of the United States. Recently the Inspector General of the DOD released recommendations spanning multiple cybersecurity implementation concerns to the Air Force, Special Operations Command, Cyber Command, DOD Chief Information Officer, National Security Agency, Defense IS Agency (Office of the Inspector General, 2019).

B. RESEARCH QUESTIONS

The importance of cybersecurity continues to increase due to information system requirements becoming more robust. Keeping up with peer competitors in relation to

cybersecurity while keeping spending under control is important for the DOD to maintain competitive advantage in future fights and deterrence operations. Understanding future budget growth curves will allow senior leaders to make informed decisions regarding future budgets and acquisitions. This research conducts a systematic literature review of current cybersecurity investment and budgeting risk research. Conducting this research helps answer the following questions.

- 1. What Research on Cybersecurity Spending Informs the Current Marine Corps' Buying Power Position?**
- 2. Given Data, Which Methods/Models Can Be Applied toward Marine Corps programs? Which Models are Most Likely to Address Cost Overruns Assuming Budget Constraints?**

Research sources throughout this systematic literature review which inform the Marine Corps situation suggest that a model should include both qualitative and quantitative inputs. Multiple sources highlight how frameworks that use strategic inputs based on risk appetite and constraints can improve the outputs of quantitative models. Three selected themes of robustness, constrained budgets, and risk appetite are prevalent in this research and are recommended to be a part of the selection process when choosing a model. The models used by Tavana et al. (2019) and Miaoui and Boudriga (2019) are studies that meet these standards, though they may not be the final solution for the Marine Corps.

C. SCOPE AND LIMITATIONS

The scope of the research is to assess published investment models in terms of their applicability to predicting the Marine Corps budgeting on cybersecurity. Sources are current as of 2020 when the final search iterations are conducted. The research is not intended to examine or predict overall economic effects from global recessions or financial upswings. The research is not intended to discuss how cybersecurity acquisitions should be conducted during the Planning, Programming, Budgeting, and Execution (PPBE) process. Solving budgetary constraints caused by increasing cybersecurity costs is outside of the scope of this research. As Schatz and Bashroush (2016) note, systematic literature reviews leave out wider literature that can be relevant due to missing inclusion criteria.

D. ORGANIZATION OF STUDY

This thesis contains five chapters:

- Chapter I contains an introduction on cybersecurity in the DOD and explains the scope and limitations of this research.
- Chapter II contains a background into various approaches that academic community has taken to understand cybersecurity investments.
- Chapter III details the methodology used to identify, search, select, assess, and synthesis the results of this systematic literature review.
- Chapter IV discusses the results from the lens of the Marine Corps budgeting and acquisition.
- Chapter V concludes this research by discussing limitations of the systematic literature review, proposing follow-on research, and recommending future actions based on this research.

E. SUMMARY

The introduction chapter provides background information to the proposed research topic of investigating how cybersecurity acquisitions has gained importance to the DOD. Research questions identify the direction of the research to be conducted. Noting we are limited in our research parameter of the overall financial environment allows focus on the broader research of cybersecurity spending. This systematic literature review explores the current academic research on the topic of cybersecurity spending and infer how it will affect the Marine Corps budget going forward.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

To understand the basis for my systematic literature review on cybersecurity effects on budgeting, there needs to be understanding about current studies centered around cybersecurity investment and acquisitions. Studies have shown that better informational inputs to decision makers can help assist in informing decisions (Wilson, 2018).

A. CYBERSECURITY STUDIES

Studies on the importance of cybersecurity in business and inside the DOD are increasing and display a wide breadth of possible topics. These cybersecurity studies provide the approaches and processes which are required to ensure the DOD maintains competency and competitiveness in the IT realm. This section discusses the different methods used to model cybersecurity investment and spending. The studies can be broken into qualitative, quantitative, and studies using both methods in a hybrid mix. Pfleeger and Rue show the complexity of choosing an appropriate model for cybersecurity investments due to the multitude of factors such as relevance, consistency, transparency, accuracy, and the input and outputs of a model (2008).

Recent studies discuss the importance of conducting qualitative studies on cybersecurity budgeting and spending decisions. These studies detail the expanding requirement for all parties to be involved in cybersecurity acquisition, “A proactive and flexible approach to deter and defend against cybersecurity threats must involve all appropriate stakeholders; responsibilities extend to all members of the acquisition workforce, not just IT and engineering” (Speciale & Kendall, 2018, p. 13). Kui Zeng used case studies to examine how the DOD acquires cybersecurity and how its importance is rated among other factors in the acquisition process (2016). The DOD used no cybersecurity standards in over half of the 15 cases examined by Zeng. DoDI *Cybersecurity* updated DOD policy to address previous findings that cybersecurity is not a mandatory requirement (Zeng, 2016). Case studies of three separate DOD programs, two current and one prior program, showed current DOD processes were unequipped to acquire IT and IS in a rapidly changing environment (Cesarz & Gibson, 2017). Regarding the budgetary

constraints on cybersecurity and acquisition Cesarz and Gibson stated, “the governance of IT/IS programs, in terms of appropriation limitations, has the potential for devastating effects over the life cycle of a program” (p. 37). These various case studies demonstrated the requirement to include qualitative methods in future cybersecurity focused research.

The DOD has written several documents showing that being focused on cybersecurity and including cybersecurity in all aspects of acquisition and budgeting is imperative. Since Zeng’s 2016 findings the DOD has published further guidance in the DoDI *Cybersecurity*. “Cybersecurity requirements must be identified and included throughout the life cycle of systems including acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement of all DOD IT supporting DOD tasks and missions” (Department of Defense Chief Information Officer, 2019). The *Cybersecurity* instruction shows the DOD desire to incorporate the importance of cybersecurity into all portions of the acquisition process. Other documents issued by the DOD include the DODI 8510.01 RMF for DOD IT, DoDI 8500.01 Cybersecurity, DOD Program Manager’s Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Life cycle, and DoDI 5000.02 Operation of the Defense Acquisition System which updated cybersecurity requirements in the DOD with focus on the acquisition process. These documents provide support for a study which investigates the current academic literature addressing cybersecurity investment.

Several quantitative methods are used to predict the effects of cybersecurity investments and budgeting. Sensitivity analyses have focused on the entirety of the DOD process and specifically the system design processes. Wilson (2018) used a quantitative method to study the need for improving the DOD acquisition processes of IS, similar to the qualitative study done by Cesarz and Gibson (2017). Wilson (2018) used “rapid decisions analysis process to assist in ranking alternatives” (p. 44). Wilson’s method used sensitivity analysis based around a Multi-Criteria Decision Making (MCDM) model to differentiate aspects of certain outcomes allowing decision makers to adjust priorities depending on preferences. The MCDM model allowed for ranking alternative choices to optimize decision information in the form of outputs (Wilson, 2018).

Gordon et al. (2016) conducted a cybersecurity investment study using the Gordon-Loeb Model, a quantitative mathematical economic model which analyzes investment levels. The study indicates analytical and quantitative measures can improve on makeshift cybersecurity investment decisions. The Gordon-Loeb model created a formula defined as the security breach probability function (Gordon et al., 2016). The Gordon-Loeb security breach probability function uses probability to assess if a cybersecurity breach will occur depending on certain conditions. Monetary amount to assess the cost of a breach in another input variable for the Gordon-Loeb model used for this study. A third variable is defined as an investment in cybersecurity which lowers the probability of the breach. The model highlights “a rational economic procedure for firms to use in deciding on how much to spend on cybersecurity, in light of the cybersecurity risk confronting the firm” (Gordon et al., 2016, p. 58). The study demonstrates one way to analyze and improve how cybersecurity investment can be done in industries while still recognizing that organizational concerns need to be considered when making investment decisions. Figure 1 shows the results of Gordon-Loeb Model.

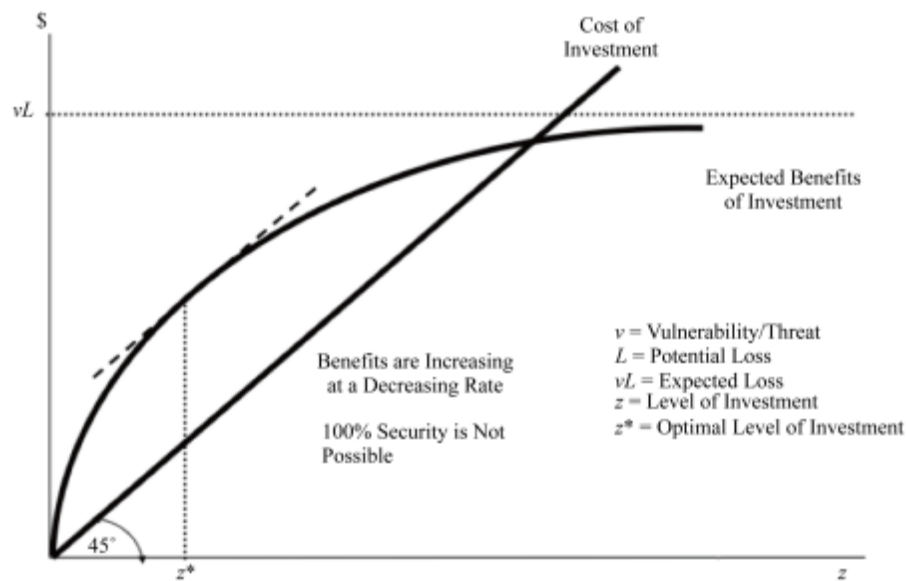


Figure 1. Decreasing benefits. Source Gordon et al. (2016).

Game theory has also been used to assess cybersecurity investment decisions. A multiple part study used game theory as an approach to support decision making relating to cyber security investments. In the 2015 study *Comparing Decision Support Approaches for Cyber Security Investment*, researchers used game theory examine cybersecurity budget decisions (Fielder et al., 2015). The 2015 study implemented a two-person zero sum game. A cybersecurity manager uses different levels of security against a cyber attacker who picks different methods of attack. Follow-on research in 2017 examined the three main challenges of investing in cybersecurity listed as lack of accurate risk assessment values, developing an all-inclusive method based on organizational environment, and threats which create a constantly changing investment strategy (Fielder et al., 2017). Figure 2 shows the proposed cybersecurity methodology by using game theory.

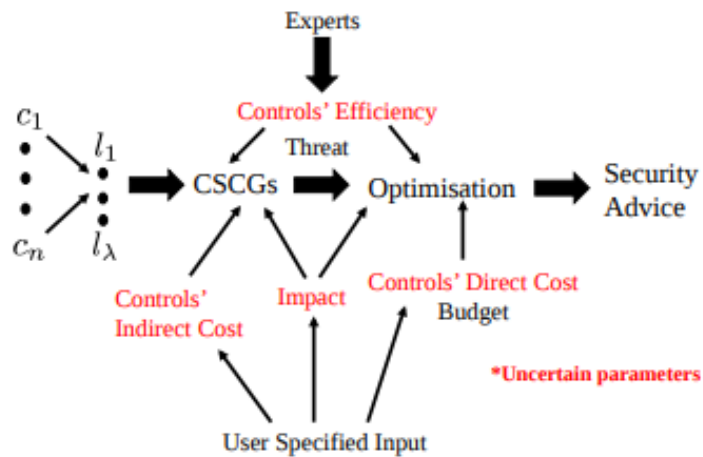


Figure 2. Game theory example. Source: Fielder et al. (2017).

The results from the game theory study demonstrates that as uncertainty increases the investment strategy must change as well. The requirement to change strategies is due to unconsidered solutions being effective as the parameters change as well as optimal solutions being eliminated due to inaccessible costs (Fielder et al., 2017). The findings using the game theory method match previous findings determining cybersecurity acquisitions and investments are not equipped to act in a rapidly changing environment.

Another economic model used was the Functional Dependency Network Analysis (FDNA) which was originally created by Garvey and Pinto in 2009. Pinto et al. adapted it to the cybersecurity domain to explain how risk management can be used to inform investment decisions (Pinto et al., 2020). This approach showed how threats and risk need to be assessed to consider how cyber attacks can create ripple effects in organizations.

The ability to find the minimum risk cost of cybersecurity investments was also demonstrated using Monte Carlo simulation in a paper by Ekelund and Iskoujina (2019). This was accomplished by defining the direct and indirect costs of defense as well as the costs of damages relating to cybersecurity attacks on an organization. The purpose of this study was to show how risk management should influence cybersecurity investments (Ekelund & Iskoujina, 2019).

This introduction on several methods is not an inclusive list to what can appear in an extensive systematic literature review but demonstrates that there are multiple ways to approaching and researching solutions to cybersecurity spending risks. Allowing multiple methods of research when conducting a systematic literature review that aim to improve cybersecurity spending modeling and prediction will allow this research to identify the most effective approaches.

B. SYSTEMATIC LITERATURE REVIEWS

This research uses the guidance of the *Guidelines for performing Systematic Literature Reviews in Software Engineering* as the model to conduct this systematic literature review. This technical report is modeled after studies done by Barbara Kitchenham and other academic authors. Systematic literature reviews can be used for multiple reasons, defined in the source as “a form of secondary study that uses a well-defined methodology to identify, analyse and interpret all available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable” (p. vi). For this study the systematic literature review is for finding a gap in current methods to suggest future studies and provide framework for new research (Kitchenham, 2007). This research is using a systematic literature review in its best attempt to provide unbiased results through a well-defined methodology, noted as an advantage by Kitchenham.

In the search and analysis phases used in this study, a similar systematic literature review study was found. That research did not address forecasting methods explicitly but did address valuation models. Schatz and Bashrouh (2017) focused on the economic value of information security investments in organizations, stating that it was difficult for practitioners to identify key approaches in current research. To conduct their research, they adopted a systematic literature review process and adopted a multiple step approach that Kitchenham and Charters proposed in a paper. The initial results for Schatz and Bashrouh was 779 sources, this large number was narrowed down to 270, then through removing duplicates and final decisions 25 papers were included in the primary study. Their findings among the final 25 papers mapped across nine categories showed that a focus on return on investment, utility maximization, and real options theory (Schatz & Bashrouh, 2017). While the topic of their review is different, it is important to note that forecast of cost growth is of little value without a way to express the value obtained from that cost. In that sense, an understanding of the models examined by Schatz and Bashrouh (2017) are a pre-requisite to obtaining value from the current study. It is noted, however, that in their paper many of the sources they found approached the problem from an academic perspective vice a practical implementation. Comparing Schatz and Bashrouh (2017) to this study no results appeared in both studies. The main reason is the differing search terms which are derived from differing research questions. Schatz and Bashrouh used “information security” OR “IT Security” OR “InfoSec” while my research used “cybersecurity” (2017). It is possible that studies found in Schatz and Bashrouh (2017) would similarly fit as a useable model for this research question.

C. CONCLUSION

The background chapter focused on recent cybersecurity studies demonstrating how different research methods from qualitative to quantitative have been used to predict costs of cybersecurity budgets or investments and the usefulness of conducting a systematic literature review. This chapter demonstrates that multiple approaches can be taken to solve similar cybersecurity budgeting questions and warrant inclusion into a systematic literature review. It was discussed how systematic literature reviews can be used as an approach to similar research topics when there is not a clear solution.

III. METHODOLOGY AND RESEARCH APPROACH

This chapter discusses the methodology and research approach used to search, identify, and analyze sources. Following protocol established by Kitchenham, it is important to identify the research question(s) and the methods. The purpose of using a systematic literature review methodology is to identify relevant studies that can help answer research questions (Kitchenham, 2007).

This thesis used the following phases to conduct the systematic literature review: identification, searching, selection, assessment, and synthesis. These phases are derived from (Kitchenham, 2007). As Kitchenham states the best search strategies are iterative and benefit from examining other systematic literature reviews. This research used multiple other systematic literature reviews to help inform of different techniques to conduct the phases of a systematic literature review. The most commonly derived techniques come from Kitchenham (2007), Schatz (2017), McElroy (2019) and Rabii et al. (2020).

The identification phase explains how this thesis took multiple iterations of research and contact to recognize there is a possible gap in knowledge to focus the research questions. The search process is explained throughout the identification and searching phases and consisted of five iterations of refining search terms. The selection of sources occurred during the searching and selection phases. Analysis of sources occurred during the selection, assessment, and synthesis phases. Synthesis was conducted solely in the synthesis phase. The marking of these phases is important to a systematic literature review to help detect as much relevant literature as possible and allow for a repeatable process (Kitchenham, 2007).

Table 1 displays the results of other systematic literature reviews that researched questions in the cyber realm. The table displays the sources captured in original search terms, with search filters, and then after inclusion and exclusion criteria were applied. The final column displays the ratio of articles kept for final discussion. This table shows that on average just 29% of source articles once filtered are kept after applying inclusion and exclusion criteria.

Table 1. Systematic Literature Review Comparison

Author Name	Original Search	With Filters	Inclusion/ exclusion criteria	Final %
(Rabii et al., 2020)	16959	82	30	37%
(Schatz & Bashroush, 2017)	779	270	22	8%
(Taylor et al., 2020)	742	72	32	44%
(Alahmari & Duncan, 2020)	N/A	50	15	30%
(Leenen, 2018)	773	76	22	29%
(Tuma et al., 2018)	5000	136	31	23%
This Paper	3972	129	27	21%
Average	4850.6	114.33	25.33	29%

A. IDENTIFICATION PHASE

The research questions examined here were derived from a thesis topic provided by Headquarters Marine Corps (HQMC) Programs & Resources (P&R) and revised through conversations with that office. The focus being on how the buying power affects acquisition and if certain programs in the Marine Corps are likely to have cost increases which diminish the buying power of the Marine Corps. After communicating with P&R it was suggested to narrow the research to how increases in cybersecurity spending affects the buying power of the Marine Corps.

After discussions with HQMC P&R, my intent was to forecast cybersecurity cost growth in Aviation Command and Control, as a demonstration of cost-growth forecasting methods. Several programs in that community are engaged in collecting data on cybersecurity costs. However, after discussions with those program offices, I was only able to obtain data for 3% of their current cybersecurity budget, and no significant history of spending. I determined it would be infeasible to forecast cost growth with these sparse data and chose to conduct a systematic literature survey instead. This turn in research was made to fully understand the current research that applies to cybersecurity investment risk. Such an understanding can be applied to improve decision making, and allow for analysis of models that can be used going forward to predict and manage cybersecurity costs in the Marine Corps.

The goal for search results was to get around 120 source returns that would enable vetting down to 40–60 results to be analyzed. These number of sources allow for an accurate analysis by a lone researcher, a further analysis of more sources could be conducted by a larger research team (Kitchenham, 2007). This assumed some duplicate search results and unusable sources due to those sources not relating to the thesis topic.

B. SEARCHING PHASE

As Kitchenham stated the best search strategies are iterative and benefit from examining other systematic literature reviews (Kitchenham, 2007). The search phase started across five different search engines; ABI/INFORM, Web of Science, ProQuest, EBSCO, and Worldcat. These search engines were selected for their broad results that would allow for a larger pool of results to initially start from and then trim to a desired amount that best lent itself for the size and scope of this research. Ultimately there were five iterations of search efforts before deciding on the final search term that best fit the scope and scale of this research. Before moving on it was determined that using peer reviewed articles only would yield the best results, non-peer reviewed results were captured for research purposes only. Search results can be seen in Appendix A.

To gain an estimate of how many results would be found during a search the term cybersecurity investment risk was queried in all five search engines without the peer review requirement. Worldcat and ProQuest returned the most with 2,586 and 1,386 results, respectively. Web of science returned the least with 71. The term cybersecurity budget risk was then run with ProQuest and Worldcat returning the most results and Web of Science with the least again. This completed the first iteration of searches. The disparity in results between the terms investment and budget was evident at this point. Web of Science was no longer used in the following iterations due to lack of results, this stems from the specificity of articles in the Web of Science search pool.

I reviewed the NPS Dudley Knox Library search basics to acquaint with the common practices of successful searches (Marlatt, n.d.). Adding quantitative as a keyword was desired since the research goal is to find an economic model that the Marine Corps can use going forward to help mitigate risk relating to cybersecurity spending. Adding

quantitative would reduce the number of results found that were relating to qualitative solutions. Quantitative was searched as a keyword or in the abstract depending on the advanced search options among the search engines.

The next iteration of searches used the term cybersecurity budget risk. Budget over investment was chosen as it more closely matches the terminology of the Marine Corps and the original thesis topic. Searching for peer reviewed results using the term cybersecurity budget risk, while looking for the term quantitative in the abstract or keyword based on search engine capabilities narrowed the results too much. For example, when adding quantitative as a keyword Worldcat went from 126 down to 38 results and ProQuest from 16 to 3. This stemmed from the term and usage of budget instead of investment. The term investment in place of budget would yield drastically more search results across all five search engines. At this point in the searches, it was shown that the search engines ABI/INFORM, Web of Science, and EBSCO would not yield enough results when using search qualifiers of peer reviewed and qualitative. Follow-on searches in those search engines were for gathering data though the results would not be used in the systematic literature review.

The third iteration of search used *forecast** to increase useful research results. The * stem symbol was used on forecast to include forecasting and other variations of the word forecast. The inclusion of forecast did not significantly expand the results. It was becoming apparent at this point the inclusion of the term investment over budget needed to be reincluded to allow for broader results based on industry terminology over Marine Corps terminology.

Another limiting factor identified was the DOD accepted standard of cybersecurity as one word was limiting results from research that uses cyber security as two words. The fourth search iteration re-ran all previous search terms using “cybersecurity” OR “cyber security” while keeping the restrictions on peer reviewed articles and using the keyword quantitative. As expected, including the two-word spelling of cybersecurity added more results. The results varied in how many new results appeared based on search engine. To retain the scope of the research it was decided that using the DOD standard of cybersecurity was in the best interest of this systematic literature review.

The fifth and final iteration of the search was to use the term cybersecurity investment risk with quantitative as a keyword and peer review. This decision was due to the large overlap of articles that were found when searching cybersecurity budget risk. A large overlap of articles was found between ProQuest and ABI/INFORM since these search engines use similar databases. Due to overlap and the larger number of results from ProQuest the results from ABI/INFORM were not used in the research. EBSCO search engine did not have a large enough result pool to choose from, just 6 results matched the fifth iteration. EBSCO search results were not considered for this reason. The search results used for this study are taken from ProQuest, 41 results, and Worldcat, 87 results, for 128 total articles. The fifth iteration resulted in 126 unique results. The two identical search results qualified for analysis in this study. For future iterations of this research best practices by Kitchenham suggests using one researcher to act as a data extractor and one as data checker for large numbers of results such as this study (Kitchenham, 2007). Figure 3 is a visual representation of the search iterations.

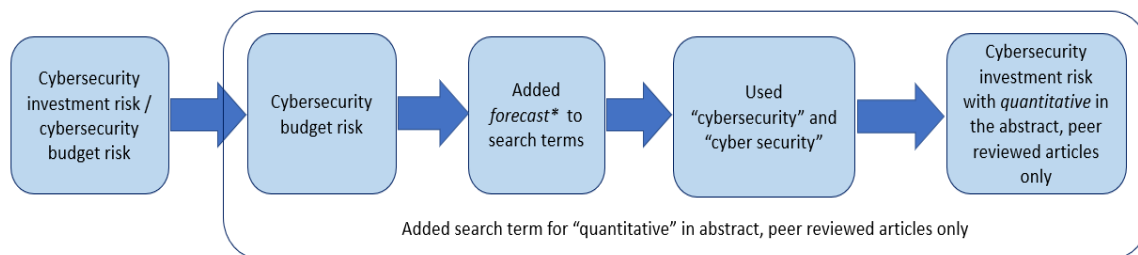


Figure 3. Search iterations flowchart

C. SELECTION PHASE

The selection phase is intended to select the highest quality sources using inclusion criteria that reduces bias (Kitchenham, 2007). To capture quality and differences in the results I used Microsoft Word, Microsoft Excel, and open source Zotero reference management software. The following categories were used to organize the results. The inclusion criteria used for this study:

- Studies using mathematical model relating to IS, cybersecurity, or similar topics.
- Studies that provided the framework or closely related to the study of cybersecurity investments.

Once a source was selected for inclusion meta data was placed in an Excel spreadsheet and it was placed in Zotero for organization and bibliographic purposes. Following Kitchenham's best practices, the initial results were liberally selected to allow maximum inclusion, this resulted in 50 results from the 126 sources which were initially selected (2007). To reduce possible bias no articles were excluded based on sector, language, journal, or authors.

The Excel spreadsheet has three categories that were used in the selection and assessment phases. Category one contained bibliographic information such as title, author(s), date, publication type, journal, and citation. Category two contained traits to distinguish between research characteristics such as research approach, sector tags, model used, output measure, and data type. Research approach used the identifiers, theory building, theory testing, application & development, and policy analysis. Sector tags consisted of the tags public and private, a mix of both is allowed for this study. The subcategories for model used is as follows:

- Is the model theoretical? Empirical? None?
- Is the model multi-period or single period?
- Is the model robust? Non-robust?

Output measure marked the results of the source models into categories such as framework, cost benefit, utility, or risk. There were eight different output measures captured among all sources. Data type consists of qualitative, quantitative, hybrid and if the data used is hypothetical, case study, historical, or collected. These characteristics were grouped using the definitions in Appendix B. The third category was directly quoted from the sources to show how the author defined their research by question/purpose, abstract,

and findings. This concluded the entries portion of the selection phase. Sources were then assessed for quality.

D. ASSESSMENT PHASE

The assessment phase is intended to assess the quality of the articles (Kitchenham, 2007). All 50 remaining articles were assessed using the inclusion criteria as well as a ranking system. During this process nine articles were found to not meet the inclusion criteria. The results had promising titles and abstracts but ultimately would not have provided value into this research.

To address the quality of sources based on the focus of this research four assessment questions were used. The questions had a ranking system giving zero, one, or two points based on the defined criteria. The first question is subjective to my assessment of which sources fit the research questions, I attempted to be unbiased and liberal in my rankings. A score of poor was given when the source did not mention cybersecurity risk in the same context as intended or mentioned it in passing during their research, if a source was between a poor or fair ranking I gave a fair to include papers. A score of fair was given when a paper mentioned topics relating to the thesis question in sections or in whole even if the paper was not solely focused on a question that matched one of the research questions presented in this thesis. Sources with a well ranking directly answered a question related to this thesis in a similar manner. Questions two through four are quantifiable and pulled from the source paper or Google Scholar.

- How well does the source address the research questions of this thesis?
0 = Poor, 1 = Fair, 2 = Well
- What conclusion does the source recommend?
0 = Theoretical, 1 = Proposes follow-on research, 2 = Proposed solution
- What is the strength of data/evidence?
0 = Unsupported opinion, 1 = Supported opinion, 2 = Empirical
- Is the source cited in other works? (Based on Google Scholar search)

0 = Poor (≤ 10), 1 = Fair (11-29), 2 = Well (≥ 30)

After quality assessment was complete it was found that 14 results received a poor rating in addressing the research question of this thesis. These 14 results were removed and 27 remaining results were used in the synthesis phase.

E. SYNTHESIS PHASE

The synthesis phase is meant to summarize and collate the results of included studies (Kitchenham, 2007). Interpretation of data will occur in Chapter IV. Definitions for tags in Tables 3–7 are found in Appendix B.

Table 2. Source Quality

	How well does the source address the research question of this thesis?	What conclusion does the source recommend?	What is the strength of data/evidence?	Is the source cited in other works? (per Google Scholar)
1	1	1	1	0
2	2	2	2	1
3	1	2	1	2
4	2	1	1	2
5	1	1	1	2
6	2	2	2	1
7	1	2	2	1
10	2	2	2	1
11	1	1	1	0
12	2	2	1	2

	How well does the source address the research question of this thesis?	What conclusion does the source recommend?	What is the strength of data/evidence?	Is the source cited in other works? (per Google Scholar)
15	2	2	1	1
16	1	2	2	0
18	1	1	1	0
20	1	1	1	0
23	1	1	2	2
24	1	2	1	0
25	1	1	1	0
26	1	1	1	2
27	2	1	2	2
28	1	2	1	2
29	1	1	1	0
30	1	1	1	0
31	1	1	1	0
32	1	1	1	0
37	1	1	2	1
39	1	1	1	2
40	1	1	1	2

Table 2 results show only the 27 sources that qualified for interpretation.

Table 3 shows the source results by the research approached used by the authors. If the approach was not directly stated in the source paper I used the definitions from SAGE research located in Appendix B to make a judgement decision.

Table 3. Results by Research Approach

Research Approach	Amount
Theory Building	9
Theory Testing	7
Application & Development	7
Policy Analysis	4

Table 4 results show if the paper was focused on public or private sector. If no clear declaration of sector was made papers that used constrained budgets or finances were marked with “public” or “both” tag. This was done to match the budgetary environment of public entities.

Table 4. Results by Sector

Sector	Amount
Public	6
Private	12
Both	9

Table 5 shows the model used by the authors. Results were placed into one category only. In some sources multiple models were presented to show the evolution of the model. In sources containing multiple models the final model was used for determining the category.

Table 5. Results by Model Used

Model	Amount
Empirical, Multiperiod, Robust	8
Empirical, Multiperiod, Non-robust	1
Empirical, Single Period, Non-robust	5
Theoretical, Single Period, Robust	1
Theoretical, Single Period, Non-robust	6
Theoretical, Multiperiod, Robust	4
Theoretical, Multiperiod, Non-robust	1

Table 6. Results by Output Measure

Output Measure	Amount
Cost Benefit	6
Expected Costs	5
Framework	5
Performance	1
Risk	3
Systematic Literature Review	1
Social Cost	1
Utility	5

Table 6 results were tagged with only one output measure.

Table 7. Results by Data Type

Data Type and Study	Amount
Hypothetical	10
Case Study	10
Historical	4
Collected	3

Table 7 results were tagged with only one output measure.

This chapter describes the first four phases used in the systematic literature review process. Identification showed us a possible gap in knowledge and marks the start of the systematic literature review. The search phase demonstrates the five iterations of searches to obtain the sample of 126 unique sources. Selection phase was done through a liberal process of cataloging sources with Zotero, entering sources into Excel, and ranking against multiple metrics. Post selection phase there were 50 sources remaining to assess. Assessment phase looked at the quality of those 50 articles based on inclusion criteria and assessment questions, nine sources were dropped due to not meeting inclusion criteria and another fourteen were dropped due to a poor assessment score. The final 27 sources were presented across multiple tables showing their tags. The synthesis phase of this systematic literature review is covered in the upcoming chapter.

IV. SOURCE ANALYSIS

In this chapter, I discuss the sources found in the systematic literature review regarding themes that best fit the Marine Corps needs and which sources best answer the research questions proposed in this thesis.

A. IMPORTANT THEMES

The models that best fit the Marine Corps should incorporate robustness, constrained budget, and risk appetite. As a theme robustness stood out amongst the papers because it was mentioned often across the sources. The second theme of constrained budgets or constrained spending match the public domain and the Marine Corps funding process that deals with a limited discretionary budget, unlike the private sector where alternate funding can be secured. The third theme of risk appetite merged from the sources and my understanding of how the Marine Corps makes decisions. The risk appetite of models is considered because the Marine Corps should understand how risk appetite effects the decision-making process of cybersecurity spending. While not the only themes that emerged across the sources these three themes make up a salient but partial list. This systematic literature review looked at the final 27 sources for these themes.

1. Robustness

A robust model helps deal with the uncertainty of cybersecurity investing and responses of internal and external factors. The sources found in this systematic literature review are not in agreement on a single interpretation of robustness. Robustness is important but there are many ways to examine robustness and no commonly accepted definition. Using an uncertainty taxonomy Aven discusses that robustness is important when problem structure is unknown (Aven, 2013b). This problem structure includes the context, system model, system outcome, and weights on the outcomes. This paper uses the guidance from Aven that a robust model should create an acceptable output when the model encounters those structural issues (Aven, 2013b). The Marine Corps' cybersecurity investment problem structure confronts unknown uncertainties. Threats can come from unknown actors, places, and times and present a wide range of uncertainties. Robust

models can help the Marine Corps deal with uncertainty from internal and external sources. Internal uncertainty can come from multiple areas including but not limited to, billet turnover, changing strategies in the DOD and service, and expanding and shrinking budgets. External uncertainty can come from many sources including emerging adaptive threats and changing international standards regarding cybersecurity. Out of 27 sources 13 claim to use a robust model. Using a model that mitigates uncertainty through robustness measures should be a priority if the Marine Corps chooses to adopt a cybersecurity investment framework and quantitative model.

The proposed mathematical programming model by Tavana et al. (2019) recognizes the importance of robustness. This model uses a “two-stage process to select an optimal project portfolio with the aim of maximizing project benefits and minimizing project risks” (p. 1). The first phase is a fuzzy analytic hierarchy process (FAHP) that weights criteria and sub-criteria of potential decisions. The second stage uses the fuzzy inference system (FIS) to consider dependencies between selected criteria. The source states that “fuzzy logic with quantitative models aids in handling the uncertainties inherent in real-world problems” (Tavana et al., 2019, p. 5). By using this two-stage process and sensitivity analysis it was concluded that their model is robust. This demonstrates that robust models can be selected for decisions that require both qualitative and quantitative inputs (Tavana et al., 2019).

Another source uses the concept of socially optimal cybersecurity investment based around robust optimization. Paul and Wang (2019) use an ellipsoidal uncertainty robust model to mitigate uncertainty across multiple aspects of cybersecurity. This approach is used to respond to information Paul and Wang obtained during their research that stated insufficient data as a problem when making cybersecurity investment decisions (Paul & Wang, 2019).

Smith and Pate-Cornell (2018) use a Bayes-adaptive Markov decision process because of its usefulness in “studying sequential decision problems when there is model uncertainty” (p. 437). This model further uses a multi-armed bandit problem because the multiple time period robust information it gives to decision makers, “sequentially allocate efforts among competing actions, whose values are uncertain at the time of allocation, but

become better understood as time passes” (Smith & Pate-Cornell, 2018, p. 437). This model informs how changing efforts which can occur in the Marine Corps due to internal and external uncertainty.

One study combines a “GARCH-based Risk Assessment and Mitigation framework” to estimate variance over time with “Markowitz’s mean-variance optimization for a given IT budget and preference” (Biswas & Mukhopadhyay, 2018, p. 276). This approach puts a premium on future time period uncertainty and how to best manage change over periods of time. One of the two main conclusions from Biwas and Mukhopadhyay was to use robust cybersecurity strategies based off careful planning (Biswas & Mukhopadhyay, 2018).

This section gave a guiding definition of robustness and demonstrates multiple models that manage uncertainty with robust models in different ways. Unknown inputs can cause structural issues in a problem and robustness allows for the model outputs to remain reliable. Sources in this systematic literature review used FHAP, ellipsoidal uncertainty, bayes-adaptive, and Markowitz’s mean-variance methods among others to deal with uncertainty. Each method has their positives and negatives and shows that policy making is an important consideration when choosing a robustness scheme (Aven, 2013b). The Marine Corps can borrow from a multitude of robust options that would allow for flexibility in future decisions to help respond to internal and external factors.

2. Constrained Budget

The Marine Corps budget, similar to other services, is growing more slowly than the common 2% inflation rate. All services are expected to receive a 3.5% cut in 2021 and remain flat through 2025 (Office of the Under Secretary of Defense (Comptroller), 2020). Analyzing sources from a constrained budget lens is important because models that assume an unconstrained environment do not match the Marine Corps budget situation. It is important for the model to emulate the budget environment of the Marine Corps. Poor investments could further shrink constrained budgets from an opportunity cost perspective. Our of 27 sources, 16 spoke of budgets or investing in a constrained way, similar to a public sector budget. These sources gave important insight to investing with a constrained budget.

A Miaoui and Boudriga study notes that “when a decision maker is constrained to under-invest due to budget limitation, he/she is not able to control the additional incurred security risk and quantify it, so that he/she can decide whether the investment is still profitable” (Miaoui & Boudriga, 2019, p. 268). The authors create a model that is designed to match the optimal investment while still satisfying a constrained budget value over. This model adjusts over time as threats change and investments may need to shift in different areas (Miaoui & Boudriga, 2019).

Another source uses a game theory model to show how constraints can impact investment decision making. Utilizing a Colonel Blotto game players are challenged to protect and attack cyber resources with varying amounts of constraints placed on those resources (Zhang et al., 2016). Through this method an optimal allocation of resource allocation is found, this could apply of offensive and defensive cyber systems. In conclusion Zhang et al. (2016) finds that targets with the most resources have higher chances of being a target.

A 2013 study on historical data of the 24 federal agencies show how constrained budgets can affect cybersecurity effectiveness. Koong et al. uses budget incentive as one of three inputs to determine how budgets, internal threats, and external threats impacted cybersecurity performance based off historical data. Budget was found to have the largest impact on cybersecurity performance.

In addition, as evidenced from this study, the most important dynamic in the information systems security performance has been the internal decisions taken in these agencies especially in assigning and distributing the budget. Indeed, as the budget in these agencies increases, the budget allocated to IT raises and thus information security performance of these agencies enhances. When agencies allocate high budget to IT, these agencies can invest more in advanced technologies that help prevent attacks.(Koong et al., 2013)

Budget constraints can have effects on different levels, they are not just a strategic issue. Different levels of management tend to overweigh the distress caused by financial issues because of job security, or in the Marine Corps case job performance reviews. Furthermore, managers tend to make decisions that prioritize security over other assets because of limited tenures (Srinidhi et al., 2015).

This section discussed different ways that studies are attempting to learn about constraints in cybersecurity budgets. Some sources approach budgets by implementing constraints into their models. Others show how constrained budgets can affect decisions made by those in positions of allocation.

3. Risk Appetite

Risk appetite is important for the Marine Corps to determine as certain systems may require more aggressive investments into cybersecurity. I am using the term risk appetite as “willingness to take on risky activities in pursuit of values” (Aven, 2013, p. 467). This allows the Marine Corps to match its risk appetite to each investment decision, whether it be high risk appetite or low risk appetite. Investing to protect one system could take a different risk appetite than investing to protect another system. Investment decisions should factor risk. Due to risk being part of the search term it was a common theme in the sources, 25 of 27 sources incorporate risk in some form as part of their studies. Four studies use risk as the output to their model: Ganin et al. (2020), Biswas and Mukhopadhyay (2018), Jenab et al. (2016), and Zhang et al. (2016).

Organizationally, how the Marine Corps sees risk will affect how those the Marines and contractors involved invest in cybersecurity. “Organizations with risk-averse decision makers have a greater tendency to invest in security measures for risk reduction” (Kissoon, 2020, p. 420). Kissoon’s study covers how it is important for leaders in decision making positions to review the amount of risk they want their organization taking. Leaders set the risk appetite for an organization (Kissoon, 2020).

Ganin et al. (2020) discuss a decision framework for cybersecurity risk management. This framework complies different aspects of threats, vulnerabilities, and consequences to calculate risk. Their model incorporates MCDM to allow for an alternate way of analyzing risk. The difficulty of calculating how risk is computed based on gains or losses demonstrates the complexity, but necessity, of including risk into cybersecurity investment decisions (Ganin et al., 2020).

Armenia et al. (2019) approach risk from a qualitative perspective. Allowing qualitative approaches to risk appetite borrows from the suggested definition that expected

values and probabilities fail to indicate the uncertainty tied to the values (Aven, 2013a). This is important because, as discussed prior, how an organization views risk will affect how they invest in cybersecurity. Knowing the probabilities and expected values without risk appetite guidance can lead to misguided cybersecurity investment. “Top management should define policies in line with the organization’s mission...and cyber risks management” (Armenia et al., 2019, p. 412). Jenab et al. (2016) comment that cybersecurity can be bureaucratic and mechanistic within organizations.

This section discussed different methods regarding how risk effects cybersecurity in organizations. Nearly all sources discuss risk and some used risk as their output when modeling cybersecurity investments. Sources spoke to how the risk appetite of an organization effects how cybersecurity investments are made. The Marine Corps should match their risk appetite of desired level of cybersecurity protection to the desired cost risks of their investments. Failing to match risk levels between cybersecurity protection and fiscal spending could result in investments that are deemed too risk seeking or too risk averse. To accomplish this the Marine Corps should ensure that policies and risk management are incorporated into cybersecurity investment decision making.

B. ADDRESSING THE RESEARCH QUESTIONS

1. Informing the Marine Corps Situation

The first research question posed in this thesis was on what research on cybersecurity spending informs the current Marine Corps’ buying power position. The sources found in this systematic literature review had varying results that spoke to frameworks, game theory methods, and quantitative models in attempts to explain the most efficient ways to invest in cybersecurity. No one source answers the Marine Corps’ situation exactly as these studies were based around different research questions. These sources can help give direction to the Marine Corps and avoid common mistakes that these authors may have run into when looking at cybersecurity investment. I believe that three sources best fit what the Marine Corps should examine when looking into cybersecurity investments in the future. These sources could inform the Marine Corps position by

providing the framework and structure for potential models; they may not have ideal quantitative models as part of the source.

The Marine Corps should recognize the different aspects of cybersecurity investments and have a framework and model that has similar traits to the Paul and Wang (2019) research that manages risk across separate functions of cybersecurity. Paul and Wang's discussions of risk appetite and use of social cost as their output was a unique concept among the sources found (2019). While their final model in the paper used a private firm, they considered constrained budgets throughout their model. The study was also unique because it talks about different aspects of cybersecurity while some other sources lumped cybersecurity as one entity. Their research on different aspects of cybersecurity is a recommendation the Marine Corps could follow. "This evidence points to a serious flaw in frameworks that consider only prevention. When resources are highly constrained, the damage of leaving out containment & detection safeguards may seem negligible but not in the current environment of increasing concern over breaches and cybersecurity spending" (Paul & Wang, 2019, p. 8). They further conclude that investment decisions in containment & detection have positive impacts in social cost when resources are constrained, while their benefits in non-constrained scenarios are minimal (Paul & Wang, 2019).

A research paper done in 2013 has useful research lessons that can help inform the Marine Corps on their cybersecurity budgeting regarding future buying power. Garvey et al. (2013) informs the Marine Corps situation through the use of a tabletop approach, which uses a cybersecurity event matrix to determine monetized and non-monetized costs. Considering costs in a monetized and non-monetized way can fit the Marine Corps. This matrix helps inform of risk across different aspects of cybersecurity, similar to the Paul and Wang model. The paper by Garvey et al. shows that spending to reduce cybersecurity events is not linear and timing of the investments will cross fiscal years (2013). Another way this research can inform the Marine Corps' situation is through their conclusion that decisions are made with uncertainties, informed assessment is crucial, and "Cybersecurity economic analyses must inform countermeasure investment decisions" (Garvey et al., 2013, p. 325).

Understanding the uncertainty and constraints of the situation can allow the Marine Corps to select quantitative models moving forward under a proper cybersecurity investment framework. Ganin et al. research uses a multi-criteria decision framework in a Monte Carlo simulation using triangular distribution for cybersecurity risk management. The MCDA used threats, vulnerabilities, and consequences as their criteria. This research is distinctive because it understands that social and physical domains must be considered along with the information domain (Ganin et al., 2020). The Marine Corps must understand the importance of protecting social and physical domains along with information to remain mission ready. Ganin et al. also conclude that metrics link to strategy (2020).

The Marine Corps should select a quantitative model that is complimented by a framework. This will help inform the Marine Corps' future budget situations and how decisions are affected by their environment. A robust framework that understands the unique risk requirements in a constrained budget environment would help the Marine Corps implement and fully utilize a cybersecurity investment model.

2. Suggested Models

The second research question revolves around selecting methods or models that can be applied by the Marine Corps, and then selecting models that were aimed at addressing cost overruns assuming budget constraints. The models were compared in Table 8. The ideal model would be empirical, multiperiod, and robust. The models would be multiperiod to ensure that a multiple time periods of investments would be considered. Robustness is important for the factors described at the beginning of Chapter IV. The models were examined to see if they had monetary outputs that considered risk.

Table 8. Model Comparison Table

Model Used	Total Amount	Output		Monetary		Risk	
		Yes	No	Yes	No	Yes	No
Empirical, Multiperiod, Robust	8	8		5	3	8	
Empirical, Multiperiod, Non-robust	1	1			1		1
Empirical, Single Period, Non-robust	5	1	4	1	4	5	
Theoretical, Single Period, Robust	1		1		1	1	
Theoretical, Single Period, Non-robust	6	4	2	3	3	5	1
Theoretical, Multiperiod, Robust	4	4		3	1	4	
Theoretical, Multiperiod, Non-robust	1		1		1	1	
Systematic Literature Review	1	1			1		1

This narrowed the suggested models to five. Among the five sources two best fit the themes of robustness, constrained budgets, and risk appetite while also allowing for the qualitative inputs that should be part of a cybersecurity investment framework. These sources are Tavana et al. (2019) and Miaoui and Boudriga (2019). Tavana et al. (number two in Table 2, p. 22) scored well on the source quality metrics with twos in three categories and a one in its citation score due to it being cited 13 times. Miaoui and Boudriga (number 10 in Table 2, p. 22) had the same score with three twos and a one in citation score due to being cited 11 times. The other two sources that scored as well in quality of source were

not suggested because one uses a theoretical model and the other being too heavily private sector focused. While neither model can be implemented without adjustment, they are both quality models that could assist the Marine Corps going forward in the future.

Tavana et al. (2019) model is a two-part model that uses FAHP to create informed qualitative inputs utilized by a FIS quantitative model to determine maximum benefit and minimal risks. The model is focused on robustness, understanding risks, and working with constraints. The FAHP portion of the model evaluates projects from a strategic-operational level which matches the Marine Corps. The FIS quantitative model step allows multiple aspects to be examined, the authors looked at three in their study. By focusing on three objectives at once instead of three objectives individually it was shown that all values benefited. When looking individually, one particular value would increase at the detriment of other values (Tavana et al., 2019).

The Miaoui and Boudriga (2019) model is based off utility theory and implements the risk appetite of the decision makers when deciding the optimal investments. Miaoui and Boudriga conducted analysis of existing cybersecurity investment models and compared them across eleven aspects of cybersecurity. It was found that current models only cover four or less aspects listed. The proposed model covered six aspects including budget constraints, investment tranches planning, and vulnerabilities and threats (Miaoui & Boudriga, 2019). The model includes outcomes for risk averse, risk neutral, and risk seeking investments.

This chapter discussed three themes that are important to the Marine Corps when choosing a cybersecurity investment framework and model. It is important any recommendations consider robustness, the challenges of working under a constrained budget, and how to properly manage risk. The research questions were discussed with examples from multiple sources highlighting how frameworks that use strategic inputs based on risk appetite and constraints can improve the outputs of quantitative models. Two models were selected as recommendations to the second research question. Both sources bring benefits to that would allow the Marine Corps to make informed investment decisions based on criteria the Marine Corps selects.

V. CONCLUSION

A. SUMMARY

The importance of a quality cybersecurity investment strategy is apparent when reading current strategic documents. The 2018 DOD Cyber Strategy document envisions the need for strong and prudent investments to help mitigate the risk to its cyber networks and infrastructure. “Defense Department faces a risk from the U.S. government’s continued budgetary uncertainty... continued fiscal uncertainty requires that DOD plan to build its cyber capabilities under a declining overall defense budget” (Department of Defense, 2018, p. 10). DoDI 8500.01 charges the Under Secretary of Defense for Acquisition, Technology, and Logistics with overseeing cybersecurity investments while the DOD SISO is responsible for guidance and oversight of the cybersecurity budget throughout the PPBE process (Department of Defense Chief Information Officer, 2019). These documents guide the services to ensure their cybersecurity investments are cohesive to the larger DOD cybersecurity investment and budgeting plans. This systematic literature review is an important step in conducting research on the common accepted academic standards of cybersecurity investing to eventually adopt and implement a framework and model that use best practices.

The purpose of this study was to look at how the Marine Corps could approach the issue of cybersecurity investing under current strategic guidance. The systematic literature review method was chosen because of the ability to locate and analyze a broad scope of conducted research and create a set of research for future actions (Kitchenham, 2007). This systematic literature review used commonly accepted terms amongst the DOD to gather 129 filtered sources and through Kitchenham’s best practices narrow to 27 final sources for synthesis and analysis. Sources were assessed by how their models approached the topic, examined the data, the outputs of models, and how they best fit themes that could benefit the Marine Corps. Quality of sources was assessed by how well the research fit the give research questions of this thesis, what the sources recommended, the strength of evidence, and number of citations in other work. Themes identified in the research were robustness, budgetary constraints, and risk appetite. Robustness allows the Marine Corps

to cope with the uncertainty surrounding cybersecurity investments. Constrained budgets match the fiscal environment of the Marine Corps. Risk appetite allows the Marine Corps to match strategic-level guidance with organizational decision makers, creating synchronization of desired risk when making decisions at all levels. Ultimately, two models were suggested as possible solutions due to their ability to combine qualitative and quantitative inputs that can be robust, work with budget constraints, and incorporate risk.

B. LIMITATIONS

The systematic literature review performed in this thesis is susceptible to the common limitations of all systematic literature reviews. Two particular limitations of this study are (1) the use of private and public sector models and (2) the inability to quantitatively test using actual budgeting data from the Marine Corps. This systematic literature review included public and private sector research sources to help answer a public sector issue. This induces biases and problems inherent to converting private sector models to a public sector challenge. The private models were included to allow a larger look at the research currently done on the topic of cybersecurity investment. The other notable limitation of this study was the inability to conduct a quantitative model test using Marine Corps cybersecurity funding numbers due to classification level.

A limitation of the Tavana et al. (2019) model is the use of the analytic hierarchy process (AHP). Rank reversal of existing options can occur in an AHP when additional options are added. While the rank order of scale-free AHP scores is correct the scores are not proportional (Karthikeyan et al., 2016).

C. FUTURE RESEARCH

Future research on the topic of cybersecurity investment risk could build from this systematic literature review through various means. I recommend that future research broaden the sources through expanded and targeted search terms. Future research could also obtain and test models using the Marine Corps' cybersecurity budgetary numbers. Examination of other systematic literature reviews that explored similar cybersecurity topics that no common phrase for "cybersecurity" has been adopted across research groups. Therefore, all terms and grammatical variations similar to cybersecurity, such as IS and IT,

should be included to gather the widest breadth of sources to assess. Expanding the terms will better capture the research done on this topic and give the Marine Corps a bigger decision pool to choose from when assessing a model to adopt. Future research should also strive to obtain cybersecurity budgeting data to evaluate which models inform and predict the Marine Corps' situation.

D. RECOMMENDATIONS

The Marine Corps can enhance their investment decisions by adopting a cybersecurity investment model. A model that forecasts growth in the cybersecurity realm would help predict future costs against a constrained budget. Research sources throughout this systematic literature review indicate that a model should include both qualitative and quantitative inputs to allow organizations to match risk appetite to their allotted budgets. The Marine Corps should adopt a robust framework and model to meet their needs. The framework should be designed around the unique challenges of a constrained budget, fluctuating internal and external threats, and specialist cybersecurity inputs to create useable metrics. These metrics would be used as part of a robust quantitative model that can forecast the cybersecurity budget to inform leaders and decisions makers how to best allot a limited budget. The methods used by Tavana et al. (2019) and Miaoui and Boudriga (2019) are studies that meet these standards, though they may not be the final solution for the Marine Corps.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SEARCH RESULTS

Search Engine / Search iteration	Search Term	Results	Peer Reviewed	“Cybersecurity” or “Cyber Security” (Peer Reviewed, Quantitative) 4th Iteration of searches
ABI/INFORM				
1	Cybersecurity Investment Risk (NOFT)	615	31	2
1	Cybersecurity Budget Risk (NOFT)	204	7	1
2	Cybersecurity Budget Risk (NOFT); quantitative (Abstract)	11	1	21
2	Cybersecurity Budget Risk (Anywhere); quantitative (Abstract)	56	11	86
3	Cybersecurity AND budget risk forecast* AND quantitative(abstrack)	26	3	83
5	Cybersecurity Investment Risk (Anywhere); quantitative (Abstract)	107	20	2
Web of Science				
1	Cybersecurity Investment Risk (All Fields)	71	N/A	N/A
1	Cybersecurity Budget Risk (All Fields)	26	N/A	N/A
2	Cybersecurity Budget Risk (All Fields); quantitative (Abstract)	1	N/A	N/A
3	Cybersecurity AND budget risk forecast* AND quantitative(abstrack)	N/A	N/A	N/A

Search Engine / Search iteration	Search Term	Results	Peer Reviewed	“Cybersecurity” or “Cyber Security” (Peer Reviewed, Quantitative) 4th Iteration of searches
5	Cybersecurity Investment Risk; quantitative (Abstract)	N/A	N/A	N/A
ProQuest				
1	Cybersecurity Investment Risk (NOFT)	1386	65	83
1	Cybersecurity Budget Risk (NOFT)	465	16	78
2	Cybersecurity Budget Risk (NOFT); quantitative (Abstract)	30	3	3
2	Cybersecurity Budget Risk (Anywhere); quantitative (Abstract)	143	26	46
3	Cybersecurity budget risk forecast*(Anywhere); quantitative (Abstract)	72	8	13
5	Cybersecurity Investment Risk (Anywhere); quantitative (Abstract)	275	41	83
EBSCO				
1	Cybersecurity Investment Risk (All Fields)	2248 5	1299	20
1	Cybersecurity Budget Risk (All Fields)	9714	606	18
2	Cybersecurity Budget Risk (All Fields); quantitative (Abstract)	13	9	18
3	Cybersecurity budget risk forecast*; quantitative (Abstract)	5	3	8
5	Cybersecurity Investment Risk; quantitative (Abstract)	25	6	20

Search Engine / Search iteration	Search Term	Results	Peer Reviewed	“Cybersecurity” or “Cyber Security” (Peer Reviewed, Quantitative) 4th Iteration of searches
Worldcat				
1	Cybersecurity Investment Risk (Keyword)	2586	354	541
1	Cybersecurity Budget Risk (Keyword)	971	126	61
2	Cybersecurity Budget Risk (Keyword); quantitative (Keyword)	38	38	61
3	Cybersecurity budget risk forecast*; quantitative (Abstract)	62	12	18
5	Cybersecurity Investment Risk; quantitative (Abstract)	573	87	541

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DEFINITIONS

Tag	Definition	Source
No.	“A distinction of word form denoting reference to one person or thing or to more than one.”	(“Oxford English Dictionary,” n.d.)
Title	“The name of a book, composition, or other artistic work.”	(“Oxford English Dictionary,” n.d.)
Author(s)	“A writer of a book, article, or report.”	(“Oxford English Dictionary,” n.d.)
Date	“The day of the month or year as specified by a number.”	(“Oxford English Dictionary,” n.d.)
Publication Type	“The preparation and issuing of a book, journal, piece of music, or other work for public sale.”	(“Oxford English Dictionary,” n.d.)
Journal/Publisher	“A person or company that prepares and issues books, journals, music, or other works for sale.”	(“Oxford English Dictionary,” n.d.)
Research Approach	Research Approach (Theory building, theory testing, application & development, Policy analysis/rhetoric) of source	
-Theory Building	“A term with many meanings but broadly speaking a set of interrelated ideas or concepts relevant to the explanation or interpretation of a particular topic or domain.”	(“SAGE Research Methods,” n.d.)
-Theory Testing	“The process of subjecting a theory to empirical scrutiny.”	Research Methods,” n.d.)
-Application & Building	“Applied research is inquiry using the application of scientific methodology with the purpose of	Research Methods,” n.d.)

Tag	Definition	Source
	generating empirical observations to solve critical problems in society.”	
-Policy analysis	“Policy analysis research studies set up to evaluate the effects of a policy or policies during the implementation and maturation stages are often referred to as process studies.”	Research Methods,” n.d.)
Sector Tags	Sector tags (Public, Private) of source	
-Public	“Of or provided by the government rather than an independent, commercial company.”	(“Oxford English Dictionary,” n.d.)
-Private	“(Of a service or industry) provided or owned by an individual or an independent, commercial company rather than by the government.”	(“Oxford English Dictionary,” n.d.)
Data Type	Data Type (Quantitative, Qualitative, Hybrid) and (none, hypothetical, laboratory, pilot/case, historical, collected) of source	
-Quantitative	“Relating to, measuring, or measured by the quantity of something rather than its quality.”	(“Oxford English Dictionary,” n.d.)
-Qualitative	“Relating to, measuring, or measured by the quality of something rather than its quantity.”	(“Oxford English Dictionary,” n.d.)
-Hybrid	A mix of both quantitative and qualitative data, per the definitions listed	
-None	“No amount; not at all.”	(“Oxford English Dictionary,” n.d.)
-Hypothetical	“Of, based on, or serving as a hypothesis.”	(“Oxford English Dictionary,” n.d.)
-Laboratory	“A test conducted under controlled scientific conditions in a laboratory or similar setting.”	(“Oxford English

Tag	Definition	Source
		Dictionary,” n.d.)
-Pilot/case	“A process or record of research in which detailed consideration is given to the development of a particular person, group, or situation over a period of time.”	(“Oxford English Dictionary,” n.d.)
-Historical	“Of or concerning history; concerning past events.”	(“Oxford English Dictionary,” n.d.)
-Collected	“(Of individual works) brought together in one volume or edition.”	(“Oxford English Dictionary,” n.d.)
Research Question/Purpose	“The reason for which something is done or created or for which something exists.”	(“Oxford English Dictionary,” n.d.)
Abstract	“Make a written summary of (an article or book).”	(“Oxford English Dictionary,” n.d.)
Findings	“A conclusion reached as a result of an inquiry, investigation, or trial.”	(“Oxford English Dictionary,” n.d.)
Citation	“A quotation from or reference to a book, paper, or author, especially in a scholarly work.”	(“Oxford English Dictionary,” n.d.)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. BIBLIOGRAPHIC INFORMATION

No.	Title	Author(s)	Date	Journal/Publisher
1	Optimum spending on cybersecurity measures	Kissoon, Tara	2020	Emerald Publishing
2	A hybrid mathematical programming model for optimal project portfolio selection using fuzzy inference system and analytic hierarchy process	Tavana, Madjid; Khosrojerdi, Ghasem; Mina, Hassan; Rahman, Amirah	2019	Elsevier
3	Cybersecurity strategies: the queries methodology	Carin, L., Cybenko, G., & Hughes, J.	2008	Computer
4	Cybersecurity economic issues: clearing the path to good practice.	Pfleeger, S. L., & Rue, R.	2008	IEEE
5	Multicriteria decision framework for cybersecurity risk assessment and management.	Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I.	2020	Risk Analysis
6	Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making	Benaroch, M.	2018	Information Systems Research
7	Cyber risk analysis for a smart grid: how smart is smart enough? A multiarmed bandit approach to cyber security investment	Smith, M. D., & Pate-Cornell, M. E.	2018	IEEE
10	Enterprise security investment through time when facing different types of vulnerabilities	Miaoui, Y., & Boudriga, N.	2019	Information Systems Frontiers
11	Towards the definition of a dynamic and systemic assessment for cybersecurity risks	Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M.	2019	Systems Research and Behavioral Science

No.	Title	Author(s)	Date	Journal/Publisher
12	Economic valuation for information security investment: a systematic literature review	Schatz, D., & Bashroush, R.	2017	Information Systems Frontiers : A Journal of Research and Innovation
15	A macro method for measuring economic-benefit returns on cybersecurity investments: the table top approach	Garvey, P. R., Moynihan, R. A., & Servi, L.	2013	Systems Engineering
16	G-ram framework for software risk assessment and mitigation strategies in organisations	Biswas, B., & Mukhopadhyay, A.	2018	Journal of Enterprise Information Management
18	Enterprise security economics: a self-defense versus cyber-insurance dilemma	Miaoui, Y., & Boudriga, N.	2019	Applied Stochastic Models in Business and Industry
20	Flow-graph and markovian methods for cyber security analysis	Jenab, K., Khoury, S., & LaFevor, K.	2016	International Journal of Enterprise Information Systems
23	Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation	Zhang, Y., Wang, L., Xiang, Y., & Ten, C.-W	2016	IEEE
24	Push and pull effects of homeland information security incentives	Koong, K. S., Merhi, M. I., & Sun, J.	2013	Information Management & Computer Security
25	Socially optimal IT investment for cybersecurity	Paul, Jomon A; Wang, Xinfang (Jocelyn)	2019	Decision Support Systems
26	Quantitative metrics and risk assessment: The three tenets model of cybersecurity	Hughes, Jeff; Cybenko, George.	2013	Technology Innovation Management Review
27	Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors	Srinidhi, Bin; Yan, Jia; Tayi, Giri Kumar	2015	Decision Support Systems

No.	Title	Author(s)	Date	Journal/Publisher
28	Defining and computing a value based cyber-security measure	Aissa, Anis Ben; Abercrombie, Robert K; Sheldon, Frederick T; Mili, Ali	2012	Information Systems and eBusiness Management
29	Maximizing security management performance and decisions with the MFC cyber security model: e- learning case study	Rjaibi, N; Rabai, L B A	2017	EAI Endorsed Transitions on e-Learning
30	Towards the design of a collaborative cybersecurity networked organisation: identification and prioritisation of governance needs and objectives.	Tagarev, Todor	2020	Future Internet
31	A real-world information security performance assessment using a multidimensional socio-technical approach	Prislan, Kaja; Mihelič, Anže; Bernik, Igor	2020	Plos one
32	Continuous quantitative risk management in smart grids using attack defense trees	Rios, Erkuden; Rego, Angel; Iturbe, Eider; Higuero, Marivi; Larrucea, Xabier.Sensors	2020	Basel
37	An analysis of economic impact on IOT industry under GDPR	Seo, Junwoo; Kim, Kyoungmin; Park, Mookyu; Park, Moosung; Lee, Kyungho	2018	Mobile Information Systems
39	The law and economics of software security	Hahn, Robert W; Layne-Farrar, Anne	2006	Harvard Journal of Law and Public Policy
40	Resilience metrics for cyber systems	Linkov, Igor; Eisenberg, Daniel A; Plourde, Kenton; Seager, Thomas P; Allen, Julia; et al.	2013	Environment Systems & Decisions

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. RESEARCH CHARACTERISTICS

No	Research Approach	Sector Tags	Model Used	Output Measure	Data Type
1	Theory Building	Private	Empirical, Single Period, Non-robust	Framework	Quantitative, Case Study
2	Theory Building	Public, Private	Empirical, Multiperiod, Robust	Cost Benefit	Hybrid, Case study
3	Application & Development	Public, Private	Theoretical, Single Period, Non-robust	Cost Benefit	Hybrid, Hypothetical
4	Theory Building	Public, Private	Empirical, Single Period, Non-robust	Framework	Qualitative, Historical
5	Theory Building	Public, Private	Empirical, Multiperiod, Robust	Risk	Hybrid, Case study
6	Application & Development	Private	Empirical, Multiperiod, Robust	Cost Benefit	Quantitative, Case Study
7	Application & Development	Public	Empirical, Multiperiod, Robust	Utility	Hybrid, Case study
10	Application & Development	Public, Private	Empirical, Multiperiod, Robust	Utility	Hybrid, Historical
11	Policy Analysis	Private	Theoretical, Single Period, Non-robust	Framework	Qualitative, Case study
12	Theory Building	Public, Private	Systematic literature review	Systematic literature review	Hybrid, Collected
15	Theory Building	Public	Theoretical, Multiperiod, Robust	Cost Benefit	Hybrid, Hypothetical
16	Application & Development	Private	Empirical, Multiperiod, Robust	Risk	Hybrid, Historical
18	Theory Testing	Private	Theoretical, Multiperiod, Robust	Utility	Hybrid, Hypothetical

No	Research Approach	Sector Tags	Model Used	Output Measure	Data Type
20	Theory testing	Public, Private	Theoretical, Multiperiod, Robust	Risk	Hybrid, Hypothetical
23	Theory Testing	Public	Theoretical, Single Period, Non-robust	Risk	Hybrid, Hypothetical
24	Policy Analysis	Public	Empirical, Multiperiod, Non-robust	Performance	Hybrid, Historical
25	Application & Development	Private	Empirical, Multiperiod, Robust	Social Cost	Hybrid, Case study
26	Theory Building	Private	Theoretical, Multiperiod, Non-robust	Framework	Hybrid, Case study
27	Theory Testing	Private	Theoretical, Multiperiod, Robust	Expected Costs	Hybrid, Hypothetical
28	Theory Building	Private	Theoretical, Single Period, Non-robust	Expected Costs	Hybrid, Hypothetical
29	Theory testing	Private	Empirical, Single Period, Non-robust	Expected Costs	Hybrid, Case study
30	Theory Building	Public	Empirical, Single Period, Non-robust	Framework	Hybrid, Collected
31	Application & Development	Private	Empirical, Single Period, Non-robust	Utility	Hybrid, Collected
32	Theory testing	Public, Private	Theoretical, Single Period, Non-robust	Cost Benefit	Hybrid, hypothetical
37	Policy Analysis	Public, Private	Empirical, Multiperiod, Robust	Expected Costs	Hybrid, Case study
39	Policy Analysis	Public, private	Theoretical, Single Period, Non-robust	Expected Costs	Hybrid, Hypothetical
40	Application & Development	Public	Theoretical, Single Period, Robust	Framework	Hybrid, Hypothetical

LIST OF REFERENCES

- Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5. <https://doi.org/10.1109/CyberSA49311.2020.9139638>
- Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems Research & Behavioral Science*, 36(4), 404–423. <https://doi.org/10.1002/sres.2556>
- Aven, T. (2013a). On the meaning and use of the risk appetite concept. *Risk Analysis*, 33(3), 462–468. <https://doi.org/10.1111/j.1539-6924.2012.01887.x>
- Aven, T. (2013b). On how to deal with deep uncertainties in a risk assessment and management context: Perspective. *Risk Analysis*, 33(12), 2082–2091. <https://doi.org/10.1111/risa.12067>
- Biswas, B., & Mukhopadhyay, A. (2018). G-ram framework for software risk assessment and mitigation strategies in organisations. *Journal of Enterprise Information Management*, 31(2), 276–299. <https://doi.org/10.1108/JEIM-05-2017-0069>
- Cesarz, Z. J., & Gibson, D. K. (2017). *Navy and Marine Corps IT/IS acquisition: A way forward* [Master's Thesis, Naval Postgraduate School]. NPS Archive: Calhoun. <https://apps.dtic.mil/dtic/tr/fulltext/u2/1053128.pdf>
- Department of Defense Chief Information Officer. (2015, September). *DOD program manager's guidebook for integrating the cybersecurity risk management framework (RMF) into the system acquisition life cycle*. [http://www.acqnotes.com/wp-content/uploads/2014/09/PM-Guidebook-for-Integrating-Cybersecurity-RMF-into-System-Acquisition-Life cycle-Sep-2015.pdf](http://www.acqnotes.com/wp-content/uploads/2014/09/PM-Guidebook-for-Integrating-Cybersecurity-RMF-into-System-Acquisition-Life-cycle-Sep-2015.pdf)
- Department of Defense Chief Information Officer. (2007). *DOD information assurance certification and accreditation process (DIACAP)*. Department of Defense. <http://www.acqnotes.com/Attachments/DOD%20Instruction%208510.01.pdf>
- Department of Defense Chief Information Officer. (2019). *DoDI 8500.01 Cybersecurity*. DOD. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf
- Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics – balancing operational security spending. *Information Technology & People*, 32(5), 1318–1342. <https://doi.org/10.1108/ITP-05-2018-0252>
- Fielder, A., Konig, S., Panaousis, E., Schauer, S., & Rass, S. (2017). Uncertainty in cyber security investments. *ArXiv:1712.05893 [Cs]*. <http://arxiv.org/abs/1712.05893>
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2015). Comparing decision support approaches for cyber security investment. *ArXiv:1502.05532 [Cs]*. <http://arxiv.org/abs/1502.05532>

- Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 40(1), 183–199. <https://doi.org/10.1111/risa.12891>
- Garvey, P. R., Moynihan, R. A., & Servi, L. (2013). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering*, 16(3), 313–328. <https://doi.org/10.1002/sys.21236>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, 07(02), 49–59. <https://doi.org/10.4236/jis.2016.72004>
- Jenab, K., Khoury, S., & LaFevor, K. (2016). Flow-graph and Markovian methods for cyber security analysis. *International Journal of Enterprise Information Systems (IJEIS)*, 12(1), 59–84. <https://doi.org/10.4018/IJEIS.2016010104>
- Karthikeyan, R., Venkatesan, K. G. S., & Chandrasekar, A. (2016). A comparison of strengths and weaknesses for analytical hierarchy process. *Journal of Chemical and Pharmaceutical Sciences*, 9(3), 4.
- Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, 14(3), 417–431. <https://doi.org/10.1108/TG-11-2019-0112>
- Kitchenham, B. (2007). *Guidelines for performing systematic literature reviews in software engineering*. https://dlwqtxts1xzle7.cloudfront.net/35830450/2_143465389588742151.pdf?1417739236=&response-content-disposition=inline%3B+filename%3DSystematic_Literature_Reviews_SLR.pdf&Expires=1611151939&Signature=HAgKl0qY7H8oqodj-G1Q~438CtgJhc9gldMude7XEa0BOvnIYmSOSu7gyiV~s7Ez-~sElpJqB4AfUWHmV~z1RgAjLWbCBciugHx~2LpHsDYxMvhcsYP80vS6iK93AFGpGEcLWVb4Irr~3LmqZFFc3hrPjOqgfGZ6ZJe8KCIviPK5nO0-ws1pjeAE2vLUB0kbYs741zUX7E1-7NtdXQ1VBVzR0ZqJveBwprBEQ7XnvR2RNOR63ca9AXThFwCyIkI0blxnkwgT8VMXVyaMxS6IC431mCFQxz7tGnnyKvjyBk7UaFn3DE1pBdKjXHiTAbctXVJYmHrMn0KqtBYPU~gQw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
- Koong, K. S., Merhi, M. I., & Sun, J. (2013). Push and pull effects of homeland information security incentives. *Information Management & Computer Security*, 21(3), 155–176. <https://doi.org/10.1108/IMCS-04-2012-0022>
- Leenen, D. L. (2018). *ICCWS 2018 13th international conference on cyber warfare and security*. Academic Conferences and publishing limited.
- Marlatt, G. E. (n.d.). *Research guides: Search basics: home*. Retrieved January 4, 2021, from <https://libguides.nps.edu/search/home>
- McElroy, P. A. (2019). *Identifying key meta-narrative themes across public-sector enterprise risk management literature in support of the Marine Corps' future implementation* [Master's Thesis]. NPS Archive: Calhoun. <http://hdl.handle.net/10945/64025>

- Miaoui, Y., & Boudriga, N. (2019). Enterprise security investment through time when facing different types of vulnerabilities. *Information Systems Frontiers*, 21(2), 261–300. <https://doi.org/10.1007/s10796-017-9745-3>
- Office of the Inspector General. (2019). *DOD OIG semiannual report to the congress October 1, 2018 through March 31, 2019.pdf*. Department of Defense. <https://media.defense.gov/2019/Dec/11/2002223355/-1/-1/1/dod%20oig%20semiannual%20report%20to%20the%20congress%20october%201,%202018%20through%20march%202019.pdf>
- Office of the Under Secretary of Defense (Comptroller). (2020). *National defense budget estimates for FY 2021* (p. 300). https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/FY21_Green_Book.pdf
- Oxford English Dictionary. (n.d.). In *Oxford English Dictionary*. Retrieved February 16, 2021, from <https://www.oed.com/>
- Paul, J. A., & Wang, X. (Jocelyn). (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, 122, 113069. <https://doi.org/10.1016/j.dss.2019.05.009>
- Pfleeger, S. L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software*, 25(1), 35–42. <https://doi.org/10.1109/MS.2008.4>
- Pinto, A., Tatar, U., Keskin, O., Kucukkaya, G., Kucukozyigit, A. C., Poyraz, O. I., & Alfaqiri, A. (2020). Cybersecurity acquisition framework based on risk management: Economics perspective. *Acquisition Research: Creating Synergy for Informed Change*, 13. <https://event.nps.edu/conf/app/researchsymposium/unsecured/dlprop/659/52>
- President of the United States. (2017). *National security strategy*. Department of Defense. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- Rabii, A., Assoul, S., Ouazzani, T. K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information & Computer Security*, 28(4), 627–644. <https://doi.org/10.1108/ICS-03-2019-0039>
- SAGE research methods. (n.d.). In *SAGE Research*. Retrieved February 16, 2021, from <https://methods.sagepub.com/>
- Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: A systematic literature review. *Information Systems Frontiers*, 19(5), 1205–1228. <https://doi.org/10.1007/s10796-016-9648-8>
- Secretary of Defense. (2018). *The DOD cyber strategy*. Department of Defense. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
- Smith, M. D., & Pate-Cornell, M. E. (2018). Cyber risk analysis for a smart grid: How smart is smart enough? A multiarmed bandit approach to cyber security investment. *IEEE Transactions on Engineering Management*, 65(3), 434–447. <https://doi.org/10.1109/TEM.2018.2798408>

- Speciale, S., & Kendall, K. (2018). Financial management's key role in cybersecurity. *Defense Acquisition, XLVII*(5), 47.
- Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75*, 49–62. <https://doi.org/10.1016/j.dss.2015.04.011>
- Tavana, M., Khosrojerdi, G., Mina, H., & Rahman, A. (2019). A hybrid mathematical programming model for optimal project portfolio selection using fuzzy inference system and analytic hierarchy process. *Evaluation and Program Planning, 77*, 101703. <https://doi.org/10.1016/j.evalprogplan.2019.101703>
- Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*(2), 147–156. <https://doi.org/10.1016/j.dcan.2019.01.005>
- Tuma, K., Calikli, G., & Scandariato, R. (2018). Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software, 144*, 275–294. <https://doi.org/10.1016/j.jss.2018.06.073>
- Wilson, J. (2018). *Exploring a threat-focused acquisition methodology using multi-criteria decision methods to increase delivery-cycles for information and cyber-related capabilities* [Doctorate, George Washington University]. GWU Archive: GW ScholarSpace. https://scholarspace.library.gwu.edu/concern/gw_etds/5425k9888?locale=en
- Zeng, K. (2016). *Exploring cybersecurity requirements in the defense acquisition process* [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations and Theses Global. <https://search.proquest.com/docview/1822511621?pq-origsite=gscholar>
- Zhang, Y., Wang, L., Xiang, Y., & Ten, C. (2016). Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. *IEEE Transactions on Power Systems, 31*(6), 4379–4394. <https://doi.org/10.1109/TPWRS.2015.2510626>

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California