ODU-CE-21-018

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Cybersecurity Acquisition Framework Based on Risk Management: Economics Perspective

December 30, 2020

C. Ariel Pinto, Associate Professor
Omer Faruk Keskin, Graduate Research Assistant
Goksel Kucukkaya, Graduate Research Assistant
Omer Ilker Poyraz, Graduate Research Assistant
Abdulrahman Alfaqiri, Graduate Research Assistant
Old Dominion University

Unal Tatar, Assistant Professor
University at Albany, State University of New York

Ali Can Kucukozyigit, Lecturer
Arizona State University

Disclaimer: This material is based upon work supported by the Naval Postgraduate School Acquisition Research Program under Grant No. HQ0034-18-1-0010. The views expressed in written materials or publications, and/or made by speakers, moderators, and presenters, do not necessarily reflect the official policies of the Naval Postgraduate School nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact the Acquisition Research Program (ARP) via email, arp@nps.edu or at 831-656-3793.

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School

Abstract

Cyber attacks continuously target organizations, however, the mitigation actions taken for defense are not sufficiently effective. Ability to compute the cost of attacks is crucial to assess the effectiveness of countermeasure investments. In this study, we developed a framework to have a well-informed decision-making process in cybersecurity acquisition by evaluating the business impact caused by the operability losses of assets. We tested the developed framework using various attack and mitigation scenarios. The findings suggest that using a simulation approach to calculate the business impact of cyber attacks provides the ability to support decision-making process.

THIS PAGE LEFT INTENTIONALLY BLANK

About the Authors

C. Ariel Pinto, Ph.D., Associate Professor of Engineering Management and Systems Engineering at Old Dominion University. His works focus on multi-disciplinary approaches to risk management in engineered systems and systems engineering, including the effects security and non-security related disruptions in the continuity of operation of organizations and information systems.

Unal Tatar, Ph.D., is currently an Assistant Professor of Cybersecurity at the College of Emergency Preparedness, Homeland Security, and Cybersecurity, University at Albany. He has 15+ years of cybersecurity experience of cybersecurity in government, industry, and academia. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar's research is funded by NSF, NSA, DOD, NATO, and Society of Actuaries. Dr. Tatar holds a BSc degree in Computer Engineering, an MS degree in Cryptography, and Ph.D. in Engineering Management and Systems Engineering. His main topics of interest are information/cybersecurity risk management, cyber resiliency, cyber insurance, and blockchain.

Ali Can Kucukozyigit, Ph.D., is a faculty of Industrial Engineering at Arizona State University. His research focus on project management, risk management, leadership skills, and information operations. He specializes on quantitative methods to identify how the importance of a leadership skills change as per the organizational level and environment.

Omer Faruk Keskin is a Ph.D. Candidate in the Engineering Management and Systems Engineering Department at Old Dominion University. He holds a Master of Science degree in Engineering Management and a bachelor's degree in Systems Engineering. He is a graduate research assistant and has worked in several projects, including grant proposal writing phase. His main fields of research include enterprise cyber risk management and risk quantification, modeling, and simulation.

Goksel Kucukkaya is a Ph.D. Candidate in the Engineering Management and Systems Engineering Department at Old Dominion University. His research focuses on

developing risk quantification methodology for augmented anomaly detection in cybersecurity.

Omer Ilker Poyraz, Ph.D., in the Engineering Management and Systems Engineering Department at Old Dominion University. His research focuses on estimating the cost of data breach incidents on large organizations.

Abdulrahman Alfaqiri is a Ph.D. Candidate in the Engineering Management and Systems Engineering Department at Old Dominion University. His research focuses on determining factors that influences organizational resilience against various types of disruptive events.

ODU-CE-21-018

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Cybersecurity Acquisition Framework Based on Risk Management: Economics Perspective

December 30, 2020

C. Ariel Pinto, Associate Professor
Omer Faruk Keskin, Graduate Research Assistant
Goksel Kucukkaya, Graduate Research Assistant
Omer Ilker Poyraz, Graduate Research Assistant
Abdulrahman Alfaqiri, Graduate Research Assistant
Old Dominion University

Unal Tatar, Assistant Professor
University at Albany, State University of New York

Ali Can Kucukozyigit, Lecturer
Arizona State University

Disclaimer: This material is based upon work supported by the Naval Postgraduate School Acquisition Research Program under Grant No. HQ0034-18-1-0010. The views expressed in written materials or publications, and/or made by speakers, moderators, and presenters, do not necessarily reflect the official policies of the Naval Postgraduate School nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

THIS PAGE LEFT INTENTIONALLY BLANK

Table of Contents

THIS PAGE LEFT INTENTIONALLY BLANK

List of Figures

List of Tables

THIS PAGE LEFT INTENTIONALLY BLANK

List of Acronyms and Abbreviations

FDNA	Functional Dependency Network Analysis
SOD	Strength of Dependency
COD	Criticality of Dependency
CIA	confidentiality, integrity, and availability
NIST	National Institute of Standards and Technology
A	Asset
BP	Business Process

THIS PAGE LEFT INTENTIONALLY BLANK

Introduction

Risk management against cyber threats is gaining more importance with the increasing number of successful cyber attacks. The consequences of cyber attacks can be so severe that an organization may not even survive the attack. Consequences may involve data breach, loss of data and equipment, disruption of operations and business, and reputation damage. Cybersecurity investments are considered to be implemented by decision-makers to reduce the likelihood and impact of cyber attacks. Acquisition of cybersecurity products and services is not the same as any other asset since it is difficult to measure a cybersecurity product's benefits.

This report presents a scenario-based framework to calculate the cost of a cyber attack and assess the effects of mitigation actions to inform cybersecurity acquisition process (i.e., cybersecurity investment). A cyber attack targets an organization's assets; however, its impact on the business cannot be directly measured. Decision-makers of an organization should identify the dependencies among the assets and the business processes to understand how an asset's degradation would impact the business. The developed framework adapts Functional Dependency Network Analysis (FDNA) to calculate a cyber attack's impact by considering these dependencies. Based on the internal dependency relationships, the cascading impacts can be calculated using the developed framework, and a more accurate estimate of the cost of attacks can be made.

The organization of this paper is as follows: Section 2 provides a literature review analysis conducted to determine how the systems are required, what challenges and issues exist in cybersecurity acquisition, and what solutions exist to address these challenges. Section 3 provides the details about the methodology by presenting the original FDNA, how it is modified to serve the purpose of cybersecurity acquisition, and calculating the cost of an attack. Section 4 presents the implementation of the developed framework on a sample organization along with the simulation results. In Section 5, the validation phase is presented. Finally, Section 6 is the conclusion.

THIS PAGE LEFT INTENTIONALLY BLANK

Literature Review Analysis

A systematic approach is employed in the literature review phase, as depicted in Figure-1. First, the search keywords are identified: cyber, security, cybersecurity, acquisition, impact, damage, mission, business, risk, assessment, and situational awareness. Second, the search keys-words are used to search through the previously-identified databases (see Figure 1), and the resulting articles are screened for their relevance to the objectives of the systematic literature review. Third, relevant articles that fit the purpose of the systematic literature review are further reviewed and aggregately analyzed based on three research questions, namely:

Q1: How are systems being acquired?

Q2: What are challenges and issues in cybersecurity acquisition?

Q3: What are solutions to the challenges in cybersecurity acquisition?

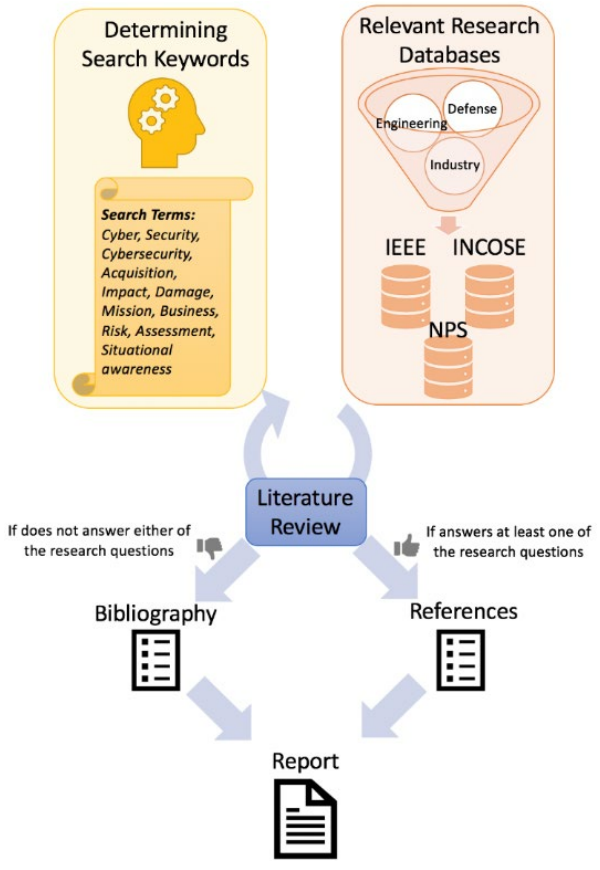


Figure 1. Systematic literature review process

Challenges and Implications in Literature

Cybersecurity in system development and acquisition system life cycle worked by several scholars (Bayuk & Horowitz, 2011). However, some significant challenges and implications have been more recently identified. We listed important issues related to cyber risk analysis from an acquisition perspective.

1. *Measuring cyber risk*: There is a lack of consistent and widely accepted means of measuring current and future cyber risk pertaining to the organizational mission (Erickson, 2016).
2. *Enterprise-level view*: There is a lack of enterprise-level cybersecurity acquisition strategy that includes technical and non-technical aspects that appeal to organizational executives (Bradley & Norville, 2018). For example, Bradley and Norville (2018) discussed some organizational and technical challenges that federal agencies face during cybersecurity modernization processes. One of these challenges is that legacy systems are very interconnected, and any modernization process that is not comprehensive will pose the entire critical infrastructure to a severe threat. Furthermore, the process of replacing legacy systems should involve all stakeholders at all levels within the relevant federal agencies to ensure secure and smooth modernization.
3. *Inclusion of threat and vulnerabilities*: Another challenge is the inclusion of threats and inherent vulnerabilities when choosing among mitigation strategies and solutions (Bastow, 2014; Huff et al., 2018; Shaw & Tremaine, 2018a; Nussbaum & Berg, 2020). Bastow (2014) indicated that entirely relying on commercial off-the-shelf products exposes industrial control systems to new threats such as malicious code and spyware as well as human errors and physical disruptions. Furthermore, constantly emerging vulnerabilities may lead to cascading failures (Reid & Rhodes, 2018; Karabacak & Tatar, 2014). However, no direct solution method has been identified.
4. *Support for a risk-based decisions:* There is a need for a risk-based decision-making framework for cybersecurity strategy prioritization that considers all components of risk assessment –threat, vulnerability, and consequences. Besides, current methods fail to integrate across different domains of cyber systems (Ganin et al., 2017).
5. *Differences among organizations:* There are differences in risk profile between organizations. Vertically integrated organizations typically carry higher risk profiles than horizontally integrated organizations (Kaestner et al., 2016).
6. *Emerging business models:* Unknown software architectural representations, heterogeneous software IP licenses, and emerging new business models also pose a challenge (Scacchi & Alspaugh, 2015, 2016).
7. *Data sharing:* Difficulties in sharing data causes problems to cybersecurity acquisition risk assessment (Smullen & Breaux, 2016).

Proposed Solutions in Literature

Proposed solutions can be grouped into two primary categories; 1) organizational and 2) methodological. Organizational solutions pertain to recommendations that specify changes are needed at an enterprise or organizational level. The acquisition process can be addressed at the executive level and not explicitly at the technical level. On the other hand, methodological solutions pertain to recommendations that were considered to affect the technical rather than the organizational level of the acquisition process and explicitly describe changes in the method of acquisition. Findings are detailed in the following sections and summarized in Table 1.

Organizational Solutions:

Some of the organizational recommendations are primarily guiding principles. Bayuk & Horowitz (2011) provides an architectural approach to systems security engineering to strengthen current approaches. Bradley and Norville (2018) identified classes of new reusable system security solutions and an architectural framework based on reusing the patterns of solutions. Ganin et al. (2017) presented a decision-analysis-based approach that quantifies threat, vulnerability, and consequences through assessing the overall utility of cybersecurity management alternatives. Other recommendations also provide methodological ways to implements such recommendations (Garvey et al., 2013, Reid & Rhodes, 2018, and Shaw & Tremaine, 2018b).

Bahsi et al. (2018) did a comprehensive literature review on how the impacts of cyber actions can be assessed from the perspective of enterprise missions or business processes. They concluded that impact assessment is vital towards various cyber-security processes such as risk assessment, incident handling, and event monitoring or vulnerability management. They also concluded that a socio-technical, systemic framework that evaluates the propagation of impacts should be used to evaluate economic impacts.

These organizational solutions can be summarized by the following guiding principles:

1. Early identification of security requirements,
2. Integration of security requirements in technology selection, testing, and verification processes,
3. Added emphasis on the potential use of the system in the cloud environment,
4. System developers to be knowledgeable and skilled in cybersecurity in their respective sub-system purview,
5. Representation of systems (both existing and to-be-acquired) in three layers: mission, service, and asset.

Methodological Solutions:

The methodological recommendations include:

1. *Decision analytics* - Multi-criteria risk and decision-analytic approach and Pareto optimal economic return are used to calculate the investment amount based on the impact of cyber-attacks and merit points of countermeasures. The tabletop approach was used in which investments were made using expertise regarding merit points of countermeasure and impact of cyber intrusion.
2. *Cost-Tradeoff analysis* - Tradeoff method to minimize cost while maintaining the desired level of security effectiveness against adversaries who would exploit those vulnerabilities, e.g., Huff et al. (2018) employed Model-based Systems Engineering approach to assess the vulnerabilities and determine alternatives to secure their system (Scacchi & Alspaugh, 2016; Keskin et al. 2018).
3. *Failure propagation* - Quantification of failure propagation potential during conceptual design prior to selecting candidate architectures, e.g., O'Halloran et al. (2017) also considered a dependency of assets while calculating failure,
4. *Advance tools* - Using sophisticated information technology tools such as artificial intelligence (i.e., deep autoencoder neural network supported by Blockchain technology) that would perform cyber threats analysis and incident management with much fewer manual operations, e.g., Graf & King (2018).

Table 1. Summary of proposed solutions, both organizational and methodological.

Organizational proposed solutions	Methodological proposed solutions
• Early identification • Integration • Cloud environment • Skilled and knowledgeable workforce • Layered enterprise representation	• Decision analytics • Cost-Tradeoff analysis • Failure propagation • Advance tools

Potential research areas

Based on the outcomes of the systematic literature review, Cybersecurity Acquisition Framework was Developed in this project. The framework has the following key deliverables:

1. Application of FDNA on cyber risk assessment,
2. Method to calculate monetary value of cybersecurity risk, and
3. Economics based risk management framework for effective cybersecurity acquisition.

The following research areas provide synergistic alignment between the results of the systematic literature review.

1. How can FDNA be applied towards representing ripple effects of cybersecurity failure throughout an enterprise?
2. How can the resulting representation of ripple effects enable economic (i.e., monetary) measurement of risk of cybersecurity failure?
3. How can all these be included into the Acquisition Process?

THIS PAGE LEFT INTENTIONALLY BLANK

Research Methodology

In this section, details of the methodology of this study are presented. The following subsections provide details for FDNA developed by Garvey and Pinto (2009), how it is adapted to the cybersecurity domain in order to assess impact propagation among the entities of an enterprise, and how the cost of attacks can be calculated.

Original FDNA

FDNA is a methodology based on graph theory. It helps decision-makers assess the ripple effects among supplier and dependent nodes of an enterprise. The purpose of FDNA is to assess how the failure of some systems (entities) affects the operability of other dependent systems within an enterprise. The enterprise is visualized as a directed graph based on the dependencies among entities, which represent specific functionalities within the operation of the enterprise (Garvey and Pinto, 2009).

Enterprise is represented as a capability portfolio, which is a functional dependency network where the capabilities are fed by the functions of the enterprise. A functional dependency network consists of feeder nodes, receiver nodes, and feeder & receiver nodes, as depicted in Figure 2. Feeder nodes are also called supplier nodes, parent nodes, or leaf nodes. The operation of feeder nodes does not rely on any other nodes. Receiver nodes are also called dependent nodes or child nodes. Receiver nodes' operation is dependent on other nodes, and no other nodes are dependent on them. Other nodes are both dependent on some other nodes and predecessor to some other nodes.

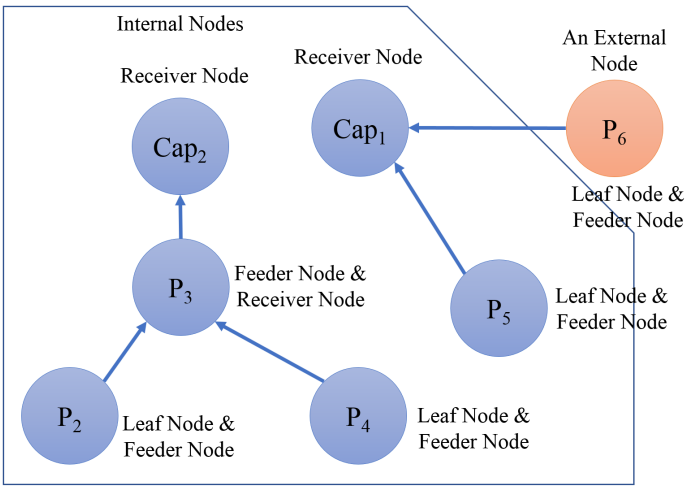


Figure 2. FDNA capability portfolio. Adapted from Tatar (2019)

FDNA Algebra

In FDNA, a dependency exists when the operation of a receiver node partially or fully depends on a feeder node. The dependency of node j on node i is illustrated in Figure 3, where P_i and P_j indicate the operability of nodes i and j, respectively.

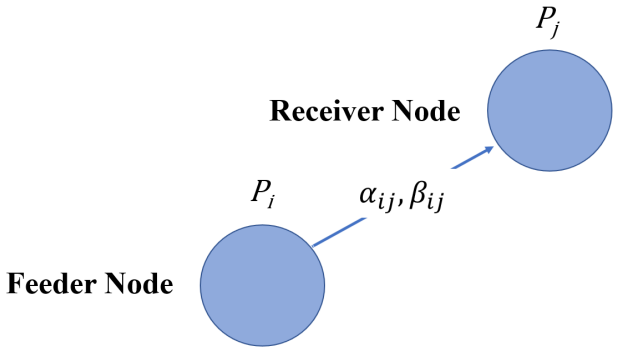


Figure 3. FDNA Dependency relationship

Operability indicates to what extend the node performing its function, i.e., its level of performance. If a node is fully functioning, its operability is 100 utils, and if it is completely inoperable, its operability value is 0 utils. This measure is not necessarily linear. The physical (countable/measurable) output does not have to affect the operability value linearly. This relationship between the measurable output of the system and the operability value of the relevant FDNA node is determined based on the perception and expectations of the user. In FDNA algebra, operability values are employed as the

measure of performance for each node rather than the physical output of the relevant system.

$$0 \leq Pi, Pj \leq 100$$

The dependency relationship is determined by two parameters, α and β values. The α and β values represent the Strength of Dependency (SOD) and Criticality of Dependency (COD), respectively. SOD is about how much of the receiver node's operation depends on the operation of the feeder node. COD is determined based on the degree that the dependent node's operation would degrade in the case that the receiver node is not operable for a long time. α can have values from zero to one, and β can have a value from zero to one hundred.

$$0 \leq \alpha_{ij} \leq 1\,, 0 \leq \beta_{ij} \leq 100$$

Operability of a receiver node, P_j, is determined by a function of the values of strength of dependency (α), criticality of dependency (β), and operability of the feeder node (P_i), as follows:

$$P_j = f\left(\alpha_{ij}, \beta_{ij}, P_i\right), 0 \leq \alpha_{ij} \leq 1\,, 0 \leq \beta_{ij} \leq 100\,, 0 \leq Pi, Pj \leq 100$$

Where P_j and P_i are operability of nodes j and i, respectively, α_{ij} is SOD fraction, and β_{ij} is COD parameter. The operability of the receiver node is determined as the minimum of SODPj and CODPj.

$$P_j = Min\left(SODP_j, CODP_j\right)$$

These values are computed using the following equation:

$$P_j = Min\left(\alpha_{ij} P_i + 100\left(1 - \alpha_{ij}\right), Pi + \beta_{ij}\right)$$

In the case that there are n feeder nodes, $SODP_j$ is calculated by taking an average of $SODP_{ji}$ values for each feeder node, and $CODP_j$ is calculated by taking the minimum of $CODP_{ji}$ values for each feeder node.

$$SODP_j = Average\left(SODP_{j1}, SODP_{j2}, SODP_{j3}, \ldots, SODP_{jn}\right)$$

$$SODP_{ji} = \alpha_{ij} P_i + 100\left(1 - \alpha_{ij}\right)$$

$$CODP_j = Min\left(CODP_{j1}, CODP_{j2}, CODP_{j3}, \dots, CODP_{jn}\right)$$

$$CODP_{ji} = P_i + \beta_{ij}$$

Where $0 \leq \alpha_{ij} \leq 1$, $0 \leq \beta_{ij} \leq 100$, $0 \leq Pi, Pj \leq 100, i = 1,2,3, \dots, n$

How to assign α and β values

Determining the degree of dependency of nodes is an essential step of FDNA. Firstly, the strength of dependency fraction, α_{ij}, is determined. Then, the criticality of dependency parameter, β_{ij}, is determined.

The baseline operability level (BOL) is the operability value of a receiver node when its feeder node's operability is zero. In order to find the α value, the following question is asked: What is the operability value of the receiver node when its feeder node is wholly inoperable? The answer is equal to the baseline operability value. Baseline operability value equation from which the α_{ij} is retrieved is presented below:

$$Baseline\ Operability\ Level = 100\left(1 - \alpha_{ij}\right)$$

If the answer to the question is zero, then α_{ij} is zero; if the answer is 40, then α_{ij} is 0.6; if the answer is one hundred, then α_{ij} is zero. While the strength of dependency increases, the baseline operability level decreases, and vice versa. α_{ij} can have a value greater than or equal to zero and less than or equal to one.

The criticality of dependency indicates how the receiver node's operability degrades from its baseline operability level when the feeder node is inoperable in some extend. In calculations, this effect is considered as the receiver's operability level that is constrained by its feeders' operability levels. In this case, P_j cannot be higher than $P_i + \beta_{ij}$ for all feeder nodes. β_{ij} can have a value greater than or equal to zero and less than or equal to one hundred.

Previous Research Utilized FDNA

Functional Dependency Network Analysis (FDNA) has been successfully used in various applications such as characterization and examination of system of systems, cybersecurity, critical infrastructure, and navigation systems (Costa, McShane, & Pinto,

2015; Garrido-Pelaz, González-Manzano, & Pastrana, 2016; Garvey, Pinto, & Santos, 2014; Guariniello & DeLaurentis, 2014; Servi & Garvey, 2017; Wang, Zhang, & Li, 2014).

Previous research from diverse application areas show that FDNA can be implemented in cybersecurity domain to study the interdependent systems. Relationship among the elements of business and organization network can be modeled and simulated by implementing this approach.

Adapting FDNA for Cyber Impact Assessment

FDNA is modified in order to adapt to the cyber domain and conduct cybersecurity acquisition impact assessment. The modifications include introducing assets to business processes impact propagation model and inoperability impact propagation of confidentiality, integrity, and availability.

Impact Propagation from Assets to Business Processes

In order to measure the impact of cybersecurity acquisition, an organization needs to know how an asset contributes to the main processes that add value to the organization. This is because the return on investment on cybersecurity products and services can be observed as it affects the business processes. In order to make this assessment, impact propagation is needed to be analyzed among the entities of the organization. These entities are either assets or business processes. The corresponding definitions are provided below:

Business processes are the organizational goals that add value to the organization (Bahsi et al., 2018; Jakobson, 2011; Shameli-Sendi et al., 2016; Tatar, 2019).

Assets include any hardware, software, data, and people of the organization, and contribute to the realization of the business processes (Bahsi et al., 2018; Jakobson, 2011; Shameli-Sendi et al., 2016; Tatar & Karabacak, 2012)

Assets belong to the asset level, and business processes belong to the business process level. The operations of some assets depend on other assets. The viability of the business processes is dependent on the assets. A sample functional dependency network is depicted in Figure 4.

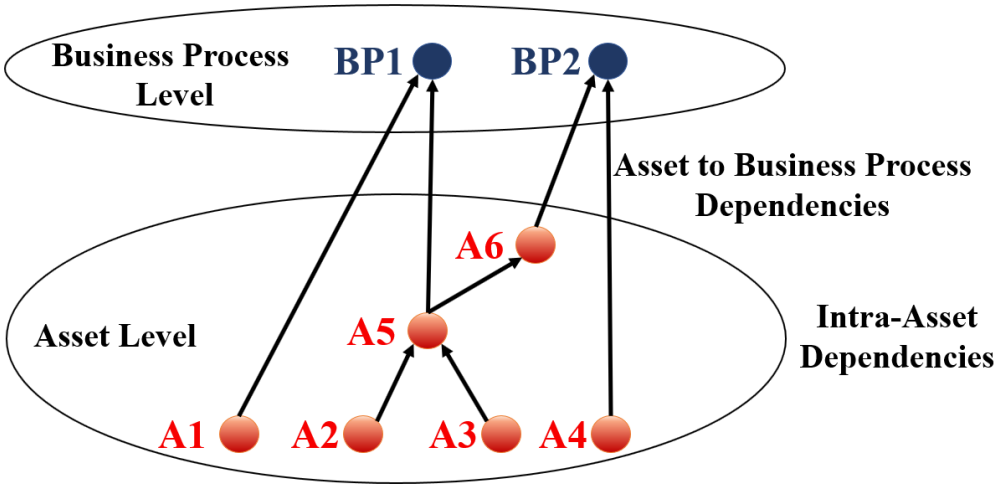


Figure 4. Dependency relationships among entities of an organization

Confidentiality, Integrity, and Availability Dependency

Generating a graph of an organization that depicts the dependency relationships is not sufficient to assess the impact propagation. Cybersecurity studies and practice heavily depend on confidentiality, integrity, and availability (CIA) concepts. National Institute of Standards and Technology (NIST) has established the CIA concept as a fundamental aspect of security controls and assessment (2018). NIST security controls "are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations."

Confidentiality means "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." (National Institute of Standards and Technology [NIST], 2018)

Integrity means "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity." (NIST, 2018)

Availability means "Ensuring timely and reliable access to and use of information." (NIST, 2018)

It is crucial to determine how the entities of an organization depend on each other from the perspective of confidentiality, integrity, and availability. The dependency relationship between the two nodes is presented in Figure 5.

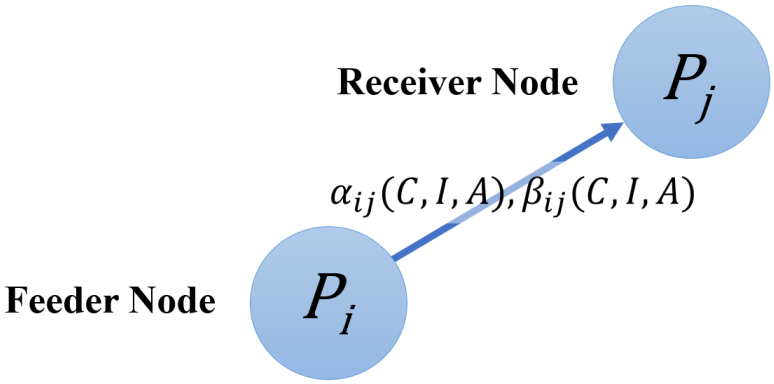


Figure 5. Dependency relationship between two nodes

The α and β values are separately assigned as it was discussed in Section 3.1.2 from confidentiality, integrity, and availability perspectives. Then, their average is taken as the α_{ij} and β_{ij} values.

$$\alpha_{ij}(C,I,A) = \frac{\alpha_{ij}(C) + \alpha_{ij}(I) + \alpha_{ij}(A)}{3}$$

$$\beta_{ij}(C,I,A) = \frac{\beta_{ij}(C) + \beta_{ij}(I) + \beta_{ij}(A)}{3}$$

After α and β values assigned, impact propagation assessment is conducted using the FDNA algebra.

Cost Calculation

Cost estimation is an integral part of management. Decisions related to risk management are not independent of the expected loss of a risk item. The expectation from a cybersecurity acquisition is a return on investment similar to other expenditures. However, mostly the return of cybersecurity is not a positive income. It is instead not to

be breached or continuing operation. Therefore, calculating the cost of a cyber risk event becomes crucial to anticipate the possible effects of a cybersecurity investment.

There are several loss items commonly experienced by the organizations that become a victim of cyber attacks. The cost of a cyber incident can be estimated by adding up these estimated loss items (Council of Economic Advisors, 2018).

Table 2. Cost items used to calculate cost of a cyber incident

Loss Items
Loss of Revenue
Loss of Data and Equipment
Loss of Intellectual Property
Cybersecurity Improvements
Court Settlement & fees
Customer protection
Regulatory Penalties
Forensics

To calculate the cost of cyber attacks, organizations need to estimate the cost items for each business process. For example, each business process has a different rate of revenue, and loss of operability for different business processes is not equal. These cost items can be determined based on scenarios, or an average value can be assigned. The method can be adjusted based on the characteristics of the industry sector, organization, and business process.

Implementation of the Developed Framework

This section provides guidance on how to implement the developed framework. Step by step guide is presented, and after that, the developed framework is implemented on a simulation network model along with the results of disruptions scenarios.

Phases to Implement the Methodology

1. **Identify the functional nodes**
    - 1.1. What are the main business processes of the organization? What are the areas that we focus on to make a profit or create value? (business processes/mission)
    - 1.2. Determine what assets play a role in facilitating each specific business process. (Assets)
    - 1.3. Determine what assets help other assets to function properly. (Other Assets)
2. **Come up with the functional dependency topology**
    - 2.1. Determine the existence of functional dependency among the nodes. (Arrows)
3. **Determine the input variables**
    - 3.1. For each dependency, determine the strength of dependency fraction value for Confidentiality, Integrity, and Availability. (Alpha)
    - 3.2. For each dependency, determine the criticality of dependency parameter for Confidentiality, Integrity, and Availability. (Beta)
    - 3.3. For each Business Process, determine the cost values. (Costs values)
4. **Compute the cost for the fully operable network scenario (Outputs/results/delivery)**
    - 4.1. For each node, input 100 for operability value.
    - 4.2. Analyze cascading impact propagation and calculate the operability of each node
    - 4.3. Plot the results
5. **Compute the cost for different disruption scenarios**
    - 5.1 Come up with different cyber attack scenarios, including diminishing operability values of different nodes partially or fully (Different input operability values for assets).
    - 5.2 Calculate costs with different input values based on the scenarios developed in 5.1 using the steps of phase 4.

6. **Compute the cost for different acquisition strategies**
    6.1. Come up with different acquisition strategies, such as improving security.
    6.2. Adjust the input values by going thru phase 4.
7. **Compare the outputs of different scenarios**
    7.1. Compare the results of steps 4.3, 5.2, and 6.2.

The phases above should be taken into consideration iteratively using a spiral development process (Figure 6). The first four phases are conducted repeatedly until the whole graph satisfactorily represents the functional network of the enterprise. Only after that, the last three phases are started being considered. Another spiral development process would be undertaken for the last three phases, too. Then, the outcomes of the approach would be discussed.

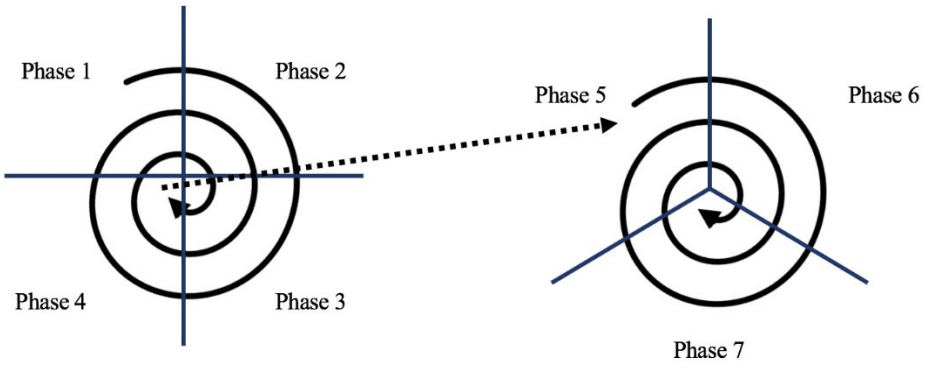


Figure 6. Spiral development process model for the implementation of the framework

Simulation Model and Scenarios

As a case study, the developed framework is applied to a sample organization by generating its simulation network model (Figure 7). The organization has three business processes that are dependent on the operation of 12 assets.

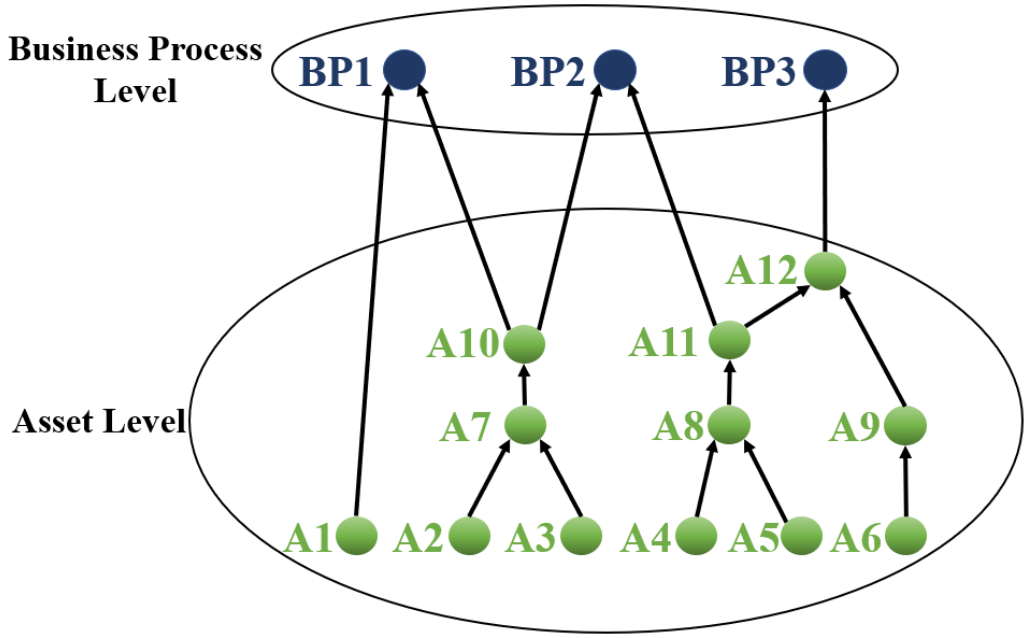


Figure 7. Simulation network

The functional dependency network presents how each business process is dependent on the assets. In order to keep the simulation simple, the α_{ij} and β_{ij} values were assigned equal for all dependency relationships, as provided in Table 3. These values indicate that the confidentiality and integrity of the network entities, including assets and business processes, are relatively more dependent on other entities.

Table 3. Values for Strength of Dependency and Criticality of Dependency

	α_{ij}	β_{ij}
Average	0.433	43.33
C	0.6	25
I	0.5	35
A	0.2	70

When all assets are fully operational, the operability values of both business processes are equal to one hundred, i.e., fully operable. Different disruption scenarios cause operability loss on the business processes:

1. In the first set of scenarios, only one asset is failed in each scenario.

2. In the second set of scenarios, pairs of two assets become inoperable at the same time.
3. In the third set of scenarios, groups of three assets become inoperable at the same time.
4. In the fourth set of scenarios, groups of five or six assets become inoperable at the same time.
5. In the fifth set of scenarios, a cybersecurity product, which is an antivirus software, is acquired for the assets, and its effects on the business processes are benchmarked.

For each disruption scenario, after the operability loss of each Business Process has been computed, cost calculation is done using the loss values for completely inoperable conditions presented in Table 4.

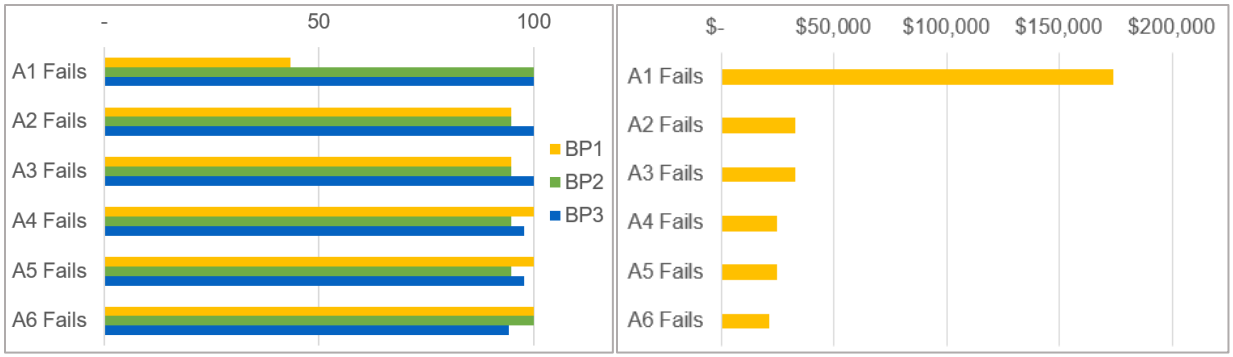
Table 4. Loss values of completely inoperable Business Processes[1]

Loss Item	BP1	BP2	BP3
Loss of Revenue	$ 45,000	$ 38,000	$ 51,000
Loss of Data and Equipment	$ 58,000	$ 52,000	$ 65,000
Loss of Intellectual Property	$ 92,000	$ 103,000	$ 113,000
Cybersecurity Improvements	$ 23,000	$ 32,000	$ 35,000
Court Settlement & fees	$ 55,000	$ 49,000	$ 62,000
Customer protection	$ 14,000	$ 12,000	$ 15,000
Regulatory Penalties	$ 11,000	$ 13,000	$ 15,000
Forensics	$ 9,000	$ 7,000	$ 8,000
TOTAL	$ 307,000	$ 306,000	$ 364,000

Only one Asset Becomes Inoperable

In this set, only one asset fails in each scenario. The cascading effects are analyzed, and the operability levels of each business process and the total cost of each incident scenario are presented in Figure 8.

[1] The data given represents the incurred costs when each business process fails and is generated by the authors to provide a realistic scenario.



(a) (b)

Figure 8. (a) Operability levels of business processes when one asset fails at a time. (b) Total costs of incidents when one asset fails at a time.

As it can be observed, the most significant impact on Business Process 1 (BP1) is caused by Asset 1 (A1). Its operability value decreases by 56.67 utils. The reason for this is that BP1 is directly dependent on A1. Therefore, any disruption in A1 shows a significant effect on BP1. Neither of the other scenarios results in a business process that is significantly affected. The cost of the incident if A1 fails is $173,967, and the scenario with the second largest cost is $32,614. This cost is caused by either A2 or A3 fails. Since A7 is dependent on each of these assets at the same rate, their effects are the same. The same concept applies for A4 and A5 since A8 is dependent on both of these assets with the same strength of dependency and criticality of dependency.

Pairs of Two Assets Become Inoperable

In this set, each pair of two assets fails simultaneously in each scenario. The cascading effects are analyzed, and the operability levels of each business process and the total cost of each incident scenario are presented in Figure 9.

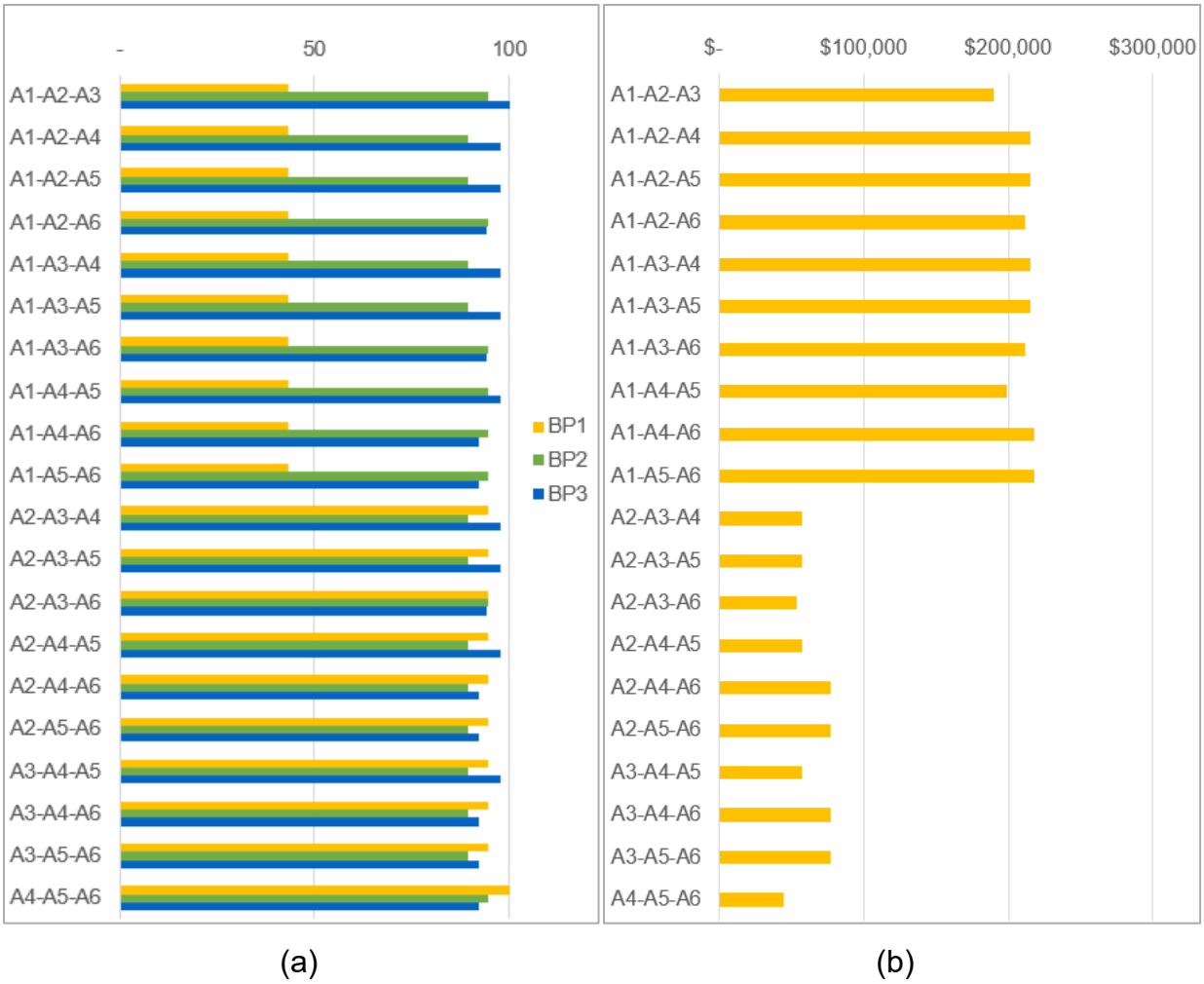
(a) (b)

Figure 9. (a) Operability levels of business processes when pairs of assets fail. (b) Total costs when pairs of assets fail.

As can be observed, the most significant impact on BP1 is caused by the inoperability of A1 and any of the other assets at the same time. Operability value of BP1 decreases by 56.67 utils, which is equal to the impact when only A1 is inoperable. The reason of this similarity is that FDNA dependencies are based on the weakest link rule (effect of A1 is greater than A10's). Based on the cost estimates, when A1 and A4 (or A5) fail to operate at the same time, the effect is the greatest compared to the others.

Groups of Three Assets Become Inoperable

In this set, each group of three assets fails simultaneously in each scenario. The cascading effects are analyzed, and the operability levels of each business process and the total cost of each incident scenario are presented in Figure 10.



(a) (b)

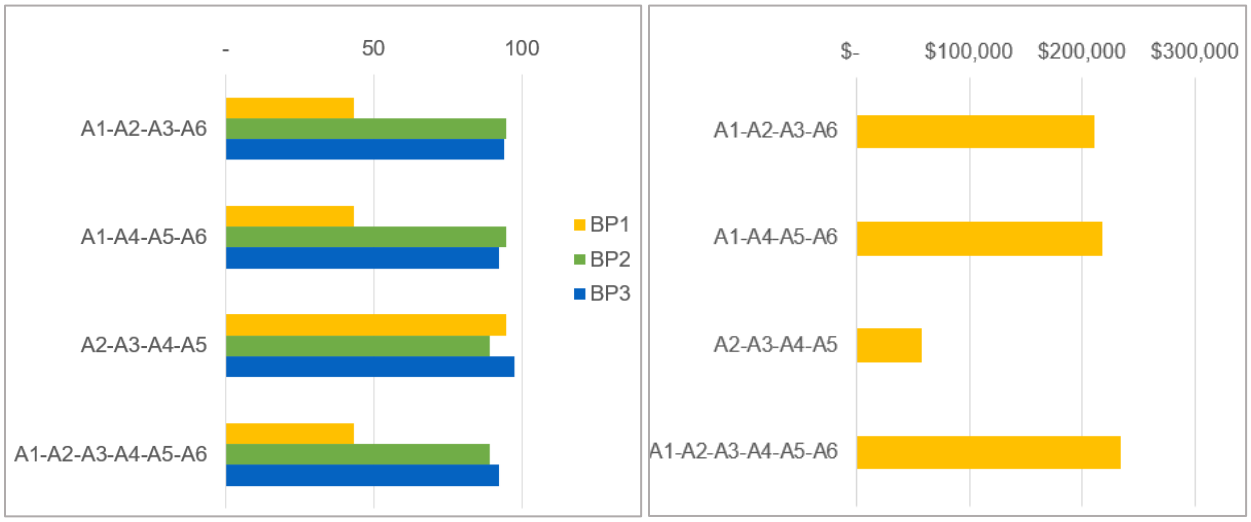
Figure 10. (a) Operability levels of business processes when groups of three assets fail. (b) Total costs when groups of three assets fail.

Similarly, the groups that include A1 have the same significant impact on the operability of BP1. For BP2 and BP3, it can be observed that the operability levels are slightly lower than the previous scenarios.

When A1, A4, and A6 become inoperable at the same time, the operability of BP1, BP2, and BP3 decreases to 43.33 utils, 94.68 utils, and 92.37 utils, respectively. This causes a total cost of $218,005. Inoperability of A1, A5, and A6 also cause the same impact since A4 and A5 have the same effect on the network.

Groups of Four or More Assets Become Inoperable

In this set, each group of three assets fails simultaneously in each scenario. The cascading effects are analyzed, and the operability levels of each business process and the total cost of each incident scenario are presented in Figure 11.



(a) (b)

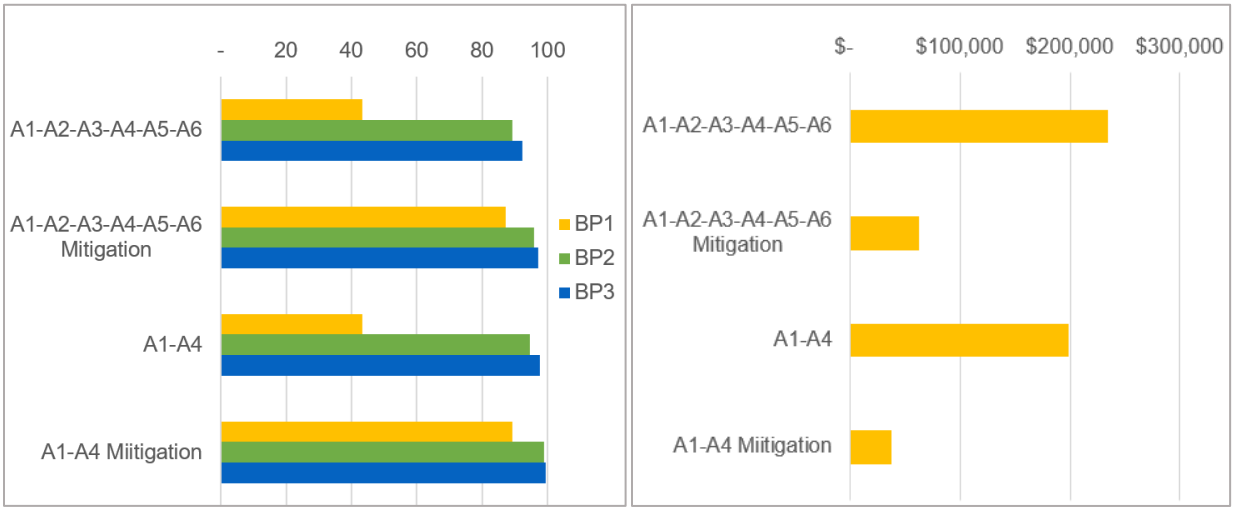
Figure 11. (a) Operability levels of business processes when groups of four or more assets fail. (b) Total costs when groups of four or more assets fail.

The groups that include A1 have a significant impact on the operability of BP1. When A1, A2, A3, A4, A5, and A6 become inoperable at the same time, the operability of BP1, BP2, and BP3 decreases to 43.33 utils, 89.36 utils, and 92.37 utils, respectively. This causes a total cost of $234,285. It is expected that this scenario causes the highest cost among all scenarios since it includes the failure of all six assets at the same time.

Mitigation Scenarios

In this set, two mitigation scenarios are compared to the relevant scenarios without mitigation action. One scenario includes failure of all six assets, and the other scenario includes failure of the A1 and A4 pair simultaneously. The mitigation action is the acquisition of a cybersecurity product such as an antivirus program that reduces the impact of the attack on the target assets. Without the mitigation action, the operability of such assets reduces to zero. However, after the mitigation is implemented, the attack

reduces the operability to 50 utils instead of zero. The cascading effects are analyzed based on this difference, and the operability levels of each business process and the total cost of each incident scenario are presented in Figure 12.



(a) (b)

Figure 12. (a) Operability levels of business processes for two mitigation scenarios compared to the relevant scenarios. (b) Total costs for two mitigation scenarios compared to the relevant scenarios.

The first mitigation scenario is compared to when A1, A2, A3, A4, A5, and A6 become inoperable at the same time. In the mitigation scenario, the operability of BP1, BP2, and BP3 decreases to 87.13 utils, 95.93 utils, and 97.08 utils, respectively. The estimated cost is $62,567.

The second mitigation scenario is compared to when A1 and A4 become inoperable concurrently. In the mitigation scenario, the operability of BP1, BP2, and BP3 decreases to 89.17 utils, 98.98 utils, and 99.56 utils. The estimated cost is $37,975.

Analysis and Results

FDNA is used in these scenarios to calculate the operability loss of Business Processes after some of the Assets become inoperable. After the cascading effects are computed, the total cost of the incident is calculated for each scenario based on the impact on the operability levels of the Business Processes.

In the first mitigation scenario, the operability of A1, A2, A3, A4, A5, and A6 decrease by 50 at the same time instead of 100 (without mitigation). As a result, the operability of BP1, BP2, and BP3 decreases to 87.13 utils, 95.93 utils, and 97.08 utils, respectively. Without mitigation, the operability levels are 43.33 utils, 89.36 utils, and 92.37 utils, respectively. Furthermore, the cost is reduced from $234,285 to $62,567 by 73%.

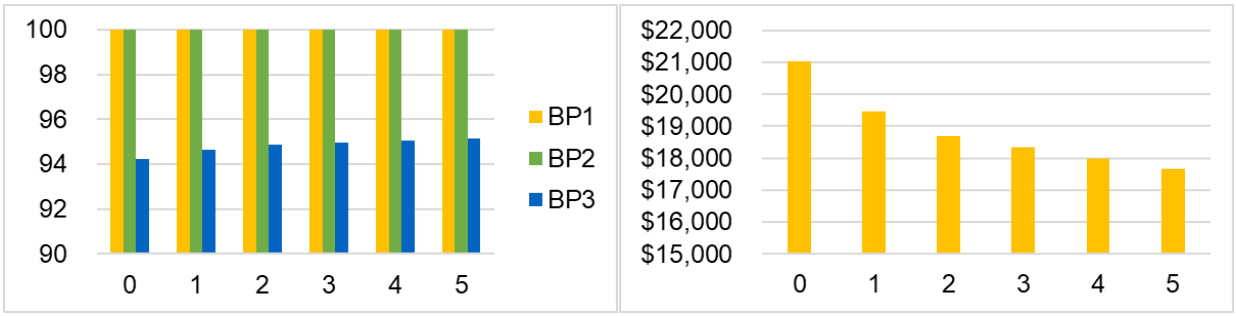
In the second mitigation scenario, the operability of A1 and A4 decrease by 50 at the same time instead of 100 (without mitigation). As a result, operability of BP1, BP2, and BP3 decreases to 89.17 utils, 98.98 utils, and 99.56 utils, respectively. Without mitigation, the operability levels are 43.33 utils, 94.68 utils, and 97.69 utils, respectively. Moreover, the cost is reduced from $198,639 to $37,975 by 81%.

As can be seen from these scenarios, the mitigation approach saves more than $160,000 in case that such attacks occur. This approach can provide an estimate on the return on investment for the decision-makers.

Validation

In order to validate the developed framework, a sensitivity analysis was conducted on the simulation network model. For each scenario in sensitivity analysis, the input value slightly changed to monitor the differences in the output of the model. Sensitivity analysis was conducted for the scenarios that A6 fails, and the pair of A2 and A3 fails simultaneously. For each group, the lower limit and upper limit were investigated.

In the first set of scenarios, input was the lower limit of the operability value of A6. The output values are presented in Figure 13.

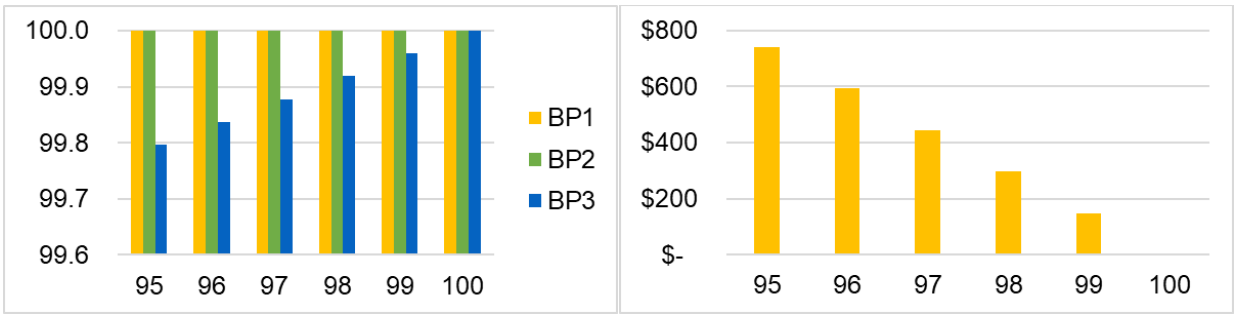


(a) (b)

Figure 13. (a) Operability levels of business processes for sensitivity analysis at lower limit when A6 fails. (b) Total costs for sensitivity analysis at lower limit when A6 fails.

For each scenario in this set, operability values of 0, 1, 2, 3, 4, and 5 were given to A6. Note that the horizontal axis does not cross the vertical axis at the value of zero to ease reading the graphs. When operability of A6 is equal to 0, operability of BP3 decreases to 94.66 utils, and the cost is $21,031. When operability of A6 is equal to 5 utils, operability of BP3 decreases to 95.15 utils, and the cost is $17,657.

In the second set of scenarios, input was the upper limit of the operability value of A6. The output values are presented in Figure 14.

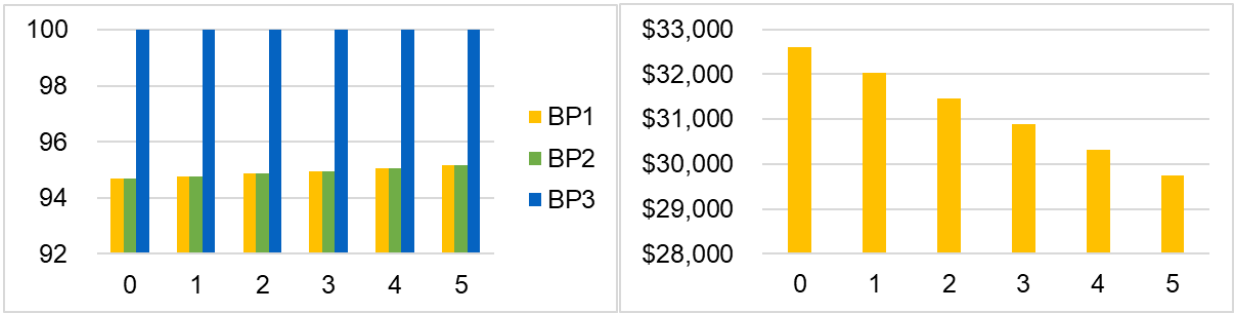


(a) (b)

Figure 14. (a) Operability levels of business processes for sensitivity analysis at upper limit when A6 fails. (b) Total costs for sensitivity analysis at upper limit when A6 fails.

For each scenario in this set, operability values of 95 utils, 96 utils, 97 utils, 98 utils, 99 utils, and 100 utils were given to A6. When operability of A6 is equal to 95 utils, operability of BP3 decreases to 99.80 utils, and the cost is $740. When operability of A6 is equal to 99 utils, operability of BP3 decreases to 99.96 utils, and the cost is $148.

In the third set of scenarios, input was the lower limit of the operability values of A2 and A3. The output values are presented in Figure 15.



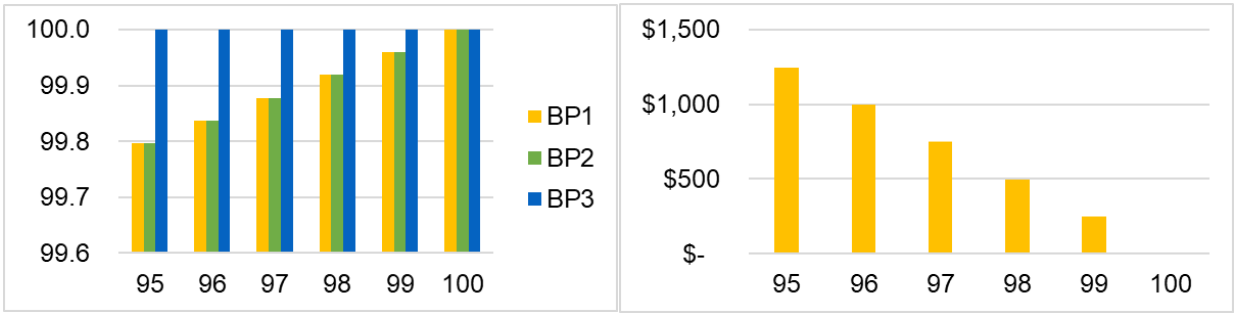
(a) (b)

Figure 15. (a) Operability levels of business processes for sensitivity analysis at lower limit when A2 and A3 fails simultaneously. (b) Total costs for sensitivity analysis at lower limit when A2 and A3 fails simultaneously.

For each scenario in this set, operability values of 0, 1 util, 2 utils, 3 utils, 4 utils, and 5 utils were given to A2 and A3. When operability of A2 and A3 are equal to 0, operability of BP1 and BP2 decreases to 96.68 utils, and the cost is $32,614. When

operability of A2 and A3 are equal to 5 utils, operability of BP1 and BP2 decreases to 95.15 utils, and the cost is $29,736.

In the last set of scenarios, input was the lower limit of the operability values of A2 and A3. The output values are presented in Figure 16.



(a) (b)

Figure 16. (a) Operability levels of business processes for sensitivity analysis at lower limit when A2 and A3 fails simultaneously. (b) Total costs for sensitivity analysis at lower limit when A2 and A3 fails simultaneously.

For each scenario in this set, operability values of 95 utils, 96 utils, 97 utils, 98 utils, 99 utils, and 100 utils were given to A2 and A3. When operability of A2 and A3 are equal to 95 utils, the operability of BP1 and BP2 decreases to 99.80 utils, and the cost is $1,247. When operability of A2 and A3 are equal to 99 utils, operability of BP1 and BP2 decreases to 99.96 utils, and the cost is $249.

According to the sensitivity analysis results, a gradual change in the input causes an expected gradual change in the output values.

THIS PAGE LEFT INTENTIONALLY BLANK

Conclusion

This report presents a framework developed to compute the cost of a cyber attack scenario to be able to provide the ability to conduct simulations to determine the effects of different acquisition scenarios. This risk-informed acquisition approach for cybersecurity investments can help organizations strengthen the network to reduce the likelihood and consequences of cyber attacks.

This report provides the details of how FDNA is adapted to the cybersecurity domain. The developed framework can help organizations calculate the cascading impacts through the internal dependencies to estimate the cost of different attack scenarios. As the simulation scenarios present, the cost of a cyber attack can be significant, and it can be reduced by implementing various acquisition scenarios. This framework can help the decision-makers decide which scenario provides the most return on investment.

THIS PAGE LEFT INTENTIONALLY BLANK

References

Bahşi, H., Udokwu, C. J., Tatar, U., & Norta, A. (2018, March). Impact Assessment of Cyber Actions on Missions or Business Processes: A Systematic Literature Review. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*(p. 11). Academic Conferences and publishing limited.

Bastow, M. D. (2014). Cyber security of the railway signalling & control system. In 9th IET International Conference on System Safety and Cyber Security

Bayuk, J. L., & Horowitz, B. M. (2011). An architectural system engineering methodology for addressing cyber security. Systems Engineering, 14(3), 294-304.

Bradley, I. D., & Norville, B. (2018, April). An enterprise cybersecurity strategy for federal critical infrastructure modernization. In 2018 Integrated Communications, Navigation, Surveillance Conference (ICNS) (pp. 1C4-1). IEEE.

Costa, A., McShane, M. K., & Pinto, C. A. (2015). Investigating Interbank Contagion with Agent-based Modeling and Functional Dependency Network Analysis (FDNA).

Council of Economic Advisors. (2018). *The cost of malicious cyber activity to the US economy.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Erickson, B. (2016). Cybersecurity Figure of Merit. In Proceedings of the Thirteenth Annual Acquisition Research Symposium (pp. 323–324). Naval Postgraduate School, Monterey, CA

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis.

Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). Shall we collaborate?: A model to analyse the benefits of information sharing. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (pp. 15-24). ACM.

Garvey, P. R., & Pinto, C. A. (2009). Introduction to functional dependency network analysis. In The MITRE Corporation and Old Dominion, *Second International Symposium on Engineering Systems*, MIT, Cambridge, Massachusetts (Vol. 5).

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.

Garvey, P. R., Pinto, C. A., & Santos, J. R. (2014). Modelling and measuring the operability of interdependent systems and systems of systems: advances in methods and applications. *International Journal of System of Systems Engineering*, *5*(1), 1-24.

Graf, R., & King, R. (2018, May). Neural network and blockchain based technique for cyber threat intelligence and situational awareness. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 409-426). IEEE.

Guariniello, C., & DeLaurentis, D. (2014). Communications, information, and cyber security in systems-of-systems: Assessing the impact of attacks through interdependency analysis. *Procedia Computer Science*, *28*, 720-727.

Huff, J., Medal, H., & Griendling, K. (2018). A model-based system engineering approach to critical infrastructure vulnerability assessment and decision analysis. Systems Engineering.

Jakobson, G. (2011) "Mission Cyber Security Situation Assessment Using Impact Dependency Graphs", *Proceedings of the 14th International Conference on Information Fusion (FUSION)*, pp 1-8.

Kaestner, S., Arndt, C., & Dillon-Merrill, R. (2016). The Cybersecurity Challenge in Acquisition. Acquisition Research Symposium. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1016746.pdf

Karabacak, B., & Tatar, Ü. (2014). Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. *Critical Infrastructure Protection*, *116*, 63.

Keskin, O., Tatar, U., Poyraz, O., Pinto, A., & Gheorghe, A. (2018, March). Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 343). Academic Conferences and publishing limited.

National Institute of Standards and Technology. (2018). *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy* (NIST SP 800-37 Revision 2; Special Publication). https://doi.org/10.6028/NIST.SP.800-37r2

Nussbaum, B., & Berg, G. (2020). Cybersecurity implications of commercial off the shelf (COTS) equipment in space infrastructure. *Space infrastructures: From risk to resilience governance*, 91-99.

O'Halloran, B. M., Papakonstantinou, N., Giammarco, K., & Van Bossuyt, D. L. (2017, July). A Graph Theory Approach to Functional Failure Propagation in Early Complex Cyber-Physical Systems (CCPSs). In *INCOSE International Symposium* (Vol. 27, No. 1, pp. 1734-1748).

Reid, J., & Rhodes, D. H. (2018). Applying Cause-Effect Mapping to Assess Cybersecurity Vulnerabilities in Model-Centric Acquisition Program Environments.

Reid, J., & Rhodes, D. H. (2018). Assessing vulnerabilities in model-centric acquisition programs using cause-effect mapping.

Scacchi, W., & Alspaugh, T. A. (2015). Achieving Better Buying Power Through Acquisition of Open Architecture Software Systems for Web-Based and Mobile Devices. Acquisition Research Symposium. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/53560/UCI-AM-16-010.pdf?sequence=1

Scacchi, W., & Alspaugh, T. A. (2016). Achieving Better Buying Power through Acquisition of Open Architecture Software Systems Volume I. Acquisition Research Symposium.

Servi, L. D., & Garvey, P. R. (2017). Deriving global criticality conditions from local dependencies using functional dependency network analysis (FDNA). *Systems Engineering*, *20*(4), 297-306.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M., 2016. Taxonomy of information security risk assessment (ISRA). *Computers & security*, *57*, pp.14-30.

Shaw, P. & Tremaine, R. (2018a). Cybersecurity: Converting Shock into Action (Part 1). Acquisition Research Symposium. Retrieved from https://calhoun.nps.edu/handle/10945/58776

Shaw, P., & Tremaine, R. (2018). *Cybersecurity: Converting Shock into Action (Part 2)*. Calhoun. https://calhoun.nps.edu/handle/10945/63021

Smullen, D. & Breaux, T. (2016). Improving Security in Software Acquisition with Data Retention Specifications. Acquisition Research Symposium. Retrieved from https://calhoun.nps.edu/handle/10945/58892

Tatar, U. (2019). Quantifying Impact of Cyber Actions on Missions or Business Processes: A Multilayer Propagative Approach.

Tatar, Ü., & Karabacak, B. (2012, June). An hierarchical asset valuation method for information security risk analysis. In *International Conference on Information Society (i-Society 2012)* (pp. 286-291). IEEE.

Wang, Y., Zhang, W. X., & Li, Q. (2014). Functional dependency network analysis of security of navigation satellite system. In *Applied Mechanics and Materials* (Vol. 522, pp. 1192-1196). Trans Tech Publications.

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net