2020-04-27

Cybersecurity Acquisition Framework Based on Risk Management: Economics Perspective

Kucukkaya, Goksel; Keskin, Omer; Poyraz, Omer; r, Ali Can Kucukozyigit; Pinto, C. Ariel; Tatar, Unal

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/64762

SYM-AM-20-058

Proceedings

of the

Seventeenth Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 13–14, 2020

Published: April 13, 2020

Approved for public release; distribution is unlimited.

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

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

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 any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Cybersecurity Acquisition Framework Based on Risk Management: Economics Perspective

C. Ariel Pinto—is an 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 of security and non-security related disruptions in the continuity of operation of organizations and information systems.[cpinto@odu.edu]

Unal Tatar—is currently an Assistant Professor of Cybersecurity at the College of Emergency Preparedness, Homeland Security, and Cybersecurity, University at Albany. He has more than 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. Tatar's research is funded by NSF, NSA, ONR, and the Society of Actuaries. Tatar holds a BSc degree in Computer Engineering, an MS degree in Cryptography, and a PhD in Engineering Management and Systems Engineering. His main topics of interest are information/cybersecurity risk management, cyber resiliency, cyber insurance, and blockchain. [utatar@albany.edu]

Omer Keskin—is a PhD candidate in the Engineering Management and Systems Engineering Department at Old Dominion University. He holds a master's 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. [okesk001@odu.edu]

Ali Can Kucukozyigit—is a faculty of Industrial Engineering at Arizona State University. His research focuses 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 org level and environment. [Ali.Kucukozyigit@asu.edu]

Goksel Kucukkaya—is a PhD 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. [gkucu001@odu.edu]

Omer Ilker Poyraz—is a PhD candidate 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. [iegri001@odu.edu]

Abdulrahman Alfaqiri—is a PhD candidate in the Engineering Management and Systems Engineering Department at Old Dominion University. His research focuses on determining factors that influence organizational resilience against various types of disruptive events. [aalfa001@odu.edu]

Abstract

Investments in the cyber domain are subject to constraints that may be similar to those in other domains, such as cost and effectiveness. However, cyber is a dynamic domain where the effectiveness and efficiency of investments are harder to measure. The interdependency of assets poses an additional challenge to make decisions on investments for the cyber domain. Therefore, organizations need to answer hard questions: whether, how much, and when to invest in cybersecurity. Analyzing the attack surface of a system or an enterprise in cyberspace, prioritizing assets according to their business values, and quantifying cybersecurity risk in monetary values would help to make better decisions while choosing a risk management strategy. The aim of this article is to develop a risk-informed cybersecurity investment decision model by considering the ripple effects in an organization based on the Functional Dependency Network Analysis (FDNA) methodology. Several simulations are conducted to test the effectiveness of the developed model.

Introduction

The acquisition of cybersecurity products has different characteristics than other equipment and services. For example, a production machine that is acquired has measurable inputs and outputs that can be compared with the existing systems and other available systems on the market. Cybersecurity products and services typically do not generate anything, but rather prevent unwanted cyber incidents from occurring. It leads to the point that when nothing happens, it actually means that the cybersecurity products and services are doing their jobs well. With the uncertainty of the likelihood of an attack occurring, assessing the impact of an attack and reducing its possible consequences gains more importance.

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 since the return on investment of cybersecurity products and services can be observed as it affects the business processes. The purpose of this study is to provide a methodology to quantify the impact propagation from assets of an organization to its business processes.

The sections of this study are summarized as follows: Literature Review on Calculating Economic Value of Cyber Risk and Cost of Cyber Incidents provides a literature review relating to the challenges of risk analysis methods and calculating the economic value of risk. The Method section gives details about the developed methodology. The Simulation and Results section presents simulation results, and the Conclusion section concludes the study.

Literature Review on Calculating Economic Value of Cyber Risk and Cost of Cyber Incidents

Information security economics and cybersecurity investment have been the focus of academic studies for years. The number of publications has been increasing due to escalating expenditures and loss from a security breach apart from the technical problems. Scholars suggest different methods to help organizations decide how to invest in cybersecurity to protect operational excellence and intellectual property. Prominent studies to increase the effectiveness of cybersecurity investments are reviewed below.

Previous work has addressed several types of problems. For example, Gordon and Loeb (2002) investigate the amount to invest in cybersecurity and determine that a small fractional amount of the expected loss is optimal. Arora, Hall, Pinto, Ramsey, and Telang (2004) suggest taking a risk management approach to evaluate information security solutions. They indicate that security managers should consider a risk-based return on investment (ROI) method to decide how to invest in cybersecurity to allow for the many uncertainties in the cyber domain. Other works apply various methods to determine optimal cybersecurity investment. For example, Cavusoglu, Raghunathan, S., & Yue (2008) and Fielder, Panaousis, Malacaria, Hankin, and Smeraldi (2016) compare game theory and optimization for benchmarking the efficiency of cybersecurity investments.

Cyber defense is often applied to comply with standards and best practices, which is an expensive task that requires investment in people, processes, and technology (Tatar, Çalik, Çelik, & Karabacak, 2014). Investments in the cyber domain are subject to constraints, such as cost and effectiveness, which may appear to be similar to decisions in more traditional domains. However, cyber is a dynamic risk with the effectiveness of investments being complex and unpredictable. For example, not all vulnerabilities will be exploited, but the potential remains until updates or patches have been successfully performed. These situations create questions for organizations on whether, how much, when, and how to invest in cybersecurity.

Morse and Drake (2012) developed a methodology to cope with acquisition risk. To make risk assessment more realistic and objective, they proposed a methodology to quantify acquisition risks through data-driven monetization. Cybersecurity is not within the scope of their study, but the core is calculating risk in monetary values as in this research. Shultz and Wydler (2015) studied the integration of cybersecurity into the acquisition life cycle, which involves a shift from bolt-on to built-in security. They describe how the government is moving from compliance-based requirements to a risk-based cybersecurity management framework to integrate cybersecurity into program acquisition and execution support. Erickson (2016) proposed that the Navy should develop a holistic scoring of cybersecurity standards/controls to optimize cybersecurity investments in a constrained environment. Kaestner et al. (2016) recommend that assets at risk must first be inventoried and used to estimate the potential losses of a cyberattack, which is a goal of the case study portion of this paper.

Research on the topics of the economics of cyber risk and cyber insurance—the primary method of risk transfer—has been increasing. This highlights the relevance of the topic from both a practical and an academic perspective (Eling & Schnell, 2016). Current methods commonly put more emphasis on technology and less on people, processes, and socioeconomic risk factors (Spears, 2005; Tatar et al., 2016). Major risk assessment approaches, such as the ISO/IEC 27001 and 27002 standards, are designed based on security control domains and focus more on an asset's security posture while ignoring preparedness towards a set of high-risk loss scenarios (Ruan, 2017). One of the major problems of actuaries working in the insurance sector or enterprise risk management is the quantification of cyber risk. Most security companies keep incident and loss data as proprietary to maintain a competitive advantage (Ruan, 2017). Subsequently, there is not enough data to employ statistical methods and mathematical models for appropriate calculations and predictions. This scarcity of data leads analysts to rely on scenario approaches rather than the use of the classical stochastic modeling (Lloyd's, 2015). For Rakes et al. (2012), employing expert judgment to define worst-case scenarios and estimate their likelihood for high-impact IT security breaches is a more efficient approach. A fast-changing technology environment requires a modeling approach that dynamically measures risk (Eling & Schnell, 2016).

Cybersecurity requires a risk-informed approach to make effective decisions. CISOs need to increase the effectiveness of securing organizations from cyber threats by providing information in a form that allows corporate boards and top management to make optimal cybersecurity investments. The next section provides a case study that illustrates a quantitative approach for making decisions on risk management techniques to use for a cyberattack.

Method

In this study, the Functional Dependency Network Analysis (FDNA) developed by Garvey and Pinto (2009) is adapted to the cybersecurity domain in order to assess impact propagation among the entities of an enterprise. In this section, we introduce the FDNA method and explain how it is adapted to cybersecurity.

Original FDNA

Functional Dependency Network Analysis (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 & 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 and receiver nodes, as it is depicted in Figure 1. 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.

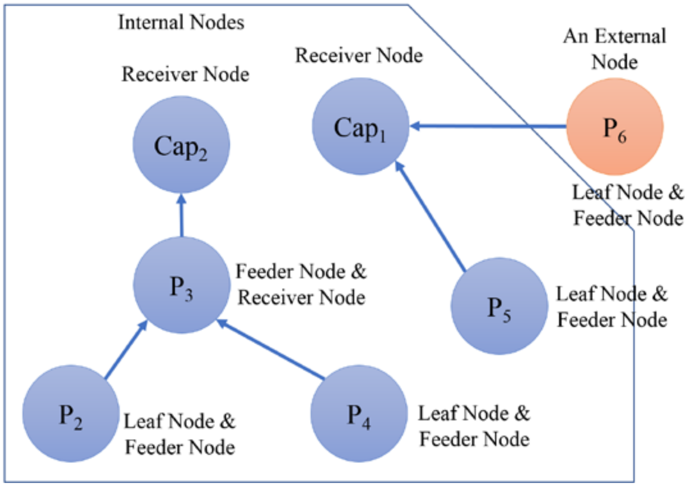

Figure 1. FDNA Capability Portfolio.
Tatar (2019).

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 2, where P_i and P_j indicate the operability of nodes *i* and *j*, respectively.

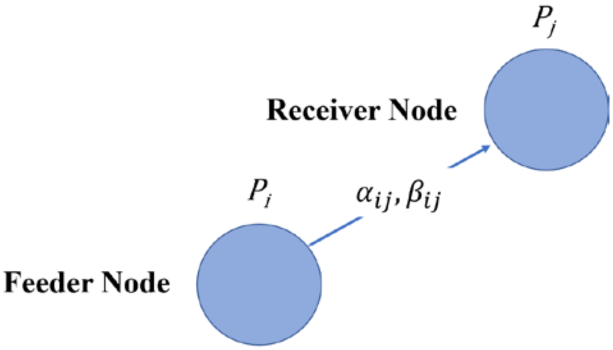

Figure 2. FDNA Dependency Relationship

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 0 to 1, and β can have a value from 0 to 100.

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

Operability of a receiver node, P_j, is determined by a function of values of α, β, and operability of the feeder node, 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 fraction. 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 COD t is calculated by taking the minimum of $CODP_{ji}$ values for each feeder node.

$$SODP_j = Average\left(SODP_{j1}, SODP_{j2}, SODP_{j3}, \dots, SODP_{jn}\right)$$
$$SODP_{ji} = \alpha_{ij}P_i + 100\left(1 - \alpha_{ij}\right)$$

$$CODP_j = Min\left(CODP_{j1}, CODP_{j2}, CODP_{j3}, \dots, CODP_{jn}\right)$$
$$CODP_{ji} = P_i + \beta_{ij}$$

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 parameter, 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 0, then α_{ij} is 0; if the answer is 40, then α_{ij} is 0.6; if the answer is 100, then α_{ij} is 0. 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 0 and less than or equal to 1.

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 0 and less than or equal to 100.

Adapting FDNA for Cyber Impact Assessment

FDNA is modified in order to adapt 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. The reason for this is that 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 needs 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 (Bahşi, Udokwu, Tatar, & Norta, 2018; Jakobson, 2011; Shameli-Sendi, Aghababaei-Barzegar, Cheriet, 2016).

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

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 3.

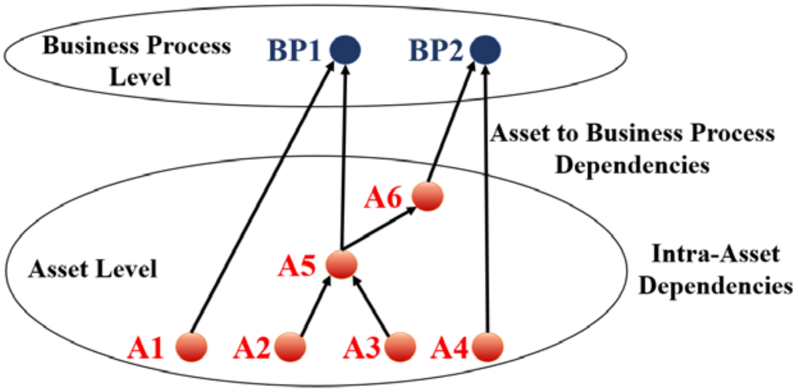

Figure 3. Dependency Relationships Among Entities of an Organization

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. The National Institute of Standards and Technology (NIST; 2013) has established the CIA concept as a fundamental aspect of security controls and assessment. 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” (NIST, 2013).

Integrity means “guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity” (NIST, 2013).

Availability means “ensuring timely and reliable access to and use of information” (NIST, 2013).

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 4.

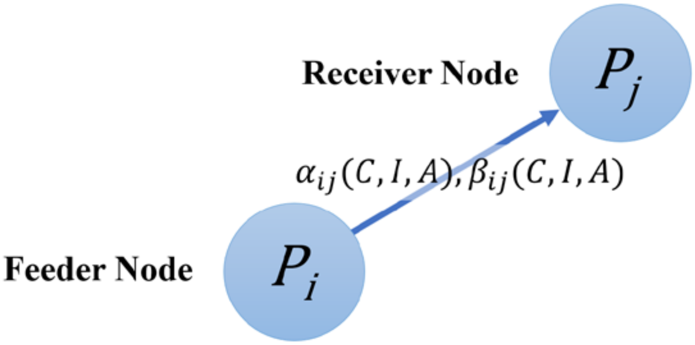

Figure 4. Dependency Relationship Between Two Nodes

The α and β values are separately assigned as it was discussed in the How to Assign α and β Values section 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.

Simulation and Results

The developed model is simulated in a sample organization. Simulations were conducted on the network presented in Figure 5. This network consists of six assets, and the organization has two business processes.

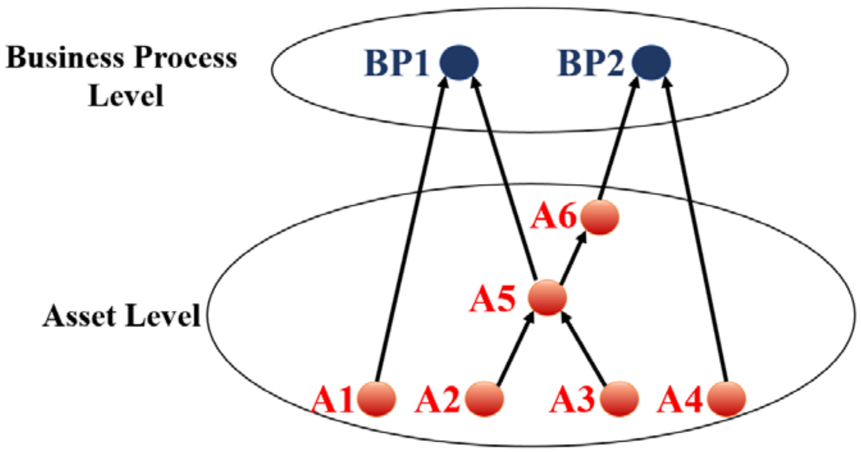

Figure 5. Simulation Network

Functional dependencies among the assets and how they relate to the business processes are presented in Figure 5. 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 1. These numbers indicate that the confidentiality and integrity of the network entities, including assets and business processes, are relatively more dependent on other entities.

Table 1. and Values for the Dependencies

	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 100 (i.e., fully operable). Different disruption scenarios cause operability loss on the business processes. In the first scenario, only one asset is failed. In the second scenario, two assets become inoperable at the same time. In the third scenario, three or four assets become inoperable. In the fourth scenario, a cybersecurity product, an antivirus software, is acquired for the assets, and its effects on the business processes are benchmarked.

Even though all the assets look the same in importance, the simulation scenarios show that some, among others, have a more critical position within the functional dependency network that causes them to be more important than others when ripple effects are taken into consideration.

Only One Asset Becomes Inoperable

In this scenario, one asset fails at a time, and their impact propagation is calculated based on these inputs. The resulted impact on the business processes is presented in Figure 6 for comparison.

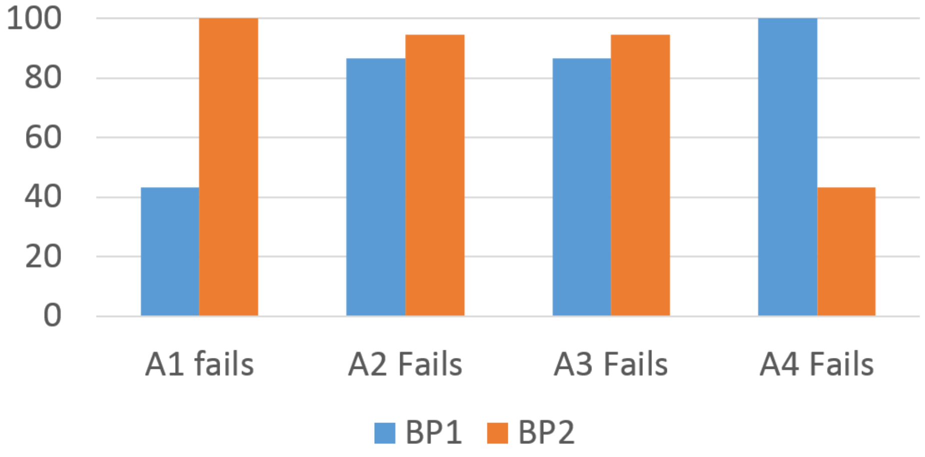

Figure 6. Only One Asset Becomes Inoperable

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. On the other hand, BP2 is affected significantly when A4 becomes inoperable. Neither BP1 nor BP2 is significantly affected when A2 or A3 fails to operate.

Two Assets Become Inoperable Simultaneously

In this scenario, two assets fail at the same time, and their impact propagation is calculated based on these inputs. The resulted impact on the business processes is presented in Figure 7 for comparison.

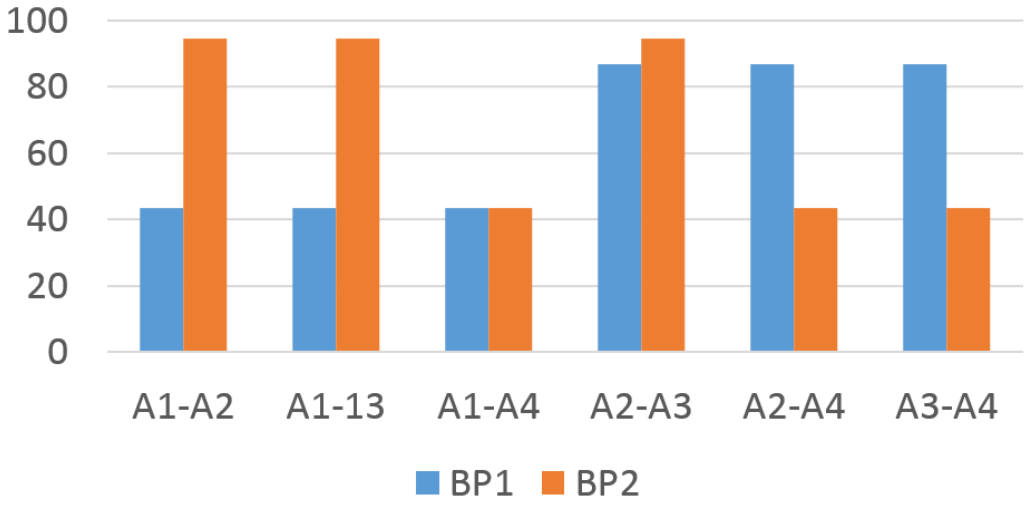

Figure 7. Two Assets Become Inoperable

As can be observed, the most significant impact on both Business Process 1 (BP1) and BP2 is caused by the inoperability of Asset 1 (A1) and A4 at the same time. Their operability values decrease by 56.67. When A2 or A3 fails to operate at the same time, the effect is much less than the inoperability of the other pairs.

Three or Four Assets Become Inoperable Simultaneously

In this scenario, three or four assets fail at the same time, and their impact propagation is calculated based on these inputs. The resulted impact on the business processes is presented in Figure 8 for comparison.

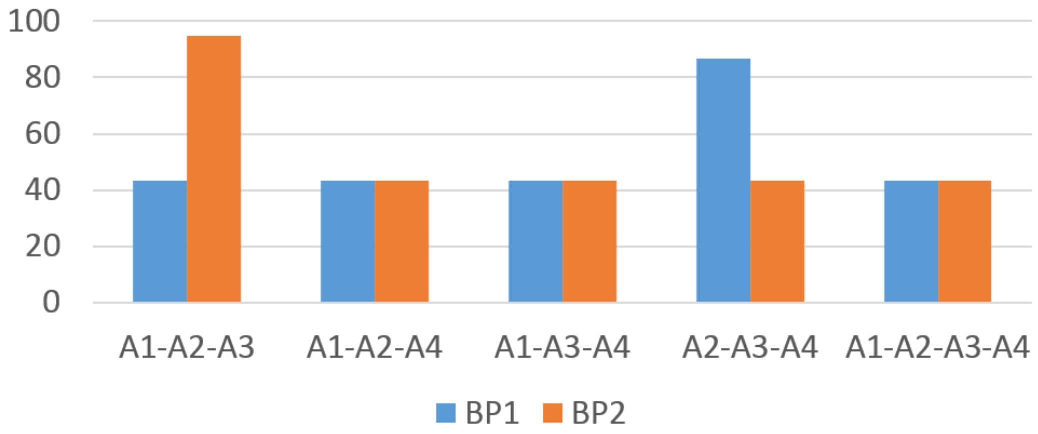

Figure 8. Three or Four Assets Become Inoperable

As it can be observed, the most significant impact on both Business Process 1 (BP1) and BP2 is observed in the cases that Asset 1 (A1) and A4 becomes inoperable at the same time regardless of A2 and A3. Their operability values decrease by 56.67. The similarities in the numbers and the critical assets are mainly caused by taking the α and β values for all dependency relations.

Mitigation Scenario Applied

In this scenario, a risk mitigation strategy is applied to the simulation network. Suppose that the organization acquires an antivirus product. This product prevents an asset from becoming wholly inoperable when an attack occurs; instead its operability decreases to 50. The resulted impact on the business processes is compared with the scenario without mitigation action in Figure 9.

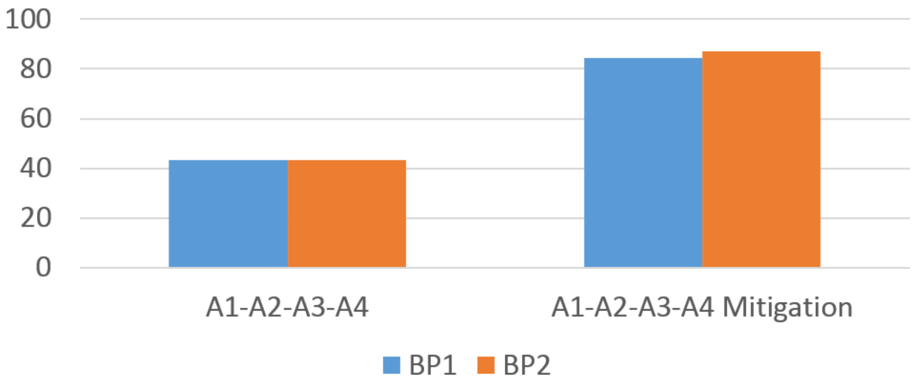

Figure 9. Outcomes of Risk Mitigation Action When Four Assets Become Inoperable

In Figure 10, outcomes of the same mitigation action are compared with the case that only A1 and A4 become entirely inoperable.

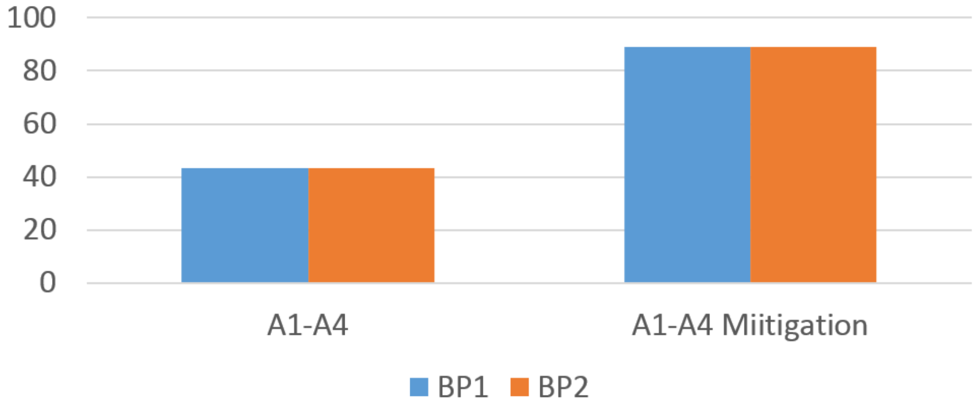

Figure 10. Outcomes of Risk Mitigation Action When A1 and A4 Become Inoperable

The mitigation action has a significant effect, even if it is not a solution that completely prevents an attack (Figures 9 and 10). Even after the acquisition of such products, operability values of assets can be decreased by 50 utils, the operability of the business processes only decreases by almost 11 utils.

Conclusion

In order to assess the impact of possible cyber-attacks, decision-makers of an organization should consider the organization not only from an asset perspective but also from a business process perspective. The relationships among the assets and the business processes should be determined by considering how critical a business process is for the viability of the organization.

Return on investment for the acquisition of cybersecurity products or services should be assessed by considering how it affects the business processes in addition to the assets of the organization. C-level decision-makers of an organization such as chief information security officer, chief information officer, and chief risk officer prefer considering the impact on the business processes in order to benchmark return on investment among several mitigation options.

The developed risk-informed cybersecurity investment decision model quantifies impact by considering the ripple effects in an organization. Simulations that are conducted to test the effectiveness of the developed model show that even though all the assets look the same in importance, some of them are more critical because of the ripple effects that occur when they become inoperable.

References

Arora, A., Hall, D., Pinto, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT Professional*, *6*(6), 35–42.

Bahşi, H., Udokwu, C. J., Tatar, U., & Norta, A. (2018). 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.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems*, *25*(2), 281–304. Retrieved from https://doi.org/10.2753/MIS0742-1222250211

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. Retrieved from https://doi.org/10.1016/j.dss.2016.02.012

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

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457.

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. In *Proceedings of the 13th Annual Acquisition Research Symposium*. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1016746.pdf

Lloyd's. (2015). Business blackout—The insurance implications of a cyber attack on the U.S. power grid. Retrieved from http://www.lloyds.com/news-and-insight/risk-insight/library/society-andsecurity/businessblackout

National Institute of Standards and Technology (NIST). (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(53), 8–13.

Nussbaum, B., & Berg, G. (2020). Cybersecurity implications of commercial off the shelf (COTS) equipment in space infrastructure. In U. Tatar, A. V. Gheorghe, O. F Keskin, & J. Muylaert (Eds.), *Space infrastructures: From risk to resilience governance* (pp. 91–99). Amsterdam, Netherlands: IOS Press.

Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega*, *40*(1), 79–88.

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, *65*(2017), 77–89. Retrieved from https://doi.org/10.1016/j.cose.2016.10.009

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

Tatar, U. (2019). *Quantifying impact of cyber actions on missions or business processes: A multilayer propagative approach* (Doctoral dissertation). Norfolk, VA: Old Dominion University.

Tatar, Ü., Çalik, O., Çelik, M., & Karabacak, B. (2014). A comparative analysis of the national cyber security strategies of leading nations. In *International Conference on Cyber Warfare and Security* (p. 211). Academic Conferences International Limited.

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

www.acquisitionresearch.net