Scoring Cyber Vulnerabilities based on Their Impact on Organizational Goals*

Omer Keskin
University at Albany
Albany, NY
okeskin@albany.edu

Nick Gannon
University at Albany
Albany, NY
ngannon@albany.edu

Brian Lopez
University at Albany
Albany, NY
blopez@albany.edu

Unal Tatar
University at Albany
Albany, NY
utatar@albany.edu

***Abstract*— Vulnerability Management, which is a vital part of risk and resiliency management efforts, is a continuous process of identifying, classifying, prioritizing, and removing vulnerabilities on devices that are likely to be used by attackers to compromise a network component. For effective and efficient vulnerability management, which requires extensive resources– such as time and personnel, vulnerabilities should be prioritized based on their criticality. One of the most common methods to prioritize vulnerabilities is the Common Vulnerability Scoring System (CVSS). However, in its severity score, the National Institute of Standards and Technology (NIST) only provides the base metric values that include exploitability and impact information for the known vulnerabilities and acknowledges the importance of temporal and environmental characteristics to have a more accurate vulnerability assessment. There is no established method to conduct the integration of these metrics. In this study, we created a testbed to assess the vulnerabilities by considering the functional dependencies between vulnerable assets, other assets, and business processes. The experiment results revealed that a vulnerability's severity significantly changes from its CVSS base score when the vulnerable asset's characteristics and role inside the organization are considered.**

Keywords*— *Cybersecurity risk, vulnerability scoring, CVSS

I. INTRODUCTION

Managing cyber risks continues its importance for the viability of organizations. Cyber risk analysis is the primary tool for managing the consequences of cyber events [1]. It is still a challenge to quantify the cyber risks to make better investment decisions. Cyber risk is defined by the National Institute of Standards and Technology (NIST) as "risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system" [2].

Based on Kaplan and Garrick's definition, risk analysis is conducted by answering three questions [3]:

1. What can go wrong?
2. What is the likelihood of it happening?
3. What is the impact if it happens?

The vulnerability of an asset is used in answering all of these three questions. This study aims to develop a cyber vulnerability scoring approach by considering the function of the vulnerable asset on an organization's business processes.

NIST hosts the National Vulnerability Database (NVD) [4], where all known hardware and software vulnerabilities are presented using the Common Vulnerability Scoring System (CVSS). CVSS is an open vulnerability evaluation framework developed by the Forum of Incident Response and Security Teams (FIRST) to communicate the severity of software vulnerabilities. It is used extensively in vulnerability studies as a standard [5].

CVSS assigns a score to a specific vulnerability based on the answers to a set of questions. Based on the characteristics of a vulnerability, a score ranging from 0 to 10 is provided, which is then transformed into a qualitative category as None, Low, Medium, High, and Critical. There are three main metric groups in CVSS [5]:

1. *Base Metrics* are common for a vulnerability within all organizations and do not change over time,
2. *Temporal Metrics* reflect the characteristics that can change over time, and
3. *Environmental Metrics* exist to adapt the score to each organization.

NIST provides Base Metric scores of the CVSS in NVD. However, Environmental Metrics should be calculated and incorporated into Base Metrics to adjust CVSS scores per the organization's particular IT infrastructure and business processes to result in more accurate cyber risk calculation.

The purpose of this study is to build a testbed to assess the vulnerabilities by considering functional dependencies among assets and business processes. The testbed will help benchmark the severity of vulnerabilities not only by looking at their CVSS scores but also by investigating how important the relevant assets and business processes for the organization.

The rest of the article is organized as follows: Section 2 provides insights about the previous research conducted in this field, Section 3 gives details about the methodology of this research, Section 4 provides the findings of this study, and Section 5 presents the conclusions and future directions.

* This material is partially based upon work supported by the National Science Foundation under Grant No. 1948261.

II. Literature Review

Having been initially released in 2004 by FIRST, CVSS has been steadily receiving updates for quite some time. Releasing the version 2.0 system in 2007, Version 3.0 in 2015, and its newest update version 3.1 in 2019, FIRST has pushed for CVSS to become a public and open vulnerability scoring standard for over a decade. The Common Vulnerability and Exposures team (CVE) has been logging vulnerabilities since 1999 and has established CVSS as one of the main scoring systems for their database by even going back to past vulnerabilities and applying them to recent ones to gauge their CVSS scores [6]. CVSS's goal is to serve as a standard for vulnerability scoring across organizations. To accomplish this goal, CVSS 2.0 introduced the concept of "domains" for vulnerability scoring.

The original FIRST score was a raw value, and its value was determined differently depending on the situation. While it is still possible to use the raw FIRST score, it has been deprecated in favor of using a CVSS base score (e.g., CVSSv2 Base Score) to express the severity of a vulnerability, which can then be translated into one of the three different CVSS domains (i.e., Base, Temporal, or Environmental) [5].

The intended use of the CVSS is to assist organizations in addressing vulnerabilities in their systems and inform them of issues that may arise in the future. By generating a CVSS score, an organization can decide where to assign time and resources to reinforce its systems. With the support of the NVD adapting the CVSS into its current design of dividing vulnerabilities into 23 distinct categories by applying a severity score to each record and the average value to each category, the CVE database adapting the CVSS scoring system, and the NIST recognizing and encouraging it, the CVSS has grown to become more and more of standard measurement for vulnerabilities. When paired with other forms of risk analysis, it has become a vital tool in an organization's repertoire.

CVSS provides a numerical score (0.1 Low to 10.0 Critical) that determines the severity of vulnerabilities that could affect other vulnerabilities in turn. It is determined through three metric groups that, when measured together, output a number that shows the severity of the vulnerability. The first metric group is the base, which rates vulnerabilities on their innate capability of doing damage and how likely they would be exploited. These base metrics can be determined by either the producer of the product rating its vulnerability or potentially their parties rating the products themselves. The next metric group is temporal, which bases vulnerabilities on time-based factors such as zero-day exploits codes, their availability to the public, and how quickly a patch has been released. Finally, the last metric group is environmental, which affects the previous metrics according to the specific environment of the user of the CVSS. Every use of the CVSS can be tailored to fit the requirements of a user's computing environment [5], [7].

As good as a scoring system CVSS is, it does have its own faults—one of the problems being how subjective the scoring system is. When generating a score, it does not take into account the number of times a vulnerability is actually exploited in the wild. Not only that, but the scoring system also does not consider any of the user's "environmental configurations, security controls or known exploits" [8]. CVSS is also limited in that it only checks to see if the vulnerability exists. This can be helpful when conducting a risk assessment but does not represent the return of investment of implementing a solution for an existing vulnerability. Some other faults of CVSS are that it does not account for user behavior, such as users clicking a malicious URL within an email. Without understanding the users' behavior, it is hard to provide an accurate representation of the risk associated with an attack. When vulnerabilities are completely scanned, in one study, it seemed like XSS and information exposure vulnerabilities are judged to have too low a Base Score. While Code injection, SQL injection, resource management errors, improper input validation, and buffer errors are considered highly dangerous [9].

When it comes to Risk analysis, the use of CVSS could be of great benefit to parties that want to see an overview of present vulnerabilities within their infrastructure. Industry standards use CVSS scores to check for compliance. This scoring system is well-used and helps the industry proactively adopt [10]. CVSS is viable when conducting risk analysis because it represents the way vulnerability assessment has evolved over time. The "Severity" represents the impact of the vulnerability on your infrastructure due to an attempted security breach. Not only that, but by using multiple techniques, it is possible to graphically see different types of attack paths a bad actor could use when attacking infrastructure. Using CVSS when conducting a risk analysis, organizations can calculate the "attack impact" a vulnerability may have within your infrastructure and take action to mitigate the risk [11]. CVSS consists of three metric groups: base, temporal, and environmental. The model uses attributes from these groups to estimate the impact a vulnerability has on infrastructure. The base group includes features that are intrinsic to the vulnerability. The temporal group has characteristics that can change over time or that depend on the infrastructure. As the name implies, environmental is about the environment the vulnerability exists in and can be subjective, depending on how you rate things like operating systems or browsers. Various vulnerabilities can be assigned different scores in each of these groups, depending on how significant they are to an organization's infrastructure. For example, a password is probably rated low in base but medium in temporal and high in environmental because some environments don't use passwords [12].

III. Methodology

The objective of this research is to build a testbed to assess the severity of vulnerabilities by considering functional dependencies among assets and business processes in addition to their CVSS scores. In order to achieve this, concepts of Functional Dependency Network Analysis are employed [13]. Firstly, the assets and business processes will be identified and described, then CVSS scores will be considered from the perspective of the impact on the vulnerable assets. Finally, the impact propagation among assets and business processes will be investigated to benchmark the severity of vulnerabilities for the organization.

A. Assets and Business Processes

Organizations consist of numerous entities. From the cybersecurity perspective, information communication technology (ICT) assets play an essential role in the operations of the organization [14]. ICT assets can be tangible, such as hardware, or intangible, such as data and intellectual property. The value added to the organization by each asset varies significantly [15]. In order to have an idea of how the failure or loss of an asset impact the organization, the assets are needed to be mapped into the business processes by considering the functional dependencies among the entities. The whole map of the network is called the impact graph [16], [17].

Operability (P_i) of each entity ($N_i, i = 1,2,3 \ldots h$) represents the level of performance the entity yields. It can have values from zero to 100 utils, from inoperable to completely operable, respectively ($0 < P_i < 100$) [13]. Since the information communication technology network of the organization is under focus in this study, each entity should be taken into consideration based on the importance of confidentiality, integrity, and availability represented by weights as in (1) [18]. For example, for a public website, availability is critical (high w_{Ai}), but for a database server of a hospital, confidentiality is vital (high w_{Ci}) because of data protection and privacy regulations. On the other hand, for a server that manages money transactions of a bank, integrity is much more critical (high w_{Ii}), while confidentiality and availability are still important. Therefore, the operability level for each node needs to be a weighted function of the operability of confidentiality, integrity, and availability (CIA) aspects (V_{Ci}, V_{Ii}, V_{Ai}) [18].

$$P_i = w_{Ci} * V_{Ci} + w_{Ii} * V_{Ii} + w_{Ai} * V_{Ai} \qquad (1)$$

B. *CVSS Impact Score*

After the assets and business processes are identified, and the relationships among these entities are determined, assets should be scanned for vulnerabilities. Using the information provided in NVD, all the assets are needed to be scanned to reveal the vulnerabilities each asset possesses. Then, each vulnerability is analyzed to reveal their impact on CIA, looking at the impact metrics, which can have a value of none, low, or high based on the characteristics of the vulnerability. The numerical values provided in [5] regarding the impact metrics are normalized to represent the operability value of CIA components of each entity. If the CIA impact value is none, after exploiting the vulnerability, the operability of CIA aspects (V_{Ci}, V_{Ii}, V_{Ai}) stays as 100 utils. If it has a high or low impact, operability degrades to zero or 61, respectively [18]. Using the degraded operability values and weights of CIA aspects in (1), the operability value of the asset can be calculated.

C. *Impact Propagation from Assets to Business Processes*

In order to analyze how impact propagates from vulnerable assets to business processes, the relationships among entities are determined based on functional dependencies. If the operation of one entity (asset or business process) contributes to the functionality of another entity, this means there is a directional functional dependency relationship. The functional dependency among entities should be considered from three perspectives, CIA. For example, when the availability of an entity is lost due to an interruption, it can cause availability loss in the dependent entities. Similarly, confidentiality loss can cause further confidentiality loss. However, loss of integrity can cause not only loss of integrity but also loss of confidentiality and availability since the loss of integrity may lead the attackers to gain full control on an asset that leads to an extended impact on the dependent entities.

All dependency relationships are subject to the Strength of Dependency (SOD) constraint, i.e., each dependency relationship among pairs of entities can have different strengths based on the characteristics of the entities and the relationship. The owner of the assets who has extensive information about the degree of dependency can determine the SOD parameter (α_{ij}) for each relationship. Equation (2) or (3) is used to calculate the operability of a dependent node (n_j) when there are only one or multiple feeder nodes (N_i), respectively.

$$P_j = SODP_j = \alpha_{ij} P_j + 100\left(1 - \alpha_{ij}\right) \quad 0 < \alpha_{ij} < 1 \qquad (2)$$

$$P_j = Average\left(SODP_{j1}, SODP_{j2}, SODP_{j3}, \ldots SODP_{jh}\right) \qquad (3)$$

After computing the operability values for each dependent node's CIA aspects sequentially, from the assets at the bottom to the business processes at the top using (2) and (3), the operability of each entity can be calculated using (1).

In summary, the application of the method starts with identifying the entities, which are all the assets and business processes. Then, weights for CIA aspects for each entity are assigned. This is followed by scanning the assets for vulnerabilities and determining the impact on CIA operability values of these entities. Finally, impact propagation is analyzed to compute the impacts of vulnerabilities on the business processes.

D. *Testbed*

The network topology of the sample organization is presented in Figure 1. The network consists of three segments, divided by different rulesets by the organizational firewall. There is a web server in the De-Militarized Zone (DMZ) that can easily be accessible by users on the Internet. A database server is located in the internal network, and user workstations exist to administer the servers. The first step of the analysis is to determine the entities and their CIA weights, as shown in Table 1. In this step, for each asset, the weights are assigned based on the importance of CIA aspects. For example, the web server hosts the public website; therefore there is not any confidential content. However, availability is highly important for this asset.

Fig. 3. Testbed network topology.

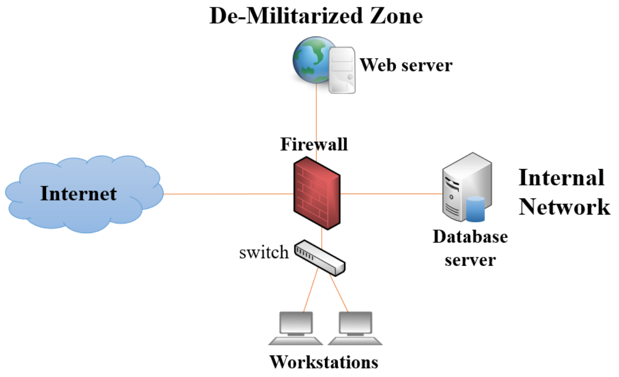

TABLE I. CIA WEIGHTS OF ENTITIES

Entit y	Name	Weights (w_{Ci}, w_{Ii}, w_{Ai})		
		Confidentiality	*Integrity*	*Availability*
A1[a]	Firewall	0.10	0.45	0.45
A2	Workstation	0.4	0.4	0.2
A3	Database Server	0.35	0.35	0.30
A4	Web Server	0.10	0.20	0.70
B1[b]	Hosting Website	0.10	0.45	0.45

[a] Assets are represented as A#

[b] Business Processes are represented as B#

After the entities are identified, and weights are determined, the assets are scanned for vulnerabilities. In Table 2, Vulnerable assets are listed with the specific vulnerabilities they possess along with the respective CIA impact metric values provided in the NVD.

The last step before starting the analyses is determining the functional dependency relationships among the entities of the network. In Figure 2, the impact graph of the network is presented. Orange nodes represent the assets of the network. The business process, which is hosting the company's website, is shown at the top by the blue node. The arrows represent the functional dependency relationships among the entities, and the strength of dependency fractions are presented in Table 3 based on the characteristics of the relationship.

TABLE II. EXISTING VULNERABILITIES & THEIR CIA METRIC VALUES

Vulnerable Asset	Vulnerability Identifier	Metric Values (V_{Ci}, V_{Ii}, V_{Ai})		
		Conf.	*Integrity*	*Avail.*
Firewall	CVE-2018-0405	High	None	None
Firewall	CVE-2020-3330	High	High	High
Workstation	CVE-2016-7291	High	None	High
Workstation	CVE-2021-27054	High	High	High
Database	CVE-2021-21484	High	High	High
Database	CVE-2019-19801	None	High	None
Web Server	CVE-2020-4719	None	High	None
Web Server	CVE-2017-10352	Low	Low	High
Web Server	CVE-2021-21513	High	High	High
Web Server	CVE-2020-9044	High	None	High

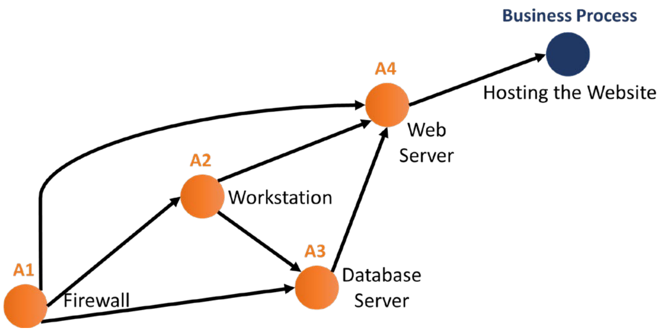

Fig. 4. Impact Graph with the functional dependency relationships.

TABLE III. STRENGTH OF DEPENDENCY FRACTION BETWEEN FEEDER (ROWS) AND RECEIVER (COLUMNS) NODE PAIRS

Alpha		receiver j											
		A2C	*A2I*	*A2A*	*A3C*	*A3I*	*A3A*	*A4C*	*A4I*	*A4A*	*B1 C*	*B1I*	*B1A*
feeder i	*A1C*	0.1			0.1			0.1					
	A1I	0.1	0.1	0.3	0.1	0.1	0.2	0.1	0.5	1			
	A1A			0.3			0.2			1			
	A2C				0.1			0.8					
	A2I				0.1	0.8	0.1	0.3	0.7	0.1			
	A2A						0.1			0.1			
	A3C							0.7					
	A3I							0.3	0.8	0.8			
	A3A									0.8			
	A4C										1		
	A4I										1	1	1
	A4A												1

IV. FINDINGS

By using the information and the network topology of the testbed, analyses are conducted to see the impact of vulnerabilities on the business process. In this section, the findings of the analyses are presented.

During the analyses, the CVSS scores of vulnerabilities are compared with the operability loss of the business process as a result of their exploitation. The analyses start with implementing the CIA operability loss for each vulnerable asset listed in Table 2. For the second vulnerability on the firewall, CVE-2020-3330, there is a high impact on all confidentiality, integrity, and availability; therefore, operability of these will degrade to zero. Then, using (2) and (3), the impact propagation is calculated for each node following the order of Assets 2, 3, 4, and finally Business Process in a cascading manner. The CVSS base score for this vulnerability is provided in NVD as 9.8, which means it is critical. And the impact analysis conducted on the testbed suggests that the operability level of the business process decreases to 76, as can be seen in Figure 3.

On the other hand, the first vulnerability on the web server, CVE-2020-4719, has a high impact only on integrity. Therefore, operability of integrity will degrade to zero while confidentiality and availability keep at 100 utils. Again, using (2) and (3), the impact propagation is calculated starting from Asset 4, resulting in the Business Process since it is only dependent on the web server. The CVSS base score for this vulnerability is provided in NVD as 4.9, which means its criticality is medium. And the impact analysis conducted on the testbed suggests that the operability level of the business process decreases to 50, as can be seen in Figure 3.

These two examples showed that the base metric score does not necessarily imply a high impact on the business. Figure 3 presents the CVSS base score of the vulnerabilities in blue bars

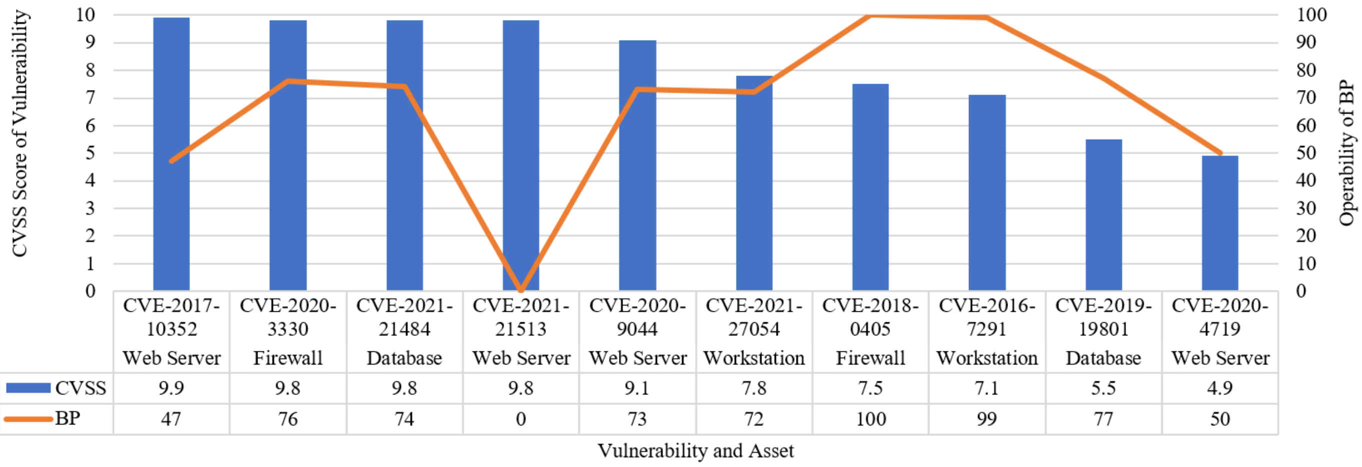

Fig. 3. Comparison of CVSS base score and impact on business process (BP).

in descending order from left to right, and the orange line represents the cascading impact on the operability level of the business process. Only two out of five vulnerabilities with the highest CVSS score (CVE-2021-21513 and CVE-2017-10352) have a significant impact on the business process. Moreover, some vulnerabilities with low CVSS score, such as CVE-2020-4719 has a high impact on the business. Therefore, the findings of the study suggest that the CVSS scores should not be solely taken into consideration to make vulnerability prioritization.

V. Conclusion

In this study, a testbed is developed to compute the impact of vulnerabilities on businesses to be able to compare and rank the vulnerabilities. The decision-makers who aim to increase the effectiveness and efficiency of the patch management practices need to consider applying this approach in their practices. The developed approach helps decision-makers focus on the most critical vulnerabilities for their organization's assets based on the business impact rather than only depending on the base score of CVSS.

Future directions for the field include implementing the likelihood aspect of cyber risk management into the vulnerability prioritization plan and automating the process of building the testbed for scalability purposes to enable organizations with thousands of assets to implement the developed approach easily.

References

[1] B. Karabacak and Ü. Tatar, "Strategies to Counter Cyber Attacks: Cyber Threats and Critical Infrastructure Protection," in *Critical Infrastructure Protection*, vol. 116, IOS Press, 2014, p. 19.

[2] National Institute of Standards and Technology, "Glossary | CSRC." https://csrc.nist.gov/glossary (accessed Apr. 13, 2021).

[3] S. Kaplan and B. J. Garrick, "On The Quantitative Definition of Risk," *Risk Analysis*, vol. 1, no. 1, pp. 11–27, 1981, doi: https://doi.org/10.1111/j.1539-6924.1981.tb01350.x.

[4] National Institute of Standards and Technology, "National Vulnerability Database," 2000. https://nvd.nist.gov/ (accessed Apr. 13, 2021).

[5] FIRST, "Common Vulnerability Scoring System version 3.1 Specification Document," Jun. 2019. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document.

[6] A. Tripathi and U. K. Singh, "On prioritization of vulnerability categories based on CVSS scores," in *2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, Nov. 2011, pp. 692–697.

[7] C. Fruhwirth and T. Mannisto, "Improving CVSS-based vulnerability prioritization and response with context information," in *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, Oct. 2009, pp. 535–544, doi: 10.1109/ESEM.2009.5314230.

[8] J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, "Improving vulnerability remediation through better exploit prediction," *Journal of Cybersecurity*, vol. 6, no. tyaa015, Jan. 2020, doi: 10.1093/cybsec/tyaa015.

[9] H. Holm and K. K. Afridi, "An expert-based investigation of the Common Vulnerability Scoring System," *Computers & Security*, vol. 53, pp. 18–30, Sep. 2015, doi: 10.1016/j.cose.2015.04.012.

[10] M. Petraityte, A. Dehghantanha, and G. Epiphaniou, "A Model for Android and iOS Applications Risk Calculation: CVSS Analysis and Enhancement Using Case-Control Studies," in *Cyber Threat Intelligence*, A. Dehghantanha, M. Conti, and T. Dargahi, Eds. Cham: Springer International Publishing, 2018, pp. 219–237.

[11] E. Doynikova and I. Kotenko, "CVSS-based Probabilistic Risk Assessment for Cyber Situational Awareness and Countermeasure Selection," in *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, Mar. 2017, pp. 346–353, doi: 10.1109/PDP.2017.44.

[12] S. H. Houmb, V. N. L. Franqueira, and E. A. Engum, "Quantifying security risk level from CVSS estimates of frequency and impact," *Journal of Systems and Software*, vol. 83, no. 9, pp. 1622–1634, Sep. 2010, doi: 10.1016/j.jss.2009.08.023.

[13] P. R. Garvey and C. A. Pinto, "Introduction to functional dependency network analysis," MIT, Cambridge, Massachusetts, Jun. 2009, vol. 5.

[14] U. Tatar, H. Bahsi, and A. Gheorghe, "Impact assessment of cyber attacks: A quantification study on power generation systems," in *2016 11th System of Systems Engineering Conference (SoSE)*, 2016, pp. 1–6.

[15] B. Karabacak and U. Tatar, "An Hierarchical Asset Valuation Method for Information Security Risk Analysis," 2012, p. 7.

[16] C. A. Pinto *et al.*, "Cybersecurity Acquisition Framework Based on Risk Management: Economics Perspective," Monterey, California. Naval Postgraduate School, Report, 2020. Accessed: Apr. 13, 2021. [Online]. Available: https://calhoun.nps.edu/handle/10945/65981.

[17] H. Bahsi, C. Udokwu, U. Tatar, and A. Norta, "Impact Assessment of Cyber Actions on Missions or Business Processes – A Systematic Literature Review," presented at the ICCWS 2018 13th International Conference on Cyber Warfare and Security, Mar. 2018.

[18] U. Tatar, O. Keskin, H. Bahsi, and C. A. Pinto, "Quantification of Cyber Risk for Actuaries An Economic-Functional Approach," May 2020. [Online]. Available: https://www.soa.org/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf.

Author Information

Omer Keskin is a Ph.D. candidate in Engineering Management at Old Dominion University and an M.S. student in cybersecurity at the University at Albany. His area of research includes organizational cybersecurity risk management, economics of cybersecurity, cyber insurance, cybersecurity education, supply-chain security, and blockchain technology.

Nick Gannon is a senior majoring in BS in Digital Forensics at the University at Albany. Nick is a recipient of NSF REU (Research Experiences for Undergraduates) Fellowship.

Brian Lopez is a senior at the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University at Albany. Brian is a recipient of NSF REU (Research Experiences for Undergraduates) Fellowship.

Dr. Unal Tatar is an assistant professor of cybersecurity in the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University at Albany. Dr. Tatar worked as a principal cybersecurity researcher in government, industry, and academia for over 15 years. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar's research is funded by the National Science Foundation, National Security Agency, Department of Defense, NATO, and Society of Actuaries. His main topics of interest are cybersecurity risk management, economics of cybersecurity, cyber insurance, privacy, cybersecurity education, supply-chain security, and blockchain. Dr. Tatar holds a BS in Computer Engineering, an MS in Cryptography, and a Ph.D. in Engineering Management and Systems Engineering.