Quantitatively Examining Service Requests of a Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses

Landon McLilly
School of Computer Science,
Colorado Technical University,
Colorado Springs, CO, USA
landon.mclilly@student.ctuonline.edu

Yanzhen Qu
School of Computer Science,
Colorado Technical University,
Colorado Springs, CO, USA
yqu@coloradotech.edu

Abstract— **With the rise of cybercrimes, limited by the funding and in-house technical resource, the small business sector is already known for struggling with cybersecurity-related issues. Regardless of 65% acknowledging they have been the target of a cyberattack and 86% believing digital risk will upsurge, only 4% of small and medium-sized business owners have executed all of the U.S. Small Business Administration's cybersecurity best practices, rendering to a survey by Nationwide [1]. To meet this challenge, we have proposed a cloud-based on-demand cybersecurity service solution for small businesses (CODCSSSB) to provide a cost-effective cybersecurity resolution for small businesses. This paper has explored how to apply a quantitative examination approach to validate the security service requests sent to and processed by the CODCSSSB to discover the weakness of design with low cost in terms of the time of development and accuracy of identifying the root cause of the design issues.**

*Keywords— **cloud computing, cybersecurity, cost-effective, small business, risk management***

I. Introduction

Research shows that 82% of small businesses have undergone security attacks where malware could bypass their antivirus software [2]. As a result, small businesses require a more robust and practical approach to defend their business computers from basic and advanced cyber threats. Characteristically, small businesses do not have the same resources, familiarity, or proficiency in implementing robust cybersecurity practices to protect their companies and the major brands they represent [3]. Information security breaches would sustain severe losses for businesses that can be either tangible such as the loss of business and the maintenance cost of system failure, or intangible such as the loss in customer trust, reputation, and competitiveness [4]. As a result, it is imperative to effectively ensure that the proper tools and best security practices are used to defend a business from internal and external threats effectively. For example, essential security services such as disabling an Active Directory account should prioritize versus creating an Active Directory account.

However, many active Active Directory accounts remain active when they should have been disabled due to human errors due to the employer no longer employing the user. About 82% of small business organizations do not have a solid foundation for effective information security risk management [5]. Most small businesses and franchise locations do not have IT expertise on-premise, so there is rarely anyone to monitor security events and respond to incidents as they occur [6]. Small businesses need an information security system that is affordable, easy to implement and use, and prevents harm by security incidents [7].

A practical modern solution to address all the challenges that small businesses face is leveraging the ability to implement and adopt a cloud-based on-demand cybersecurity web service to eliminate many of the costs associated with an on-premise service solution such as advanced firewalls and intrusion detection solutions. Technology must be used to protect the businesses' most valuable asset—the company data. Protecting the confidentiality, integrity, and accessibility of information takes time, effort, and money [8]. Therefore, a concise and grounded comparative analysis of a cloud-based cybersecurity solution is needed to address concerns regarding the cyber-defense solution for small businesses.

We have designed a cybersecurity service solution that receives requests generally asked by small businesses to achieve this purpose. As a result, the design of CODCSSSB must meet or exceed the needs of a small business environment regarding a complete cyber defense and cost-effective cybersecurity solution that meets the needs of an SMB. The system will defend an enterprise network around the clock and effectively respond to small businesses' cybersecurity requests within systems, in both theoretical and real-world scenarios. This paper examines the effectiveness of implementing an on-demand cybersecurity service solution for small businesses that will meet or exceed their business objectives. It is believed that switching to the cloud saves 35% to 50% in operation and infrastructure costs [9].

The remaining of this paper is structured as follows. The second section explores contemporary related research. The third section provides the problem statement for the research and presents the hypothesis. The fourth section describes the

978-1-7281-7624-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CSCI51800.2020.00027

methodology for the work. The fifth section shows a few illustrations of the system design of CODCSSSB. The final section presents the conclusion and future work.

II. Related Work

A. Prior Research on Cybersecurity Threats and Attacks

During the year 2017, there has been an excessive number of cybersecurity disasters that detrimentally affected businesses, individuals, and countries [10]. Since then, new categories of cyberattacks have emerged, many of them intended to be deployed against smaller businesses that cannot afford sophisticated network security infrastructure [11]. In today's business environment, companies are using technology devices that are the most convenient. However, in many cases, information security is the least of their concerns. The field comprises all the mechanisms and processes by which digital devices like computers, laptops, smartphones, tablet information, data, and services are protected from unintended access [12].

The current role of information within enterprises is altering, increasing importance and becoming more critical, and forming our interpretation of cybersecurity [13]. According to cybersecurity experts, there are likely at least 80 million internal cybersecurity attacks a year—and that number is conceivably considerably higher since numerous internal attacks that go unreported. [14]. Cyber-attacks occur due to several reasons, such as human-error and vulnerabilities being exploited in software. Over time, research has shown that aspects of passive engagement, lack of knowledge, misdirected attention, and engaging in risky cybersecurity behaviors all have the potential to increase organizational susceptibility to security flaws [15]. Since cyber threats are increasing, small businesses are still struggling to defend their organization from even the most rudimentary threats when leaders and employees have different expectations regarding IT resources, leaders and employees' information security might be perceived as less critical than other company issues [16].

Organizations must choose to implement information security awareness programs to protect their data [17]. Additionally, social engineering attacks challenge information security professionals because no technical countermeasures to-date can eliminate human vulnerability [18]. As cybersecurity experts comprehend all too well— humans are the weakest link in terms of cybersecurity efforts. Subsequently, research has exposed numerous organizations with extensive outsourced IT services lacking IT governance oversight competence [19].

B. Prior Research on Cybersecurity Solutions

Research on cybersecurity costs back approximately two decades generally focused on two themes: budgeting correctly and influential cyberattacks' economic impacts [20]. Small businesses may encompass a hybrid of information systems, and their hosted applications are characteristically subject to information security errors, which, if exploited, may lead to significant losses to the organization [21]. Malware is the biggest threat to today's electronic world as they are harmful to the users by stealing their information, corrupting data, and disabling the Network and systems by malicious attacks [22]. As a result, it is imperative to consider an effective solution to mitigate as many cyber-related issues occur through technology.

Other security tools are immensely effective against login security concerns such as two-factor authentication. Authentication is a very important consideration for several applications because it affects the system's performance in terms of security and confidentiality [23]. The progressions in multi-factor authentication with various influences deliver a safer and more protected computing environment for users and organizations, though at the expenditure of other administrative considerations. Cybersecurity awareness training for employees is indispensable, but it does not deliver the necessary skills training obligatory to protect businesses against cyber-attacks [24]. As a result, many Small businesses have been forced to rely solely on a technical solution to defend their organization against cyber threats.

III. Problem Statement, Hypothesis Statement, and Research Question

A. Problem Statement

Current research indicates that most of the Small businesses have failed at effectively implementing cybersecurity efforts due to the lack of funds, information technology employees, and familiarity with the right cybersecurity solution that meets the business objectives.

B. Hypothesis Statement

Suppose the suggested solution of a cloud-based on-demand cybersecurity service for small businesses (CODCSSSB) can process various cybersecurity requests providing cost-effective proactive and reactive cybersecurity services to Small businesses. In that case, the success rate of cybersecurity efforts in Small businesses meeting their business needs will significantly improve.

C. Research Question

How will the change of the type of cybersecurity service delivered through CODCSSSB impact meeting small businesses' business needs?

IV. Methodology

In this section, we will present our high-level design of CODCSSSB. We will first present the definitions of real-world cybersecurity requests through the system design. Then we will discuss how to determine the sample size for testing our design of CODCSSSB. Finally, to validate the functionality provided in the design of CODCSSSB, we will demonstrate how we have conducted a simulated experiment for the validation test for the security service request sent to and processed by CODCSSSB.

A. High-Level Design of CODCSSSB

Without providing concrete details, we can present a high-level abstraction of the design of CODCSSSB, as shown in FIGURE I. From the diagram in FIGURE I, we can see that the main system components include the SQL database, the CODCSSSB server, and the CODCSSSB cloud interface through which the customers can send in their cybersecurity service requests, while also through which the CODCSSSB server will deliver the solutions to the customers as the response to their service requests.

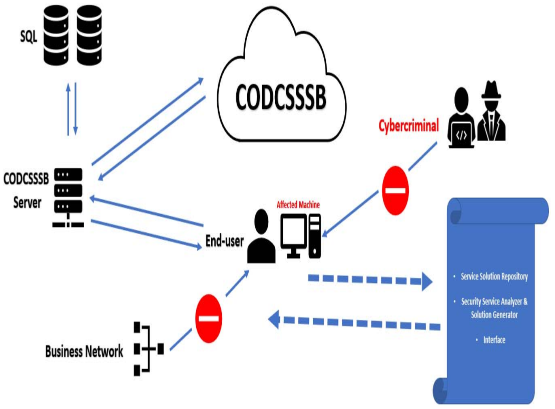


FIGURE I. OVERVIEW OF THE DESIGN OF CODCSSSB.

B. Definitions

One of the significant perceptions used in the CODCSSSB design is the security service request response (SSRR), which defines a service request from an SMB customer. A specific SSRR issued by the CODCSSSB system can either complete the cybersecurity request with a ready to use solution or it cannot due to system design limitations. Therefore, if we can examine whether the system can or cannot deliver the expected results, that will provide two benefits: one is to give the SMB customers a better position to seek services through such a web service system, and another one is to give the system developer a better understanding on what can be the additional services extended for the future deliverables of the system.

In the following subsections, we will first define a concept called "type of security service needs by small businesses" and two types of security service requests used in our discussion.

Definition 1

Let us assume we have the following:

All the security service requests sent to the CODCSSSB can be categorized into the type of security service needs by small businesses, such as network security, application security, critical infrastructure security, cloud security, as shown in TABLE I, from which we can see there are total 49 different types of security service needs by small businesses.

TABLE I. AN EXAMPLE OF THE TYPE OF CYBERSECURITY SERVICE NEEDS BY SMALL BUSINESSES

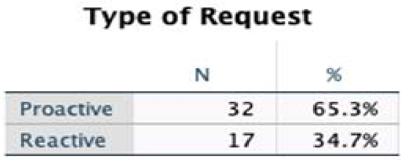
Security Service Needs by SBs	#UseCases	%
Network Security	**11**	**22.4%**
Application Security	**9**	**18.4%**
Critical Infrastructure Security	**27**	**55.1%**
Cloud Security	**1**	**2.0%**
Internet of things (ioT) security	**1**	**2.0%**
Total	**49**	**100%**

Definition 2

In terms of staying ahead of specific threats, a proactive approach to IT operations is indispensable and offers a wealth of value to the organization. Proactive methods, such as trend analysis, preventive actions, and significant problem reviews, are considered effective ways to decrease the number of support requests [25]. *Proactive requests* will be 2/3 of security service requests received by the CODCSSB. For example, setting up a user's Active Directory account a few days before the new employee arrives at work for the first day. By proactively creating the account, the employee will not have to wait until the system admin creates their account.

Reactive requests are generally service requests, such as disabling a former employee's Active Directory account. For example, if the employer no longer employs the employee, the Active Directory account should be disabled within five working days. However, other scenarios where a reactive approach could cause chain reactions to undesirable events, such as failing to patch a server on time. Furthermore, this reactive approach gives adversaries more time to get around any security measures set and delve deeper inside systems [26]. TABLE II has shown the percentages of Proactive Requests and Reactive Requests used in our experiment.

TABLE II. THE TYPE OF REQUESTS RECEIVED BY SMALL BUSINESSES.



Type of Request

	N	%
Proactive	32	65.3%
Reactive	17	34.7%

C. Determine Sample Size of Security Service Requests

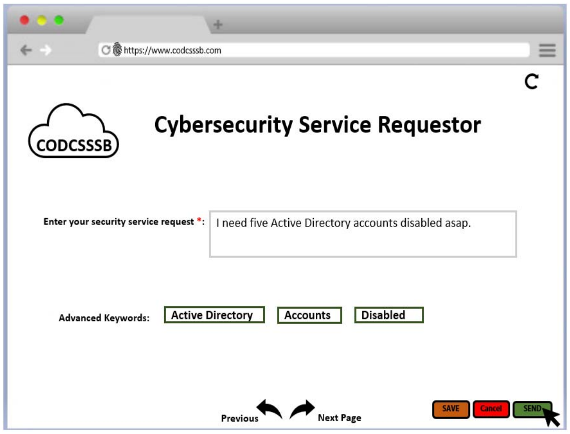
Using the two definitions above, we can use the math formula reported in [27] to estimate the minimum data samples for collecting the impact made by all the requests sent to CODCSSSB.

Considering the total number of small businesses in the US, the population size of possible service requests can reach hundreds of millions. This research have applied the math formula of determining sample size statistically recommended by the reference [27]. Based on that math formula, to achieve 5% margin of error, 95% confidence level, and 50% response distribution, we need to have at least 385 samples. Because we have 49 types of security service needs by small businesses, on average, for each type of security service need by small businesses, we only require to generate about 8 samples (385/49 = 7.86 < 8).

D. Generate Samples through Simulated Test Experiment

To validate the functionality provided in the design of CODCSSSB, we have conducted a simulated experiment for the validation test for the security service request sent to and processed by CODCSSSB.

In order to do the simulated experiment, we have first created a simple but effective CODCSSSB Simulator, which is a system consisting of three components: (1) the Emulated Interface of CODCSSSB, as shown in FIGURE II, (2) the random security service request generator, and (3) the CODCSSSB service processing Emulator. The test procedure is straightforward. We first will use the random security service request generator to create a security service request, which represents any of 49 different use cases, then we will send this request to the CODCSSSB service processing Emulator through the Emulated Interface of CODCSSSB. The security service request will be examined, then the CODCSSSB service processing Emulator will send the response to the request through the Emulated Interface of CODCSSSB with one of two possible messages: "Request is Accepted" if the existing functionality of CODCSSSB can handle the request; or "Request is Reject" if, for any of five different reasons, the existing functionality of CODCSSSB cannot handle the request. This process can be repeated to as many as we need.



Enter your security service request *: I need five Active Directory accounts disabled asap.

Advanced Keywords: Active Directory Accounts Disabled

FIGURE II. THE EMULATED INTERFACE OF CODCSSSB

Through such simulation, we have created 564 testing samples for our research project, whose testing results are as shown in TABLE III.

In TABLE III, for the requests that have been rejected, there are five different types of reasons. The detailed specification of these reasons is provided in TABLE IV.

TABLE IV. THE TOTAL NUMBER AND REASONS FOR REJECTING A REQUEST BY CODCSSSB.

Reason for Request to be Rejected	#ofRequests
R1: Availability Constraint	**58**
R2: Complexity Constraint	**58**
R3: Cannot Be Fully Automated	**59**
R4: Extensive DownTime	**49**
R5: Need Wait for a Long Duration	**46**
Total	**270**

TABLE III THE TOTAL NUMBER OF REQUESTS

Use Case	Total# Samples	Accepted	Rejected
Setting Privileged Account	18	9	9
Monitoring Data Exfiltration	11	6	5
Detection of Suspicious Network	14	7	7
Cloud Account Credentials	10	5	5
Configuration of Network	7	4	3
Asset Inventory Management	6	3	3
Network Vlan Segementation	9	5	4
Real-time Audits	20	10	10
Removal of Unused Software	9	5	4
Disabling Active Directory	14	7	7
Creating and Disabling VPN	6	3	3
Advanced Website Security	5	3	2
Cybersecurity Attack Recovery	20	10	10
Custom Activity Report	18	9	9
Device Compliance	4	2	2
Threat Assessment	10	5	5
Active Voice Monitoring	6	3	3
Vulnerability Scanning	4	2	2
DDOS Attack Recovery	19	10	9
Malware Removal	15	8	7
Physical Access Activities	4	2	2
Online Payment Processing	17	9	8
Enforcement of Password Protection	13	8	5
Data Usage by Application	4	2	2
Detection and Monitoring	13	8	5
Incident Response	13	8	5
Enforcement of Third-Party	11	6	5
Multifactor Authentication	14	7	7
Bring-your-Own-Device (BYOD)	7	4	3
Penetration Testing	18	9	9
Threat Lookup	10	5	5
Threat Data Feeds for Admin	10	5	5
Financial Threat Reporting	18	9	9
Application Security	5	3	2
IoT Security Assessment	12	6	6
Digital Forensics	18	9	9
Malware Origination Analysis	17	9	8
Data Recovery	20	10	10
Intrusion Detection and Prevention	18	9	9
Threat Simulations	8	4	4
Regulations and Compliance Audits	4	2	2
Data Backup	6	3	3
Cybersecurity Awareness Training	11	6	5
End-user and Per Machine	14	7	7
Sandbox Testing	10	5	5
Copier and Scanning Monitoring	8	4	4
Integration with Cybersecurity	7	4	3

V. EXPERIMENTS RESULTS ANALYSIS

In this section, we will analyze the results of the simulation experiments. Each sub-section will focus on one reason so that we can explore the connection between the reason and the service requests that have been rejected.

A. Availability Constraint

R1 is the reason ID representing a service request is rejected due to some kind of availability constraint of the service involved with a request. Service availability refers to providing or receiving reliable services and placing a quoted service availability requirement. The services described in this research refer to service availability as the method in which the services can be repaired, such as onsite, remote, or both. If any of these required time or human resource is not available, the service request will be rejected. For example, a service can only be accomplished onsite due to no network connectivity, such as a DDOS attack.

B. Complexity Constraint

R2 is the reason ID representing a service request is rejected due to some kind of complexity constraint involved with a request. For example, a full forensic investigation involves too many tools to complete this request. This is mostly because the requested service has some detailed parameters beyond the capacity of the current system functionality of CODCSSSB. In other words, we need to extend the system functionality further before the security service request can be processed successfully. The requests rejected due to this reason will provide system developers of CODCSSSB direct feedback on the restrictions within the current design of CODCSSSB.

Based on TABLE IV, we can found that 58 of the requests are rejected due to R2. It is about 10.3% of the total requests involved in the experiment.

C. Cannot be Fully Automated

R3 is the reason ID, which represents a service request, is rejected because at least part of the required service cannot be fully automated. For example, such a situation may happen when a new tool or new software version is just released, and the updated automation procedure has not been completed.

Based on TABLE IV, we can found that 59 of the requests are rejected due to R3. It is about 10.5% of the total requests involved in the experiment.

D. Extensive Downtime

R4 is the reason ID, which represents a service request, is rejected due to the CODCSSSB is experiencing an extensive service downtime. An enterprise may face IT service downtime costs due to various causes, including antagonistic IT attacks by hackers, non-antagonistic IT service outages, or natural catastrophes such as floods or solar storms [28]. About 16.33% of all service requests require downtime, and about 83.67% of all requests did not require any downtime. For example, the configuration of a network firewall may require a brief amount of downtime, as it would cause network disruption. DDoS attacks can have financially devastating consequences on victim businesses, and research indicates they could cost a company more than $100,000 per minute of downtime [29].

Based on TABLE IV, we can found that 49 of the requests are rejected due to R4. It is about 8.7% of the total requests involved in the experiment.

E. Need Wait for a Long Duration

R5 is the reason ID, which represents a service request, is rejected because the required service may need to wait for a long duration before it can be processed. Such a situation may happen if the CODCSSSB is conducting Disaster Recovery or Data Recovery tasks. R5 is similar to R4 as the real effect is the CODCSSSB cannot process any external service request.

Based on TABLE IV, we can found that 46 of the requests are rejected due to R5. It is about 8.2% of the total requests involved in the experiment.

F. Summary of Experiments

After analyzing the experiment results, we can now answer the following research question.

RQ: How will the change of the type of cybersecurity service delivered through CODCSSSB impact the outcome of meeting the business needs of small businesses?

Based on the experiment results, the cybersecurity services delivered through CODCSSSB will be delivered successfully, over 52% of the time. Moreover, there are five types of reasons that will cause service failure. Some of these five reasons can be addressed by improving the functionality of CODCSSSB, such as the reasons for complexity constraint and cannot be fully automated. Furthermore, some of the reasons belong to the operation management issue.

IV. Conclusion

In this paper, we have presented the design of CODCSSSB, demonstrating the cybersecurity solution's capability in determining the ability to service many of the needs of small businesses in terms of information security. We have presented an exploration of how to apply the quantitative examination approach to validate the security service requests sent to and processed by the CODCSSSB to discover the design's weakness with much low cost in terms of the time of development and accuracy of identifying the root cause of the design issues. The extent we suggest to the CODCSSSB system is intended to enhance the current cybersecurity solution landscape. The paper is limited in providing minimal sample due to system design limitations. Future work will focus on the correlations between information technology professionals and technologies versus an automated system that meets small businesses' needs

References

[1] O'Rourke, M. (2019). The Small Business Cybersecurity Knowledge Gap. Risk Management (00355593), 66(8), 36.

[2] Young Entrepreneur Council. (, 2019). Council post: The state of cybersecurity pertaining to small business. Forbes. https://www.forbes.com/sites/theyec/2019/09/18/the-state-of-cybersecurity-pertaining-to-small-business/#9c7817e31a07

[3] Musthaler, L. (2017). Small businesses are prime targets for cyber attacks: SIEM-as-a-service can help. Network World (Online).

[4] Gao, X., & Zhong, W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. Annals of Operations Research, 235(231), 277-300.

[5] Fielder, A., Konig, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. *Games, 9*(2).

[6] Musthaler, L. (2017). Small businesses are prime targets for cyber attacks: SIEM-as-a-service can help. Network World (Online).

[7] Bryan, L. L. (2020). Effective information security strategies for small business. International Journal of Cyber Criminology, 14(1), 341-360. Retrieved from https://proxy.cecybrary.com/login?url=https://search-proquest-com.proxy.cecybrary.com/docview/2404395988?accountid=144789.

[8] Radziwill, N., & Benton, M. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. Software Quality Professional, 19(14), 25-43.

[9] Singh, J. (2017). Study on challenges, opportunities, and predictions in cloud computing. International Journal of Modern Education and Computer Science, 9(3), 17-n/a.

[10] Wout, C. (2019). Develop and Maintain a Cybersecurity Organisational Culture. Proceedings of the International Conference on Cyber Warfare & Security, 457–466.

[11] Bocetta, S. (2019). How a small business should respond to a hack. CSO (Online).

[12] Saxena, K., & Awasthi, A. (2015). Development in stages of cybersecurity & risk. International Journal of Advanced Research in Computer Science, 6(8).

[13] Visner, S. S. (2016). The Cybersecurity Storm Front- Forces Shaping the Cybersecurity Landscape: A Framework for Analysis. Georgetown Journal of International Affairs, *17*(3), 85-99.

[14] Schaefer, T. C. P. A. C., Brown, B. C. P. A., Graessle, F. C. P. A., & Salzsieder, L. C. P. A. (2017). Cybersecurity: Common Risks. Strategic Finance, 99(5), 54-61.

[15] Hadlington, L. (2018). Employee's Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. International Journal of Cyber Criminology, 12(1), 269-281. DOI:

[16] Noguerol, L. O., & Branch, R. (2018). Leadership and electronic data security within small businesses: An exploratory case study. Journal of Economic Development, Management, IT, Finance, and Marketing, 10(2), 7-35.

[17] Hussain, A., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11(3). doi:http://dx.doi.org/10.3390/fi11030073

[18] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6 (23), 31-38.

[19] Ako-Nai, A., & Singh, A. M. (2019). Information technology governance framework for improving organizational performance. South African Journal of Information Management, 2*1*(1).

[20] Radziwill, N., & Benton, M. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. Software Quality Professional, 19(14), 25-43.

[21] Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., & Williams, J. (2017). Contagion in cybersecurity attacks. The Journal of the Operational Research Society, 68(7), 780-791. doi:http://dx.doi.org/10.1057/jors.2016.37.

[22] Tahir, R. (2018). A Study on Malware and Malware Detection Techniques. International Journal of Education and Management Engineering, 8(2), 20.

[23] Al-Ghaili, A., Kasim, H., Othman, M., & Hashim, W. (2020). QR code-based authentication method for IoT applications using three security layers. Telkomnika, 18(4), 2004-2011.

[24] Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*.

[25] Jantti, M., & Cater-Steel, A. (2017). Proactive Management of IT Operations to Improve IT Services. Journal of Information Systems and Technology Management: JISTEM, 14(2), 191-218.

[26] Dobson, G. B., Rege, A., & Carley, K. M. (2018). Informing active cyber defense with realistic adversarial behavior. Journal of Information Warfare, 17(2), 16-31,3A,4A.

[27] Krejcie RV, Morgan DW. Determining Sample Size for Research Activities. Educational and Psychological Measurement. 1970;30(3):607-610. DOI:10.1177/001316447003000308.

[28] Wang, S. S., & Ulrik, F. (2020). Enterprise IT service downtime cost and risk transfer in a supply chain. Operations Management Research, 13(1-2), 94-108. doi:http://dx.doi.org.proxy.cecybrary.com/10.1007/s12063-020-00148-x

[29] Gordon, R. J. (2017). DDoS attack simulation to validate the effectiveness of common and emerging threats. Journal of Information Warfare, 16(1), 49-63. Retrieved from https://proxy.cecybrary.com/login?url=https://www-proquest-com.proxy.cecybrary.com/docview/1968020419?accountid=144789