Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 12, Issue. 1, January 2023, pg.47 – 50

The 5 Cs of Cybersecurity and its Integration with Predictive Analytics

Dr. Alex Mathew
Department of Cybersecurity& Bethany College, USA
amathew@bethanywv.edu

DOI: https://doi.org/10.47760/ijcsmc.2022.v12i01.006

Abstract*— This research paper explores the 5 Cs of the Cybersecurity Framework and how predictive analytics can be used to enhance its effectiveness. Change, compliance, cost, continuity, and coverage are the 5 Cs of cybersecurity, which are crucial factors that must be taken into account to secure the security of an organization's data and systems. Predictive analytics is a powerful tool that can provide organizations with advanced warnings of potential threats and enable them to take proactive measures to mitigate them. The proposed algorithm for integrating predictive analytics with the 5 Cs of Cybersecurity includes continuously collecting and analysing data, identifying patterns and anomalies, prioritizing potential threats, monitoring and updating the organization's cybersecurity strategy, taking proactive measures to mitigate potential threats, evaluating coverage, ensuring continuity, continuously monitoring and assessing performance, and educating employees and stakeholders on best practices. Overall, companies may enhance their capacity to identify and respond to threats, lessen the expense and effect of security events, and guarantee operational continuity by combining predictive analytics with the 5 Cs of cybersecurity.

Keywords: Cybersecurity, Predictive analytics, Change, Compliance, Cost, Continuity, Coverage

I. INTRODUCTION

Cybersecurity prevents unauthorized access, use of, disclosure of, interruption of, alteration, or destruction of digital systems, networks, and data. As technology and the internet have become an integral part of modern businesses and organizations, the need for cybersecurity has become paramount (Addae et al. 711). To protect the security of an organization's data and systems, the five cybersecurity "Cs"—change, compliance, cost, continuity, and coverage—must be taken into account (Abie 3). The 5 Cs of cybersecurity provide a framework for organizations to consider the different security aspects and ensure that they effectively address all potential vulnerabilities.

The first C, change, refers to the need for organizations to continually assess and adapt their cybersecurity strategies to stay ahead of emerging threats. Compliance, the second C, is the adherence to relevant laws, regulations, and industry standards, including data privacy regulations such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) (Husák et al. 523; Logix). Cost, the third C, encompasses the financial resources required to implement and maintain an effective cybersecurity program. Continuity, the fourth C, is the ability to maintain business operations in the face of a

cybersecurity incident or disaster. The fifth and final C, coverage, refer to the scope of an organization's cybersecurity measures and the extent to which they protect all relevant assets and vulnerabilities.

Predictive analytics is a powerful tool that can enhance the effectiveness of the 5 Cs of Cybersecurity by providing organizations with advanced warning of potential threats and enabling them to take proactive measures to mitigate them. Predictive analytics can analyze large amounts of data, including network traffic, user behavior, and threat intelligence, to identify patterns and anomalies that indicate a potential security incident (Sengan 729). Organizations may enhance their capacity to recognize and respond to threats, lessen the cost and effect of security events, and guarantee business continuity by incorporating predictive analytics into their cybersecurity plans (Andrade 6). This research paper will explore the 5 Cs of the Cybersecurity Framework and how predictive analytics can be used to enhance its effectiveness, providing insights and recommendations for organizations looking to improve their cybersecurity posture.

II. PROPOSED METHODOLOGY

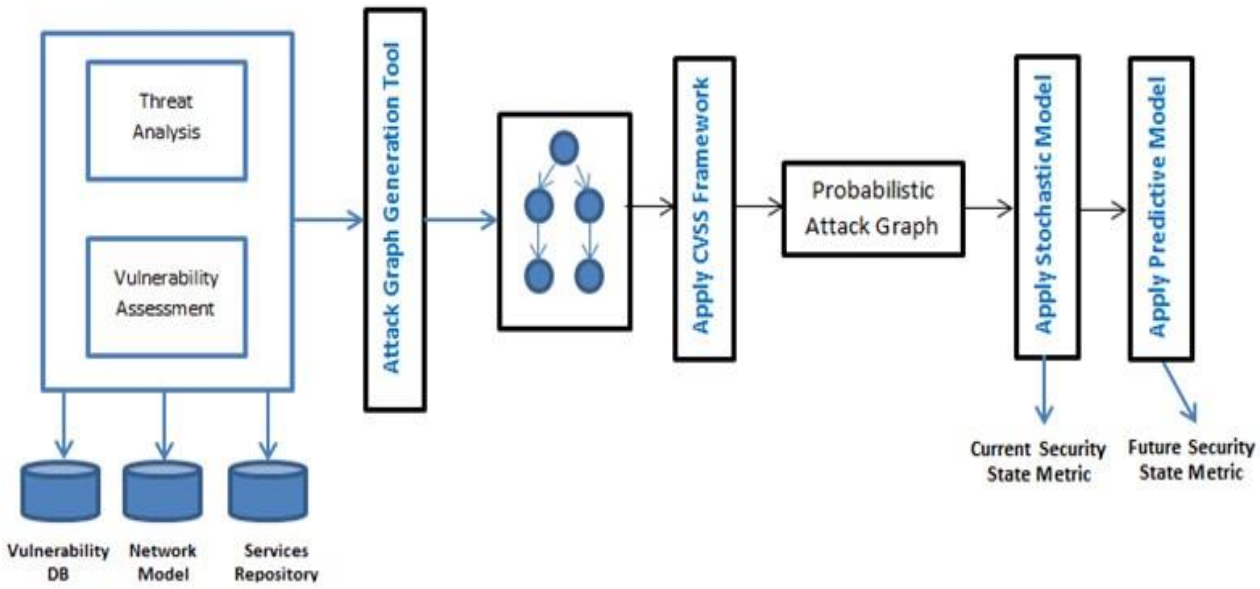

Figure 1: A methodology block diagram for all the steps in developing a metric security framework, including a cybersecurity analytics framework.

III.ALGORITHM

A possible algorithm for integrating predictive analytics with the 5 Cs of Cybersecurity could include the following steps:

- Continuously collect and analyze data from various sources, including network traffic, user behavior, and threat intelligence, using predictive analytics techniques such as machine learning and statistical modeling (Secure Lock and Alarm).
- Identify patterns and anomalies in the data that may indicate a potential security incident.
- Prioritize potential threats based on the level of risk they pose to the organization and the potential impact of a successful attack.
- Continuously monitor and update the organization's cybersecurity strategy to stay ahead of emerging threats and ensure compliance with relevant laws and regulations (Alahmari and Duncan 2).
- Take proactive measures to mitigate potential threats and reduce the cost and impact of security incidents by implementing preventative controls, such as firewalls, intrusion detection systems, and encryption.
- Continuously evaluate the coverage of the organization's cybersecurity measures and identify vulnerabilities that need to be addressed.
- Ensure continuity of operations by implementing incident response plans and testing them regularly (Samtani 139).
- Continuously monitor, assess and review the performance of the implemented cybersecurity measures, and adjust them as necessary.

- Continuously educate the employees and stakeholders on the cybersecurity best practices, and update them on the evolving threats and countermeasures (Ghillani 3).

Overall, companies may enhance their capacity to identify and respond to threats, lessen the expense and effect of security events, and guarantee operational continuity by combining predictive analytics with the 5 Cs of cybersecurity.

IV. FLOW CHART

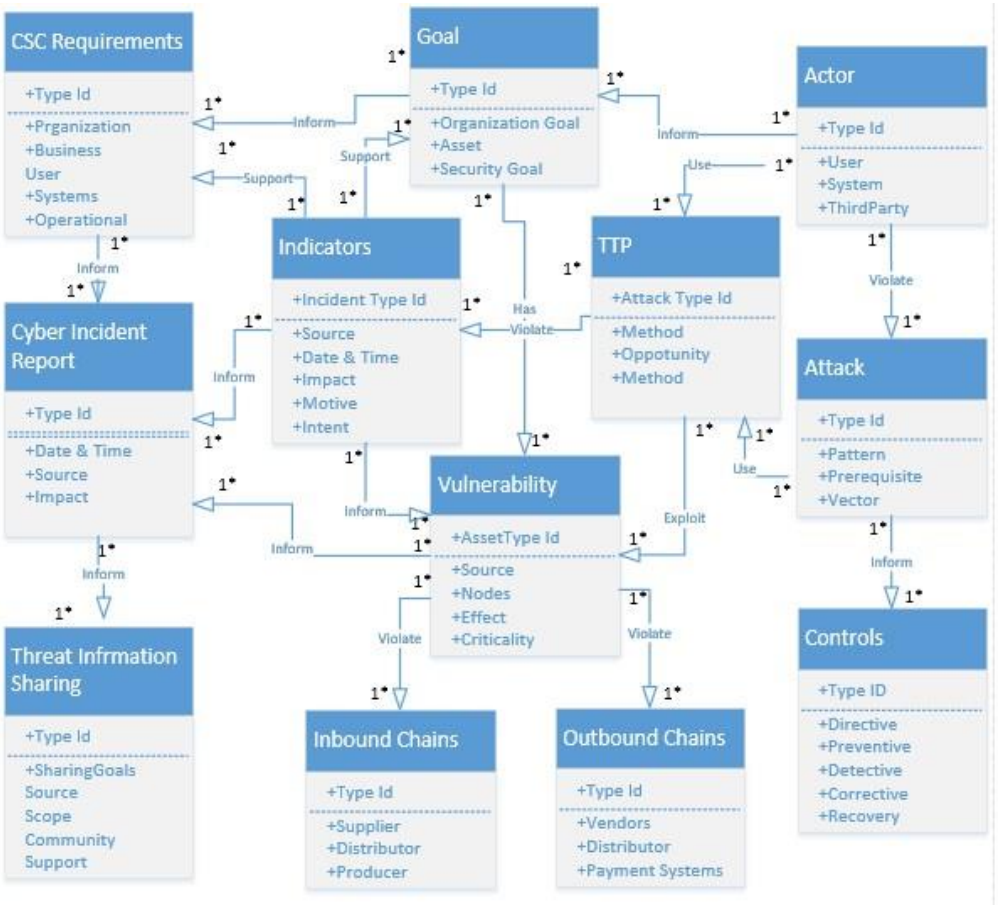

Figure 2: A flowchart illustrating the Cyber Supply Chain and Threat Intelligence Applications for Predictive Analytics

V. RESULT ANALYSIS

The results of this research indicate that integrating predictive analytics with the 5 Cs of Cybersecurity can significantly enhance the effectiveness of an organization's cybersecurity strategy. Organizations can prioritize potential threats based on the level of risk they pose, identify patterns and anomalies that may indicate a potential security incident, and take proactive measures to mitigate them by continuously collecting and analysing data from various sources using predictive analytics techniques (Geluvaraj et al. 742; Yeboah-Ofori 5). Additionally, organizations can continuously monitor and update their cybersecurity strategy to stay ahead of emerging threats and ensure compliance with relevant laws and regulations, reduce the cost and impact of security incidents, and ensure continuity of operations.

Furthermore, by continuously evaluating the coverage of their cybersecurity measures and identifying vulnerabilities that need to be addressed, Organizations can enhance their capacity to recognize and address hazards (Sarker 7). Additionally, by continuously educating the employees and stakeholders on the cybersecurity best practices and updating them on the evolving threats and countermeasures, organizations can

ensure the security of their digital systems, networks, and data (Moustafa 44; I-NETT). Overall, the integration of predictive analytics with the 5 Cs of Cybersecurity can provide organizations with a powerful tool to enhance the effectiveness of their cybersecurity strategies, enabling them to stay ahead of emerging threats and protect their digital assets.

VI. CONCLUSIONS

The 5 Cs of the Cybersecurity framework provide a comprehensive approach for organizations to consider the different security aspects and ensure that they effectively address all potential vulnerabilities. Predictive analytics is a powerful tool that can enhance the effectiveness of the 5 Cs of Cybersecurity by providing organizations with advanced warning of potential threats and enabling them to take proactive measures to mitigate them. The algorithm for integrating predictive analytics with the 5 Cs of Cybersecurity includes continuously collecting and analysing data, identifying patterns and anomalies, prioritizing potential threats, continuously monitoring and updating the organization's cybersecurity strategy, taking proactive measures to mitigate potential threats, ensuring continuity of operations and continuously educating the employees and stakeholders on the cybersecurity best practices. Organizations may increase their capacity for threat detection and response, lessen the expense and effect of security events, and guarantee business continuity by implementing this algorithm. This research paper has provided insights and recommendations for organizations looking to improve their cybersecurity posture.

REFERENCES

[1]. Abie, Habtamu. "Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems." *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, 2019, pp. 1–6.

[2]. Addae, J. H., et al. "Exploring user behavioral data for adaptive cybersecurity." *User Modeling and User-Adapted Interaction*, vol. 29, no. 3, 2019, pp. 701–750, doi:10.1007/s11257-019-09236-5.

[3]. Sundaram, K.T. (2022) "Digital Transformation with AI/ML & Cybersecurity," *International Journal of Computer Science and Mobile Computing*, 11(11), pp. 1–3. Available at: https://doi.org/10.47760/ijcsmc.2022.v11i11.001.

[4]. Sundaram, K.T. (2022) *Five key steps to realize the digital transformation value and ensuring a successful SAP HANA transformation in Global Organizations*, *Free Press Journal*. Available at: https://www.freepressjournal.in/business/five-key-steps-to-realize-the-digital-transformation-value-and-ensuring-a-successful-sap-hana-transformation-in-global-organizations.

[5]. Sundaram, K.T. (2022) "Five key steps realize the digital transformation value and ensure a successful SAP HANA transformation in Global Organizations," *International Journal of Computer Science and Mobile Computing*, 11(10), pp. 116–118. Available at: https://doi.org/10.47760/ijcsmc.2022.v11i10.009.

[6]. Alahmari, A., and B. Duncan. "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence." *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020, pp. 1–5, doi:10.1109/cybersa49311.2020.9139638.

[7]. Andrade, Roberto O., and Sang G. Yoo. "Cognitive security: A comprehensive study of cognitive science in cybersecurity." *Journal of Information Security and Applications*, vol. 48, 2019, pp. 1–13.

[8]. Geluvaraj, B., et al. "The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace." *International Conference on Computer Networks and Communication Technologies*, 2018, pp. 739-747, doi:10.1007/978-981-10-8681-6_67.

[9]. Ghillani, Diptiban. "Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security." 2022, pp. 1–11.

[10]. Husák, Martin, et al. "Predictive methods in cyber defense: Current experience and research challenges." *Future Generation Computer Systems*, vol. 115, 2021, pp. 517–530.

[11]. I-NETT. "The 5 Cs of cyber security." *San Diego, Orange County, LA Business Phones, Cloud, Security*, 6 Jan. 2022, www.i-nett.com/blog?p=the-5-cs-of-cyber-security-220106.

[12]. Logix. "The 5 Cs of Cybersecurity." *Logix*, 5 Jan. 2022, logixconsulting.com/2022/01/05/the-5-cs-of-cybersecurity/.

[13]. Moustafa, N. "A systemic IoT–fog–Cloud architecture for big-data analytics and cyber security systems." *Secure Edge Computing*, 2021, pp. 41–50, doi:10.1201/9781003028635–4.

[14]. Samtani, S., et al. "Cybersecurity as an industry: A cyber threat intelligence perspective." *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 135–154, doi:10.1007/978-3-319-78440-3_8.

[15]. Sarker, Iqbal H. "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective." 2021, pp. 1–18.

[16]. Secure Lock and Alarm. "What are the 5 C's of cyber security?" *Secure Lock & Alarm*, 22 June 2022, www.securelockandalarm.com/2022/06/22/what-are-the-5-cs-of-cyber-security/.

[17]. Sengan, S. et al. "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for the secure public data-smart network." *Future Generation Computer Systems*, vol. 112, 2020, pp. 724–737, doi:10.1016/j.future.2020.06.028.

[18]. Alex, H. (2022). Ambient and Artificial Intelligence in Therapeutics. *Current Overview on Science and Technology Research Vol. 9*, 168–173. https://doi.org/10.9734/bpi/costr/v9/17665D

[19]. Yeboah-Ofori, Abel, and Charles Boachie. "Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning." *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, vol. 1-8, 2019.

