https://doi.org/10.51408/issi2025_174

Healthcare Cybersecurity: Insights from a Scientometric Approach

Simone Di Leo[1], Cinzia Daraio[2], Fabio Nonino[3], Eugenio Oropallo[4]

[1]*dileo@diag.uniroma1.it*, [2]*daraio@diag.uniroma1.it*, [3]*fabio.nonino@uniroma1.it*, [4]*eugenio.oropallo@uniroma1.it*
Department of Computer, Control and Management Engineering Antonio Ruberti (DIAG), Sapienza University of Rome, Via Ariosto 25, Rome, 00185 (Italy)

Introduction

The increasing digitization of healthcare, driven by technological advancements and the pursuit of enhanced patient care, presents both unprecedented opportunities and significant cybersecurity challenges. While digital tools, patient phygital twins for medical planning and connected devices streamline processes and improve access to care, they simultaneously expand the attack targets for malevolent actors, potentially compromising sensitive data and patient safety (Spanakis et al., 2020). Existing technical cybersecurity countermeasures aim to protect the confidentiality, integrity, and availability of healthcare data and information systems, but the rising frequency and sophistication of cyberattacks necessitate a deeper understanding of the evolving threat landscape (Jalali et al., 2019). The SEcurity and RIghts in the CyberSpace (SERICS) project is currently developing remote healthcare solutions based on personal devices while the Phygital Twin Technologies for Innovative Surgical Training & Planning project is developing a phygital twin device and software for surgical planning, further highlighting the critical need for robust cybersecurity measures. Connected medical devices and electronic health records (as done for the patient phygital twin), while offering substantial benefits, introduce new vulnerabilities that require careful consideration. Effective incident response strategies are crucial for healthcare organizations to mitigate the impact of cybersecurity incidents and ensure timely recovery. This study addresses the critical need for robust cyber defences and effective response processes within the healthcare sector, emphasizing their contribution to overall cyber resilience through adherence to industry best practices. This is a macro-level analysis of cyber incidents across different countries and cyber actors–which aims to identify frequently targeted entities and prominent threat actors within the healthcare ecosystem. This analytical approach, leveraging real-world incident data, provides a valuable contribution by uncovering systemic vulnerabilities and informing targeted cybersecurity strategies within the context of the SERICS project and the broader healthcare landscape.

Data

This study utilizes data from the–European Repository of Cyber Incidents (EuRepoC) database (https://eurepoc.eu/), providing a comprehensive dataset of cyber incidents from 2000 to present, with ongoing daily data collection and curation. Data specific to healthcare cyber incidents, retrieved from EuRepoC (Version 1.2), shows a total of 348 incidents and 129 actors involved.

Method

Employing the methods of scientometrics (Garfield, 1972, 1955; Marchiori, 1997), the HITS algorithm (Kleinberg, 1999) analyzes networks by assigning two scores to each node: *authority* (representing value as a source of information) and *hub* (representing value as a curator or aggregator of information). Formally, these scores are defined as follows:

- *Authority Update Rule*: $\mathrm{auth}(p) = \sum \mathrm{hub}(i)$, where i represents all nodes that link to node p. So, the authority score of a node p is the sum of the hub scores of all nodes pointing to it.

- *Hub Update Rule*: hub(p) = ∑auth(i), where i represents all nodes that node p links to. So, the hub score of a node p is the sum of the authority scores of all nodes it points to.

The algorithm begins by initializing each node with both hub and authority scores of 1. It then iteratively updates these scores using the above formulas. After each iteration, the scores are normalized to prevent unbounded growth. The algorithm differentiates between individual interactions of two actors by representing each as a weighted arc. This differentiation subsequently affects the derived authority and hub scores. When applied to a network of healthcare cyber incidents, the authority score reflects how often an actor is targeted (a "defender" score), while the hub score reflects how often they initiate attacks (an "aggressor" score).

Results and conclusion

The analysis of cyber incidents within the healthcare sector yielded significant insights into the landscape of cyber threats. For the sake of brevity, we only report the results of the top 10 authorities and hubs actors. Authority results (Table 1) highlighted the United States (0.5424), Japan (0.3471), and Israel (0.3398) as prominent targets within the healthcare sector. Conversely, Hub scores (Table 2) revealed the Democratic People's Republic of Korea (0.8046) with a notably high score, followed by Iran (0.3625) and China (0.3596). Beyond nation-state actors, the analysis identified criminal groups such as CosmicBeetle, TA558, and various ransomware groups (Rhysida, LockBit, BianLian, BlackCat/ALPHV) as significant hubs, underscoring the complex and multifaceted nature of the cyberattack landscape affecting healthcare, as initially emphasized by the increasing digitization and its associated risks. These findings directly contribute to the aims of the SERICS project. By identifying frequently targeted entities and prominent threat actors, this research provides crucial information for the development of robust cybersecurity measures within the previously mentioned projects. The identification of specific threat actors and their tactics informs the design and implementation of targeted security protocols for personal, and devices used in remote healthcare, mitigating the vulnerabilities introduced by connected medical devices and sensible electronic health records. This preliminary analysis underscores the need for further research to explore correlations between Authority and Hub scores, analyze the temporal evolution of these metrics. The analysis reveals key insights with significant implications for policy development. Current cybersecurity frameworks often prioritize organizational-level security measures. However, this analysis suggests that effective policy must operate at multiple levels simultaneously, recognizing the crucial role of international cooperation. Drawing on the concept of "networked governance," a policy approach that acknowledges and addresses the interconnected nature of cyber threats, as proposed by Eggers and Goldsmith (2004), is essential.

Table 1. Top 10 Authorities.

Actor	**Authority score**
United States	0.5424
Japan	0.3471
Israel	0.3398
Korea, Republic of	0.3258
United Kingdom	0.2956
Germany	0.2551
Spain	0.2046
France	0.2027
Russia	0.1845
China	0.1838

Table 2. Top 10 Hubs.

Actor	Hub Score
Korea, Democratic People's Republic of	0.8046
Iran, Islamic Republic of	0.3625
China	0.3596
Russia	0.1051
CosmicBeetle	0.0902
TA558	0.0866
Rhysida Ransomware Group	0.076
LockBit	0.0757
BianLian Ransomware Group	0.0727
BlackCat/ALPHV	0.0727

Acknowledgments

The poster is part of the Research Projects "Phygital Twin Technologies for Innovative Surgical Training & Planning (ECS 0000024 – Rome Technopole)" and is partially supported by project SERICS (ECS B53C22003990006) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

References

Garfield, E. (1972). Citation analysis as a tool in journal evaluation: Journals can be ranked by frequency and impact of citations for science policy studies. Science, 178(4060), 471-479.,

Garfield, E. (1955). Citation indexes for science: A new dimension in documentation through association of ideas. Science, 122(3159), 108-111.

Marchiori, M. (1997). The quest for correct information on the Web: Hyper search engines. Computer Networks and ISDN Systems, 29(8-13), 1225-1235.

Kleinberg, J. M. (1999). Hubs, authorities, and communities. ACM computing surveys (CSUR), 31(4es), 5-es.

Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., ... & Magalini, S. (2020, July). Cyber-attacks and threats for healthcare–a multi-layer thread analysis. In 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) (pp. 5705-5708). IEEE.

Jalali, M. S., Russell, B., Razak, S., & Gordon, W. J. (2019). EARS to cyber incidents in health care. Journal of the American Medical Informatics Association, 26(1), 81-90.

Eggers, W. D., & Goldsmith, S. (2004). Government by network. The New Public Management Imperative.