Annotated Bibliography

1. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. *Sensors*, 23(8), 4117. https://doi.org/10.3390/s23084117

In this article, we learn about where we are in the state of IoT (internet of things), highlighting important vulnerabilities and the methods of research for the future. It focus in global approach to in the sense of security, inviting people on the field to implement better communication and management protocol issues.

This article, provides an extensive overview of “IoT” security issues. Moreover, It is published by experts in the field making it very credible.

This article helps the community to deploy understand the challenges of “IoT” security and the interdisciplinary efforts that are required to address.

2. Data Security Governance in the Era of Big Data: Status, Challenges, and Future Directions

Liyuan Sun a, Hongyun Zhang b, Chao Fang Received 10 June 2021, Accepted 18 June 2021, Available online 23 June 2021, Version of Record 29 June 2021. **https://www.sciencedirect.com/science/article/pii/S2666764921000163**

In this article focus in the development of big data and its evolution around the globe, as it poses big security risks due to the importances that has taken in these past years with the innovation of machine learning, deep data mining, etc. This paper allows to be up to date of the present situation of global data security governance.

This paper, is published by a well, regarded journal. It provides a deep examination of data security governance, making it a valuable resource for understanding in depth big data security challenges and solutions.

The research of this paper is crucial as no everybody is aware of issues can arise from bid data and points out the challenges, and then proceeds to raise solutions for further modernizing data security governance systems.

3. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure

El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An integrated approach to cyber risk management with cyber threat intelligence framework to secure critical infrastructure. *Journal of Cybersecurity and Privacy*, 4(2), 357-381. https://doi.org/10.3390/jcp4020018

This extensive article presents ideas and focus on how to manage cyber risk, specially to safeguard critical infrastructure. It is mentioned, the rapid evolution of cyber threats. This cyber

threats have become very complex, giving a very dangerous challenge to big organizations. This article, provides preventive and reactive measures to manage these risk.

The publication provided by this authors with so much expertise provides a valuable resource on the field of cyber risk management. The detailed discussion of the integration of cyber threat intelligence into risk management frameworks provides actionable insights for both practitioners and researchers.

This article is very helpful in my research due to the big relevance and effective way to understand cyber risk management strategies. The practical examples and case studies offer concrete illustrations of how these concepts can be applied in real-world scenarios.

4. A Systematic Review of Current Cybersecurity Training Methods

Julia Prümmer, Tommy van Steen, Bibi van den Berg. (2021) https://www.sciencedirect.com/science/article/pii/S0167404823004959

This paper, teaches us about the effectiveness of many cybersecurity training methods. For example, online modules, gamification, simulated cyber-attack scenarios. The researchers investigate the strengths and weaknesses of each method. The outcome shows the importance of continuous and adaptive training up to date, since technology moves at a rapid innovation of cyber threats.

This review provides insights of comprehensive examination of cybersecurity training methods. The journal where is posted is very reputable. The recommendations for

improving training programs are well-founded and practical, making this review a valuable resource for organizations looking to enhance their cybersecurity training initiatives.

This publication is very important for the foundations of my research, because allow me to understand what different methods of training are being implemented in the present and how to take advantage to either innovate for different audience. The emphasis on continuous and adaptive training aligns with the need for ongoing skill development in the face of evolving cyber threats.