Annotated Bibliography

Chen, Henry, E., & Jiang, X. (2023). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, *187*(1), 199–224. https://doi.org/10.1007/s10551-022-05107-z

This study was about the cybersecurity risk disclosures that comes after a data breach. In said study it was discovered that when companies or firms expect there to be a data breach there was an increase in the number of risk disclosures. The number gets higher depending on the severity of the data breach itself. Finally, it was shown that public scrutiny over a corporation’s deterrence of cyberattacks was a factor of rising risk disclosures. The article has over 20 different references throughout it. The authors Jing Chen, Elaine Henry, and Xi Jiang are affiliated with Stevens Institute of Technology.

PAUCH. (2023). RANSOMWARE ATTACKS AS A CYBERSECURITY INSURANCE COVERAGE THREAT. *Humanities and Social Sciences*, *30*(2), 99–107. https://doi.org/10.7862/rz.2023.hss.18

This article is focused on analyzing the risk of ransomware and its correlation to the loss ratio in cyber insurance, as well the changes in the cyber insurance over the past couple years. The graphs showed an increase of cyber related claims from 2016 to 2021. The biggest jump occurred from 2019 to 2020, around the time that the COVID-19 pandemic made many people, businesses, and organizations rely on online activities. Some of the ransom that companies paid to these cyber criminals were in the millions. The highest shown in this article was over 600 million dollars in damages from the Health Service Executive (HSE). This just goes to show how important it so to increase and improve the protection against exposure. Dariusz Pauch has contributed to 27 works including this one. He also works at the University of Szczecin.

Alanazi. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Curēus (Palo Alto, CA)*, *15*(10), e47026–e47026. https://doi.org/10.7759/cureus.47026

This source was about the growing number of cyberattacks that healthcare systems suffered which ranges from theft and damages. A study was conducted to see what clinical informaticians from a wide range of different fields of health science thought about the state of cybersecurity in healthcare by using the Delphi technique. The study results showed that majority of the participants, about 96 percent, thought cybersecurity is important for data protection. The author Abdullah T Alanazi is a part of the college of public health and health informatics in King Saud bun Abdulaziz University for Health Sciences. The article has referenced 30 other sources.

Snider, Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity (Oxford)*, *7*(1). https://doi.org/10.1093/cybsec/tyab019

This article asked the question of how does being shown cyberattacks affect the public’s support for more invasive cybersecurity policies? After the research it was that found that even more victims of cyberattacks. There was also showed that being exposed to a specific type of cyberattack let to being more support toward cybersecurity policies against that type. As the threat of cyberattack and criminal increasing in the future, so too will the public’s desire for there to be better and stronger regulations regarding cybersecurity policies. The authors of this article are: Keren L G Snider, Ryan Shandler, Shay Zandani, and Daphna Canetti. They are a part of the school of Political Science in the University of Haifa.