

Charles W. Pridgen

CYSE201S Cybersecurity & Social Science

Professor Matthew Umphlet

July 15, 2024

- Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7(1), tyab019.

The article, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," is about an experiment conducted on 1,022 Israeli participants for the purpose of providing insight on how the public is affected and reacts to hearing about lethal or non-lethal cybersecurity attacks, and how threat perception mediates either more or less support for different cybersecurity policies. The experiment included three types of cybersecurity policy which were, "cybersecurity prevention policy (CPP)," which involved the idea of the state mandating commercial companies to implement minimum levels of cybersecurity, "cybersecurity oversight policy (COP)," where the state would directly intervene in providing citizens with cybersecurity, an "cybersecurity alert policy (CAP)," which talked about the states presumed responsibility of alerting its citizens when a cyberattack has happened. The three major hypotheses for the experiment were, 1. exposure to cyberattacks, whether lethal or not, leads to increased support of cybersecurity policy compared to those not exposed to a cyberattack, 2. exposure to lethal cyberattacks will lead to more support for cybersecurity policies compared to those exposed to non-lethal cyberattacks, and 3. "Cyber threat perception will mediate

the relationship between individual exposure to cyberattacks and support for cybersecurity policies.” The participants were split into 3 groups, those who viewed a basic news coverage with very limited information of a lethal cyber-attack, a non-lethal cyber-attack, and a control group not shown any news coverage of a cyber-attack. At the beginning of the experiment, it was proven that the video stimulus gave rise to the differences in preferences for the cybersecurity policies and NOT from the participants economic/social backgrounds. Following that, the results of the experiment showed that for the group shown lethal cyberattacks, there was more support for (CAP) compared to the other two groups. For the non-lethal group, there was a great effect that led to the support for oversight policies (COP), but the overall exposure between both groups showed that whether lethal or non-lethal support for the oversight policies was the same. As far as threat perception, all three groups had great effect with the lethal group being the highest. This article provides insight on how the public reacts to cyber-attacks, showing that when exposed, people are more willing to give up civil liberties and welcome more government intervention.

- Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1), tyab021.

In the article, “Do breaches damage reputation? Evidence from 45 companies between 2002 and 2018,” by Christos Makridis, he states that there is little supporting evidence from companies experiencing data breaches that point to a decline in financial performance or security prices (Makridis, 1). Makridis provides us insight on 15 years of research, demonstrating how, despite increases in data breaches, companies are not incentivized to invest in more cybersecurity. Using data from 45 different companies,

Makridis shows that small to medium data breaches have insignificant economic effect, and on the contrary will have a positive effect. The only scenarios resulting in a negative effect are large data breaches on more salient companies. After providing a brief description of his findings, Makridis explains his data and measurements during his research followed by a section on the relationship between data breaches and intangible capital to understand the effect of data breaches on firm brand (Makridis, 2021). To finish the article, he concludes by reaffirming how only the largest, salient data breaches result in declines of intangible capital while smaller breaches have insignificant, but positive increases on intangible capital. This brings up the problem of companies not being incentivized to invest in proper cybersecurity which could potentially lead to national security vulnerabilities.

- Spithoven, R., & Drenth, A. (2024). Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality. *Journal of Cybersecurity*, 10(1).

In the article, “Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality,” by Spithoven, Remco and Drenth, Anthonie, they talk about an embedded experiment involving two phishing emails sent out to the employees of one of the 15 largest Dutch municipalities. The main goal of the experiment was to answer two questions; what group of employees run a higher risk of falling victim to phishing, and how effective is voluntary e-learning? According to their research, along with previous literature on the subject, Phishing is a

very popular worldwide affecting not only citizens, but entire organizations too. The authors define phishing as "... *'a scalable form of deception using the impersonation of an actor to obtain information from a target.'*" Before diving into the experiment, the authors provide background on previous scientific literature/empirical research on phishing. They provide information on what phishing is, human factors in phishing victimization, and measures against phishing. Once the background information was covered, the article goes on to explain the research set-up of the fieldwork study done on the municipal organization. By the end of the research experiment, 1437 participants were recorded. A table displaying the characteristics of the respondent groups like the variable and control group, gender, age, etcetera, were all provided. In the article, the author made sure to include the ethical considerations for the experiment due to the possible negative affects caused by deception, including an extensive debrief for the participants. Following the ethical considerations and participants, a section on the limitations of the experiment is included to cover things like what couldn't be fully explained during the experiment, and what measurements were actually accurate. Following the results of the phishing experiment, the article details what staff members completed the microlearning on phishing attacks. In conclusion, for this organization, results showed that older employees ranging from 40-70 years old, who have been in service with the company longer, and were full-timers fell for the phishing attempt higher than average, and it was deemed ineffective to implement the training on a voluntary basis. The end of the article includes discussion and suggestions for further research on the topic, and practical recommendations to raise awareness of phishing attacks for employees.

- Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. *Journal of Cybersecurity*, 6(1), tyaa015.

“Improving vulnerability remediation through better exploit prediction,” is an article by Jay Jacobs, Sasha Romanosky, Idris Adjerid, and Wade Baker that provides critical insight on technological exploit prediction. The authors inform the readers about the two problems faced by organizations; inefficiently consume large amounts of resources to patch low risk vulnerabilities or use a highly efficient strategy resulting in only a small number of high-risk vulnerabilities being patched, while still leaving many high-risk vulnerabilities open. The source explains that organizations currently use the Common Vulnerability Scoring System (CVSS) to remediate vulnerabilities above a certain severity score. Through their extensive research and data collection on real world or, “in the wild,” exploits, evidence reveals that very few published vulnerabilities have actually been exploited in the wild. Rather than organizations focus on random, possible exploits on known vulnerabilities based on a high CVSS severity score, the article focuses on empirical evidence gained by real world exploits observed in the wild and compiled into a dataset. To reinforce this claim, three remediation strategies were integrated with their new dataset combined with machine learning. The compiled data is explained to have been obtained from a partnering security company, along with other datasets, resulting in the most extensive dataset covering in the wild exploits which were previously unattainable. After that, the article breaks down their three key data sources used in their prediction models which were CVSS scores, published exploits, and reference tagging; also used as their three remediation strategies. In conclusion, the article

explains how vulnerability exploits that have occurred in the real world (in the wild) rather than publicly published, are far more reliable and efficient to use when making patching decisions.