Kenneth Fears
10/1/2024

Article #1 Review: Cyber Victimization in the Healthcare Industry

In this review, I will be analyzing the article “Cyber Victimization in the Healthcare Industry: Analyzing Offender Motivations and Target Characteristics through Routine Activities Routine Activities Theory (RAT) and Cyber-Routine Activities Theory (Cyber-RAT)” by Praveen, Y., Kim, M & Choi, K.

Identifying the working framework

The framework in the article is the Routine Activities Theory (RAT). This article states “Routine Activities Theory (RAT), introduced by Cohen and Felson in 1979, posits that crime will likely occur when three key elements—motivated offenders, suitable targets, and the absence of capable guardians—converge in time and space”(Praveen Y, Kim M, Choi K/2024). In the article it is learned that “the element of ‘absence of a capable guardian’ was not applicable.” (Praveen Y, Kim M, Choi K/2024). Making it more difficult to use the RAT framework, however the results still held up.

Data and Analysis

The big question being asked in the article is how and why these attacks are common within healthcare. To answer this question the writers captured the data using secondary data from a website called Hackmageddon. According to the article, “Hackmageddon compiles data on cyber-attacks, categorizing each incident by type, target industry, motivation, and outcome. It serves as a valuable resource for understanding and analyzing trends in cyber threats.”(Praveen Y,Kim M, Choi K/2024). With 76.1% falling into healthcare institutions such as critical care and patient services being the victims. Visualizing how the attacks arise on those in bad to terrible health.

Relation to Course

The article shows that about 60.9 of these attacks were for financial gain playing into how majority of these cyber crimes arise from needs of financial gain. More interesting data showed that about

8.9 percent of these attacks were known by the state. Playing into the political side of things that have been taught throughout the course. One sentence in the article states “Russia was identified as the country of origin in 84.1% of the cases driven by Financial Gain.”(Praveen Y,Kim M, Choi K/2024). Illustrating how countries play into the cybercrime side of things.

Conclusion

Given what is shown the RAT framework that was used was perfect in the study of these hacks on healthcare. With the data collected and analyzed it is found that most of these attacks happen on people using health institutions which makes them easier to attack. As well as showing that it is not just singular hackers but groups working for different countries in hopes of improving quality of life. With this data lots of new facts were learned about why attacks happen within the healthcare system. Which will allow the cybersecurity society to learn and adapt to these attacks which could help in avoiding these situations from arising in the future. From this we move one step closer to removing the chance of cyber attacks happening within healthcare.

Kenneth Fears
10/1/2024

Cites

Praveen, Y., Kim, M., & Choi, K.-S. (2024, September 16). *"Cyber Victimization in the Healthcare Industry: Analyzing Offender Motivations and Target Characteristics through Routine Activities Routine Activities Theory (RAT) and Cyber-Routine Activities Theory*. International Journal of Cybersecurity Intelligence & Cybercrime.

https://vc.bridgew.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&amp=&httpsredir=1&amp=&article=1060&amp=&context=commstud_fac