Article Review #2

Daelyn Bellamy

Department of cybersecurity

CYSE 201S Cybersecurity and Social Sciences

Today I will be reviewing two articles from the journal of cybersecurity one of them being "ransomware payments in the bitcoin ecosystem" and the other being "Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach". Using these two articles I will be going over the research questions, types of methods used, types of data and analysis done, how concepts in the article relate to things discussed in class, how topics relate to the principles of social science, and lastly the contributions the study brings to society. Now with all of that said I will start off with a summary of the two articles and then continue with each section of the paper in the order I listed them above.

First I'll be giving a quick summer of both articles. I'll be starting with the article "Ransomware payments in the Bitcoin ecosystem" In summary the arthur of this article is proposing a data driven method at which they can "identifying and gathering Bitcoin transactions, related to ransomware attacks, that goes beyond known clustering heuristics" (Paquet-Clouston et al. *Ransomware payments in the Bitcoin ecosystem*). The article "Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach" on the other hand the goal of this article is to "Our paper seeks to provide a general framework that can be easily applied to analyze different types of cyber breaches" (Goh et al. *Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach*). In this paper the authors have expanded the model of taxonomy in order to create a framework in which they can predict cyber breach outcomes, given the occurrence of a cyber breach, This as well as having a

"list of keywords that are useful in predicting the outcome type. We envision researchers, insurers, underwriters, and cybersecurity professionals can use (or expand on) our list of keywords, or use our method to yield their own set of keywords. Practitioners who seek to mitigate their cyber risk may use these keywords as a guide towards the specific attack surfaces that might be most susceptible to the corresponding breach"(Goh et al. *Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach*). Now that you have an idea of what both these articles are trying to accomplish we can now go into the next section of this paper.

Now I will be going over the hypotheses that both of these articles have and I will be starting with the first article "Ransomware payments in the Bitcoin ecosystem" The research question presented in this article by the arthur is if it is possible to create a data driven method for for identifying and gathering information on bitcoin transactions related to criminal activity(Paquet-Clouston et al. *Ransomware payments in the Bitcoin ecosystem*). The other article "Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach" however poses the question if its possible to build a framework that is capable of analyzing different cyber breaches (Goh et al. *Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach*). Now that you know what research questions were asked in each article let us go on to the types of researched methods used in each article.

I will first be looking at "Ransomware payments in the Bitcoin ecosystem" for the types of methods the authors have used in order to research. In this article the methods that the arthurs used to conduct this study was to extract bitcoin addresses from multiple different sources such as security researchers, blogs and websites. The addresses that were collected were from 67 ransomware families (Paquet-Clouston et al.). In this article "Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach" The arthur uses a sample dataset that consist of 3189 observations and a total of 39 features that can be included in their model (Goh et al. *Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach*).

In this section of the paper I will be going over the type of data and analysis done in each of the two articles I am reviewing. The first article I will be going over is "Ransomware payments in the Bitcoin ecosystem"The arthur in this article analyzes the data by "computed an outgoing-relationships graph for each family in the dataset and calculated the metric by applying the above definition"(Paquet-Clouston et al.). In total Arthur was able to find up to 2077 keys from the 35 families studied(Paquet-Clouston et al.). Now in the second article "Predictive

Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach” the arthur here analyze their data by first “identify the consistency in predictive accuracy of the LASSO under AIC” after this they took training and testing samples with 10 different seeds, which allowed them to test the stability of the models accuracy (Goh et al.).

The concepts that we discussed in class that I think best goes with this article “Ransomware payments in the Bitcoin ecosystem” is the concept of social systems within a structure and more specifically for this paper a family. The concept states that if one person gets malware on their computer then it's more likely for other people a part of that system to also get it. This relates to the article because if someone in a family gets ransomware it’s highly likely that everyone in that social system will also get it. Now for the second article “Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach” The concept that I think most relates to this article is the concept of “safe cities”. This relates to the article because Arthur is trying to develop a framework that can be used to analyze cyber breaches and then can be used by companies and organizations to see what part of their system is at most risk to a certain type of cyber attack(Goh et al.). This means that this type of framework can be very useful for people who are trying to build a cyber safe ecosystem within a city or anywhere.

Both of these articles in this paper relate to the principles of social sciences in different aspects. The article “Ransomware payments in the Bitcoin ecosystem” relates to the principle of criminology in the social sciences, because of the article's focus of trying to develop a “data-driven method for identifying and gathering information on Bitcoin transactions related to illicit activity based on footprints left on the public Bitcoin blockchain(Paquet-Clouston et al.)”. The other article “Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach” relates to the principle of sociology in the social sciences, because the arthur here is trying to create a “general framework that can be easily applied to analyze different types of cyber breaches(Goh et al.)”. I say this because the framework they’re working on has the possibility to help protect and build up our society's cyber security structure.

The contributions that the article “Ransomware payments in the Bitcoin ecosystem” has made to society has been great by developing a method that can identify and gather information on bitcoin transactions related to illegal activity at which then can be given over to law enforcement where then they can decide what actions is best to address the risk to public safety (Paquet-Clouston et al.). Now in the second article “Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach” the arthur here contributes to society by developing a framework that can analyze and different types of cyber breaches and then tell you which type of cyber breach your systems are most vulnerable to (Goh et al.). This framework is greatly beneficial to society because it gives companies and organizations a way to test for cyber attacks that they may not have fully protected themselves against.

In conclusion we have reviewed both the articles “Ransomware payments in the Bitcoin ecosystem” and “Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach”. In these articles we have reviewed the research questions that these articles have presented to us, as well as the types of research methods the arthur’s used, the type of data and analysis done, how these articles related to things in class, how they relate to the principles of social sciences, and lastly their contributes to our society. Both the articles in this paper have given us knowledge and insight into the world of cyberspace that is greatly needed by society in order to better protect us online.

REFERNANCES:

Paquet-Clouston, Masarah, et al. “Ransomware Payments in the Bitcoin Ecosystem.” *Academic.Oup.Com*, academic.oup.com/cybersecurity/article/5/1/tyz003/5488907?searchresult=1#135506148. Accessed 4 Nov. 2023.

Goh, Jing Rong, et al. “Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach.” *Academic.Oup.Com*, academic.oup.com/cybersecurity/article/9/1/tyad015/7241616. Accessed 4 Nov. 2023.