ABSTRACT

This investigation explored the topic of cybercrime and its relation to disaster events of natural or man-made origin within the United States from the years 2001 to 2016. By analyzing available public data from both the Federal Bureau of Investigation (F.B.I.) and the Federal Emergency Management Agency (F.E.M.A.), using descriptive statistics to find evidence of any possible correlation between disaster events and cybercrime. The results suggest that disaster cybercrime and cyberwar are loosely related, with the exceptions of regions with an already higher risk of disasters and cybercrime such as the states of Texas and California.

INTRODUCTION

An area that merits attention given the series of natural disasters many countries have experienced in the last twenty years is cybercrime and cybersecurity as they relate to these. During this kind of event infrastructure suffers from power outages, loss of communication, missing personnel, and structural damage which in turn can lead to poor securment of data and assets. An example of the possible dangers can be seen in the U.S. where, before and during Hurricane Irma, many web domains of questionable origin were bought with the intent of disguising themselves as non-profit organizations to steal money from unware users (MS-ISAC, 2017, p.1). Furthermore, these are not isolated incidents; similar events were observed during the passage of Hurricane Katrina (Carlson, Noble, Taft, 2005, p.11-12). Our research questions then are: How prevalent are these attacks during disasters? Are computer systems users at higher risk of becoming victims to cyber crimes as a result of natural or man-made disasters? This investigation is an exploratory research to address these questions.

RESULTS

Using the available data an overall pictures of the behavior of disasters and cybercrime in the United States is presented. The total amount for cybercrime each year follows a growing trend. In contrast, it seems there has been a steady decline in the amount of annual disasters reported from 2001 to 2016.

We found that, on average, most states have a low percentage of cybercrime, varying from 0.30 to 5.00 with only three outliers being New York (5.11), Texas (6.94) and California (14.24). By separating these and into two groups and comparing their annual amount of recorded disasters with their annual percentage of annual cybercrime from 2001 to 2016, it was apparent that states with lower percentages of annual cybercrime tended to have even lower percentages of cybercrime when exposed to higher amounts of disasters (figures below). In contrast, we found that states with already high annual percentages of cybercrime and higher amount of disasters tended to have, on average, higher amounts of cybercrime when exposed to higher amounts of disasters (figures to the right).

We obtained annual reports on cybercrime dated from 2001 to 2016 through the FBI’s IC3 website. A copy of FEMA’s Disaster list (dataset lists all official FEMA Disaster Declarations last updated on 3.6.2017). The data in its raw form consisted of 47768 entries. The disaster list data set was uploaded to a database using the “Oracle 12c Database” software. This was done for the easy manipulation of data and for the creation of useful new summarized datasets.

Using descriptive statistics on available and produced datasets the following analysis could be made:

• View of the annual cybercrime trends based on data
• View of the annual recorded disasters
• Reports on Average, Standard Deviation, and T-Test on Percentage of Cybercrime per State
• Time series report on cybercrime from 2001 through 2016
• Determination high risk states
• High risk states examination

CONCLUSION

The results obtained show that, in the US, disasters may be used as leverage for cybercrime in areas with high amounts of cybercrime and higher risks of disaster occurring. Meanwhile, the evidence suggests that states with low amounts of cybercrime and lower risk of disasters, have less cybercrime reported when subjected to higher amounts of disasters. In general, cybercrime throughout the US is increasing while each state’s annual percentage of cybercrime is relatively static. This suggests that the effect of disasters on a state’s annual cybercrime amount may be significantly small in comparison to a states total cybercrime amount.

References