Data Analysis: Disasters, Possible Leverage for Cybercrime

Author: Isaac L. Torres Torres   **Mentor: Prof. Zayira Jordan**

POLYTECHNIC UNIVERSITY OF PUERTO RICO, UNDERGRADUATE RESEARCH PROGRAM: HSI STEM GRANT

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 Investigacion (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 cybercrime 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 securement 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 unwary users (MS-ISAC, 2017, p.1). Furthermore, these are not isolated incidents; similar events were observed during the passage of Hurricane Katrina (Carlson, Nobel, 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 computer crimes as a result of natural or man-made disasters? This investigation is an exploratory research to address these questions.
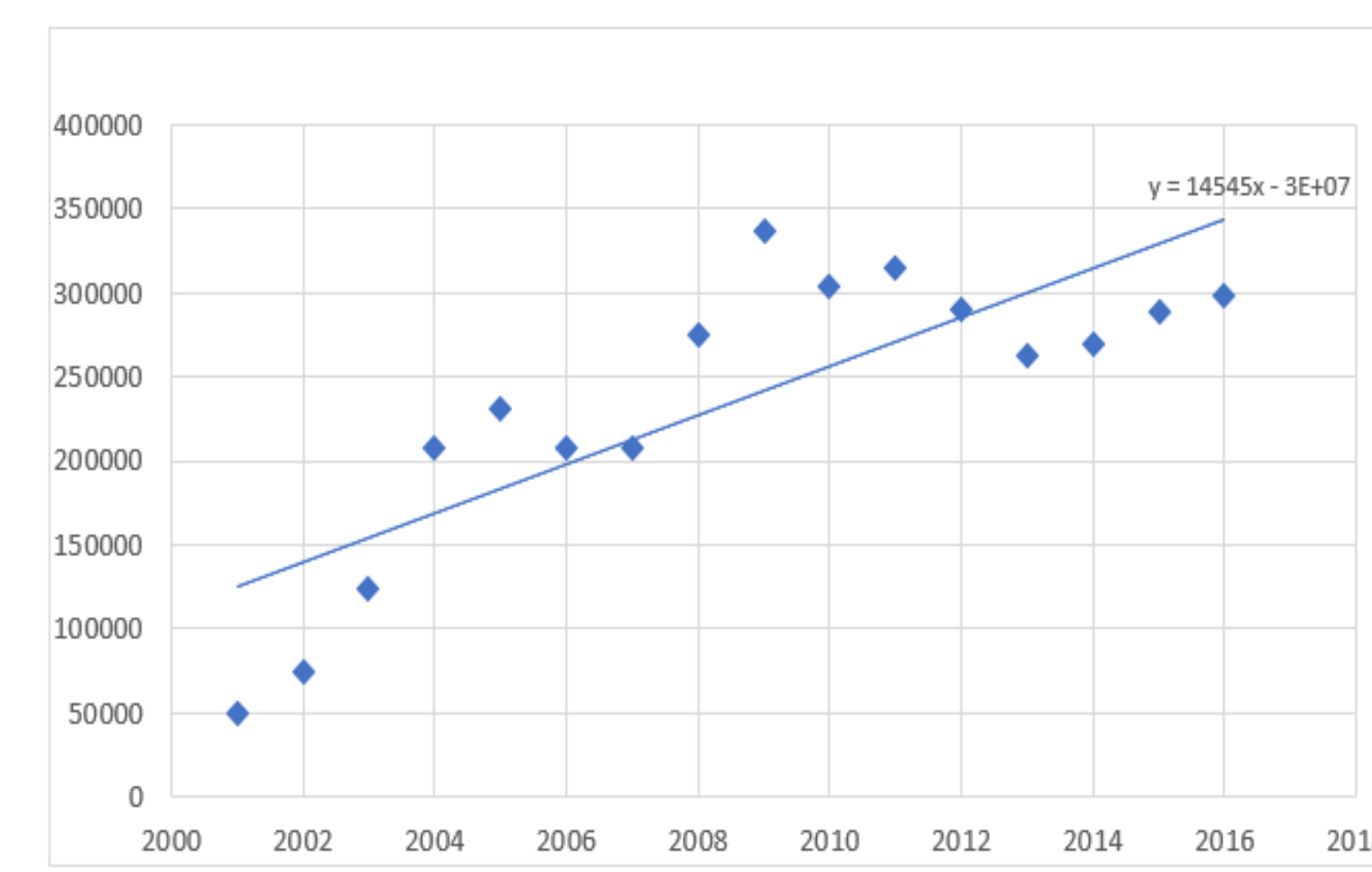
RESULTS

Total amount of declared disasters per year from 2001 to 20016.
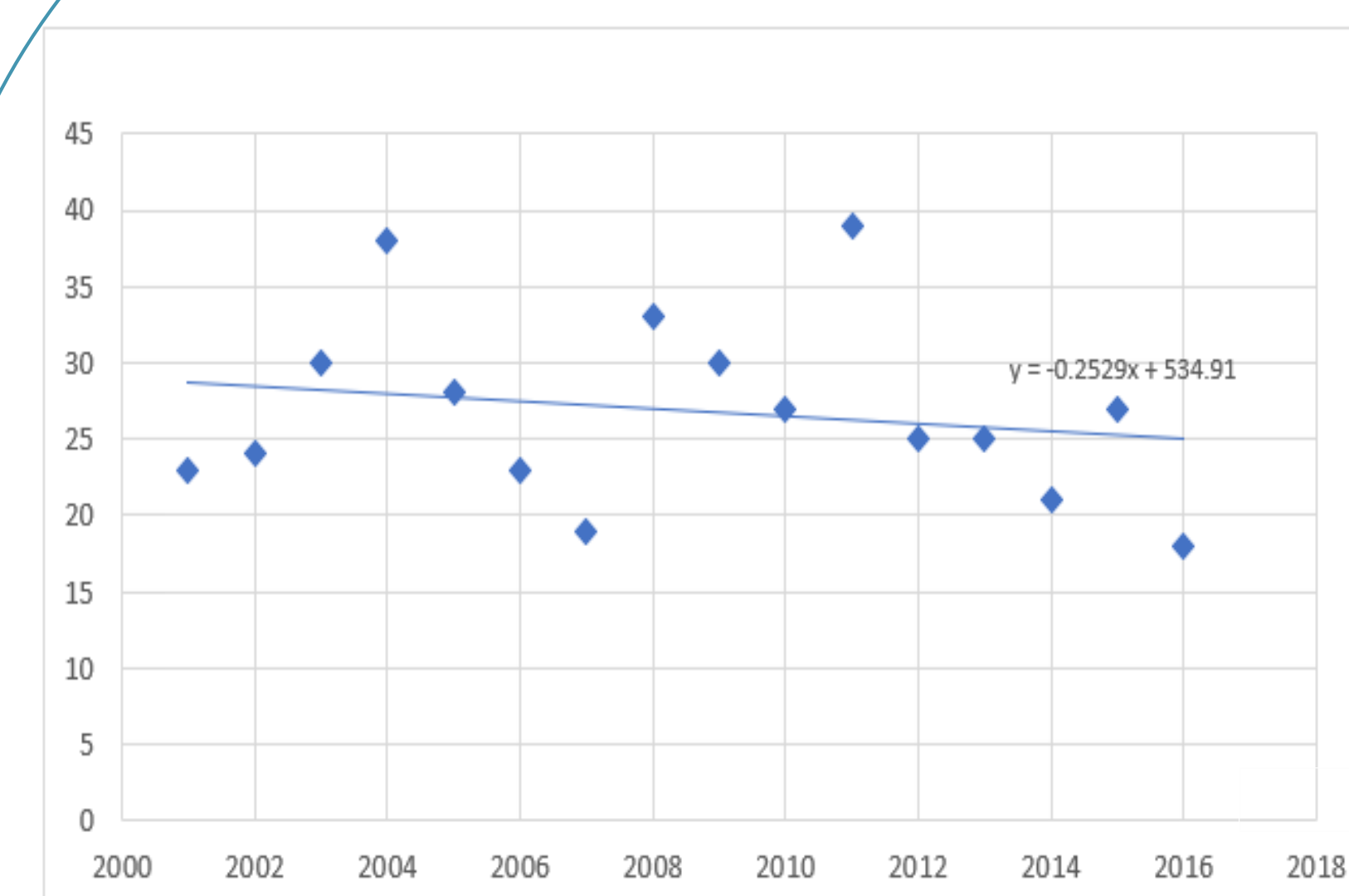
Using the available data an overall picture of the behavior of disasters and cybercrime in the United States is presented. The total amount for cybercrime each year follows a growing trend. In contrast, it seems there has been a steady decline in the amount of annual disasters reported from 2001 to 2016.

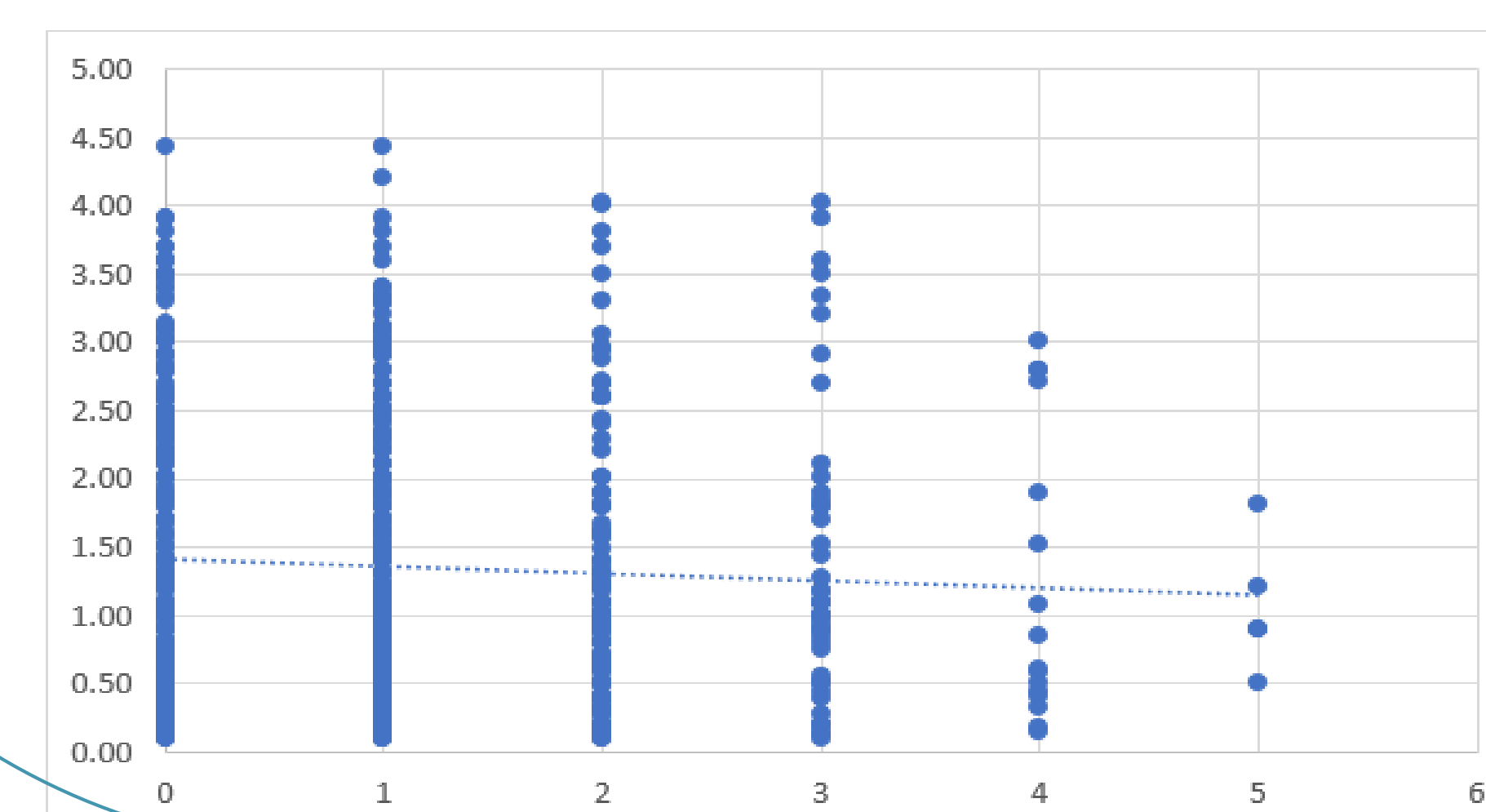Total amount of reported cybercrime per year from 2001 to 20016.

T-test results comparing each year with the following year.

Statistic	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Mean	1.982	1.992	41.24902	41.24902	1.994	1.994	1.992	1.992	1.887	1.887	1.9932	1.9892	1.8028	1.8028	1.849
Variance	7.363547	6.188506	78594.39	78594.39	5.369555	5.369555	5.897894	5.897894	6.527356	6.527356	5.570285	5.570285	4.954865	4.954865	7.48305
Observations	50	50	51	51	50	50	50	50	50	50	50	50	50	50	50
Pooled Variance	6.776027	6.151333	39697.16	39696.93	5.505218	5.603653	5.867822	5.840231	6.154962	5.582417	5.103881	6.526668	6.218958	5.262575	6.526668
Hypothesized M.D.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
df	98	98	99	99	98	98	98	98	98	98	98	98	98	98	98
t Stat	-0.01921	0.02016	0.990279	0.988716	-0.10655	-0.0169	-0.02064	0.028966	-0.1834	0.162948	0.396605	0.274393	-0.09263	-0.40627	-0.27439
P(T<=t) one-tail	0.492357	0.491978	0.162226	0.162606	0.457682	0.493276	0.491787	0.488475	0.427432	0.435447	0.346261	0.39218	0.463193	0.342714	0.39218
t Critical one-tail	1.660551	1.660551	1.660391	1.660391	1.660551	1.660551	1.660551	1.660551	1.660551	1.660551	1.660551	1.660551	1.660551	1.660551	1.660551
P(T<=t) two-tail	0.984714	0.983957	0.324452	0.325211	0.915364	0.986553	0.983574	0.976951	0.854863	0.870895	0.692521	0.784361	0.926386	0.685429	0.784361
t Critical two-tail	1.984467	1.984467	1.984217	1.984217	1.984467	1.984467	1.984467	1.984467	1.984467	1.984467	1.984467	1.984467	1.984467	1.984467	1.984467
S. Different	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No

Analyzing the percentage of cybercrime in each state vs the following year through the use of t-test statistical analysis, we can see that each test's t-value was within the calculated critical two tail value. With this, we concluded that the values are not statistically different, therefore no event or combination of events has been able to change significantly the distribution of cybercrime among the 50 states of the US.

We found that, on average, most states have a low percentage of cybercrime, varying from 0.10 to 3.60 with only three outliers being New York (6.11), 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 cyber crime 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 (figure 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).

Number of disasters vs annual percentage of cybercrime: Texas 2001-2016.
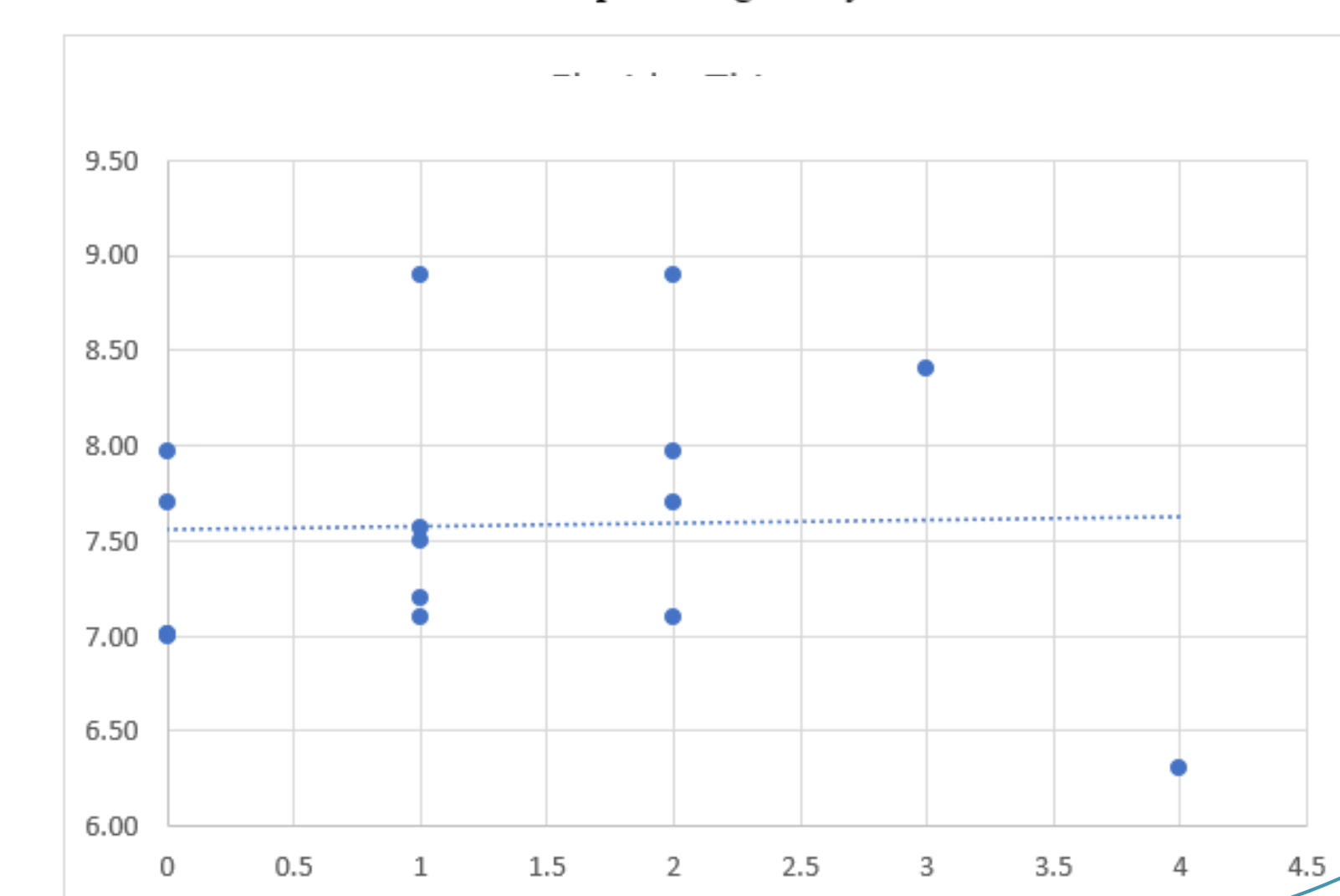

Number of annual disasters affecting each state vs percentage of annual cybercrime for each state from 2001 to 2016 (Excluding Outliers).
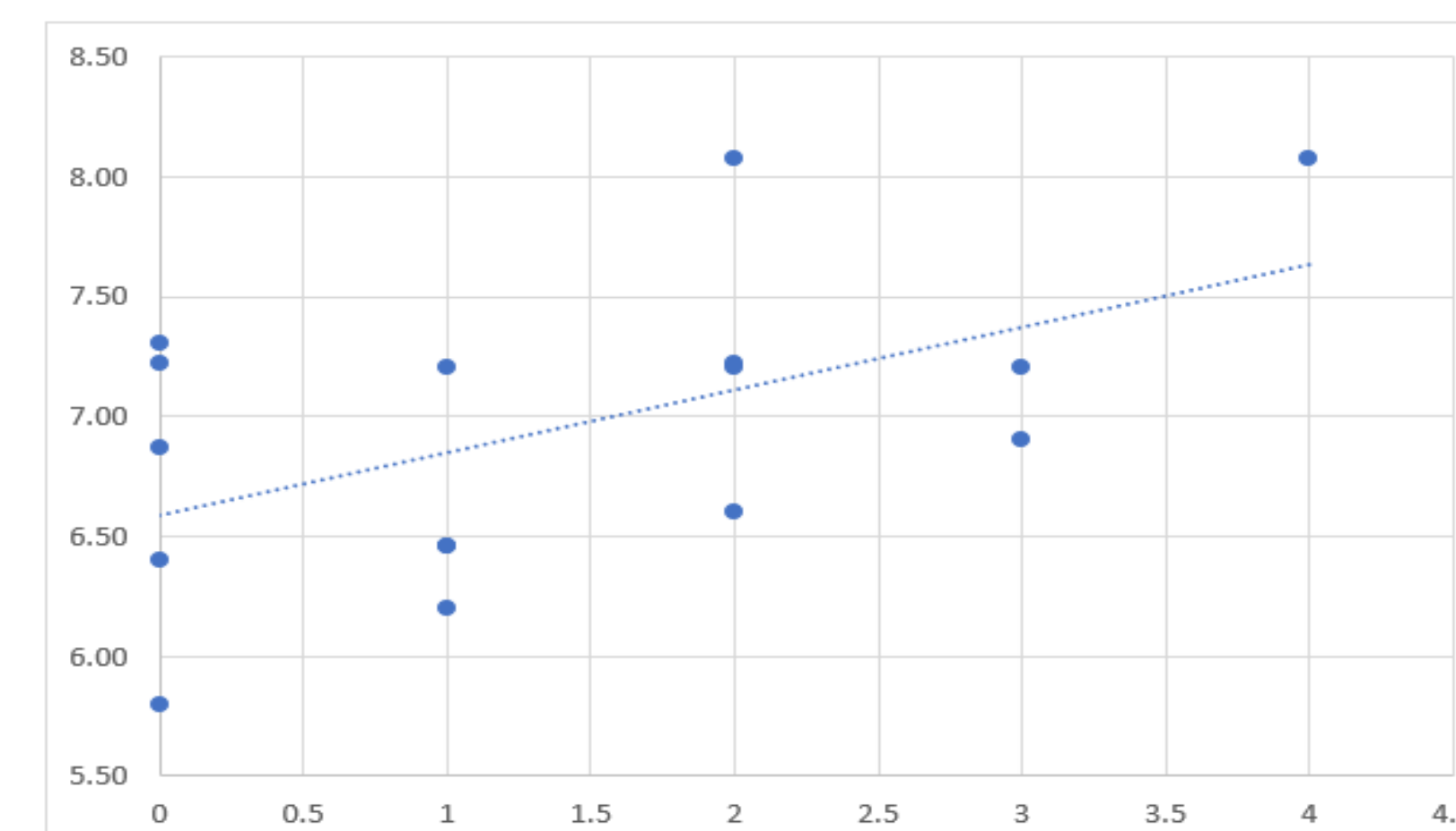
Number of disasters vs annual percentage of cybercrime: Florida 2001-2016.

METHODOLOGY

We obtained annual reports on cybercrime dated from to 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, if any, of disasters on a state's annual cybercrime amount may be significantly small in comparison to a states total cybercrime amount.

References

- Carlson, B. C., Nobel, C., Taft, D. K., Katrina, C., & Roberts, B. P. F. (2005). Cyber-looters capitalize on Katrina. eWeek, 22(36), 11–12. Retrieved from http://ezproxy.pupr.edu:2067/ehost/d etail/detail?vid=29&sid=d52f8802-b624-4d1e-9978-13758a8336bc%40sessionmgr104&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3D%3D#db=cph&AN=18329718
- "Cyber Alert: Cyber Threat Actors Expected to Leverage Hurricane Irma," MS-ISAC, 2017. [Online]. Available: https://www.cisecurity.org/ms-isac/cyber-alert-cyber-threat-actors-expected -to-leverage- hurricane-irma/. [Accessed: 08-Sep-2017]