8-10-2022

# Characterizing Data Breach Severity: A Data Analytics Approach

Amir Zadeh
*Wright State University*, amir.zadeh@wright.edu

# Characterizing Data Breach Severity: A Data Analytics Approach

*TREO Talk Paper*

**Amir Zadeh**
Wright State University
amir.zadeh@wright.edu

## Abstract

Data breaches have been causing havoc for many years and continue to rise as organizations find new ways to do business using technology. Companies spend time finding ways to protect themselves from data breaches. Cybersecurity communities share and network with one another to stand against the one that thrives to take organizations down. Avoiding data breaches remains to be a top priority and companies need to resolve a data breach dispute as soon as it happens. Resolving data breaches as soon as they happen is an important task and requires a quantitative prediction of breach likelihood to mitigate risk and prepare for response (Jeyaraj et al. 2021). Data breaches can be due to unintended disclosure (DISC), Hacking or malware (HACK), payment card fraud (CARD), insider accessing sensitive information (INSD), loss or stolen assets or records (PHYS), loss of portable devices (PORT), and loss of stationary digital equipment such a server (STAT) (Ayyagari 2012). In this study, a Cyber Security Risk Quantification and Mitigation Framework is discussed. First, a breach level index model is introduced to quantify and classify the severity of a data breach incident based on the type of data asset, account details, or financial details, which was exposed. Then, a likelihood-Impact analysis is discussed to assess the risk involved in each type of data breach. The proposed framework is applied to data breaches gathered from S&P 500 organizations to prescribe strategies that can help firms reduce the likelihood and impact of data breaches. Our results suggest that hacking and malware need to be reduced as they are the highest impact and highest probability when it comes to a data breach. The results of this study help organizations identify the likelihood and impact of a data breach and determine a plan of action on how to mitigate the risks. An interactive Tableau dashboard is built which can serve as a valuable tool to estimate the risk and impact of various types of data breaches. Implications for research and practice are discussed.

**Keywords:** Cybersecurity, Data breach, Data visualization, Breach severity, Content analysis

# REFERENCES

[1] Jeyaraj, A., A. Zadeh and V. Sethi (2021). "Cybersecurity threats and organisational response: textual analysis and panel regression." *Journal of Business Analytics* 4(1): 26-39.

[2] Ayyagari, R. (2012). "An exploratory analysis of data breaches from 2005-2011: Trends and insights." J*ournal of Information Privacy and Security* 8(2): 33-56.