Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 1, 2021

An examination of historic data breach incidents: What cybersecurity big data visualization and analytics can tell us?

Emily Africk, USA, eafrick@umich.edu

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Abstract

Data breach incidents are reported in the media to be on the rise with continuously increasing numbers. Additionally, data breaches serve a major negative impact to organizations. This study focuses on combining experience in data analytics, visualization, and quantitative analysis for business intelligence in the context of cybersecurity big-data over a period of 15-years. A large data set containing 9,015 data breaches was provided via the Privacy Rights Clearinghouse data breach database from the start of 2005 to the end of 2019. The aim of this work was to slice the data as well as represent it into a business-related visualization using time-series analysis that can help executives understand complex cybersecurity breaches, their impact, and their trend over time. We have created visualization figures along with explanations of what each visualization means in the context of cyber-attacks over time. This project was set to serve as a breakdown of the important findings from the Privacy Rights Clearinghouse data breach database of over 15-years. These findings are communicated through both key numbers and quantitative analyses for business intelligence. While our project does not cover every aspect of the dataset (due to its significant size), it serves more as a focus on one particular part of the data: incident types and their volume over the 15-year timeframe to help business executives visualize cybersecurity trends. This paper ends with a conclusion and discussion on how such cybersecurity visualizations can help industries along with future research needed.

Keywords: Cybersecurity data analytics, data breach incidents, visualizations of data breaches, cybersecurity big data, time-series analysis of data breaches.

Introduction

Cybersecurity breaches have been reported in the news and other outlets to be growing by the day (Privacy Rights Clearinghouse, 2018). Moreover, the impact of cybersecurity on companies from all sectors is significant (Hovav & Gray, 2014). According to the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3), cyber-attacks and data breach incidents "continues to grow and evolve, targeting small, medium, and large business and personal transactions" (Federal Bureau of Investigation, 2018). While there are several reports on the increase of data breach incidents over the years, there appears to be a lack of clear visualizations on how such cyber-attacks have evolved, especially when it comes to the specific major sectors that such attacks are impacting. Cybersecurity analysts are bombarded with too many security alerts and are left to sort through information in order to correctly identify cyber-attacks (Goode & Levy, 2017). Thus,

this paper was set to serve as a breakdown of the important findings from the Privacy Rights Clearinghouse data breach database of over 15-years. These findings are communicated through both key numbers and quantitative analyses for business intelligence. While this study does not cover every aspect of the dataset (due to its significant size), it serves more as a focus on one particular part of the data: incident types and their volume over the 15-year timeframe. The Privacy Rights Clearinghouse data breach database has been accumulating data about reported data breaches on a daily basis (Privacy Rights Clearinghouse, 2018). However, in order to provide accurate information when looking at visuals, this project focuses on the 15-years between the start of 2005 and the end of 2019. At the time of data analysis, there were not all 12 months of 2020 data recorded yet; thus, 2020 data was not included in this study, rather the 2005-2019 full years. The following is the main Research Question (RQ) that this study was addressing:

> RQ: What are the overall big data trends emerging from 15 years of data breach incidents as documented by the Privacy Rights Clearinghouse?

The remainder of this paper is organized into the following sections. In the Literature Review, we discuss relevant literature for three topics: data breaches, data visualization, and executive dashboards. The Methodology section provides an explanation of the dataset and further explain the time-series analysis that we performed. The Results section discusses key findings and provides relevant figures. This paper closes with the Conclusion and Discussion section, providing a brief overview of what we found as well as a discussion of study limitations and recommendations for future research.

Literature Review

Below we have provided a brief overview of the relevant literature related to data breaches, data visualization, and executive dashboards. The Data Breaches section starts with a definition of the term and discusses the massive dataset used from the Privacy Rights Clearinghouse along with a brief note on the ramifications of data breaches. The Data Visualization section then discusses the term, how it can be helpful, especially with the use of time-series visualizations in finding trends and explaining larger datasets. We believe that time-series visualizations are greatly helpful as a tool for executives to understand various concepts, as has been over the past several decades with executive dashboards of Decision Support Systems (DSSs). As such, when it comes to data breaches and their impact over time, executive dashboards are included in our discussions of the literature given that we feel it can provide a context for communicating our findings with executives.

Data Breaches

The Privacy Rights Clearinghouse (2019) defined a data breach as "a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual" (para. 1). According to Privacy Rights Clearinghouse (2019), a data breach can be a result of hacking, theft of credit/debit card numbers, lost, discarded or stolen documents/devices, or mishandled sensitive information. The rise of the information age brought the ability for cyber criminals to conduct large scale data breaches (Peretti, 2009). Cyber criminals have figured out how to hack systems and steal data, therefore, causing the potential for breaches

to leak personal data across the Internet. Such data breaches then serve as an ongoing "security and privacy threat for Internet users" (Karunakaran et al., 2018, p. 217). These breaches cause a greater impact than that of a physical incident; physical incidents present clear damage, while data breaches do not (Hovav & Gray, 2014). The research findings and information discussed in this paper explicitly look at data breach trends over a 15-year period, both overall and in each industry.

Data Visualization

According to Telea (2015), "the purpose of visualization is to get *insight,* by means of interactive graphs, into various aspects related to some process we are interested in" (p. 3). Data visualization is simply a more specific way of using visualizations. It is a technique to analyze big data in a visual manner. In other words, "data visualization concerns the manipulation of sampled and computed data for comprehensive display" (Bajaj, 1998, p. 1). Visualizations of big data are extremely important in order to capture the attention of the audience and communicate findings in a short amount of time. Furthermore, visualization also plays a role in "driving complex analyses" (Keim et al., 2013, pp. 20-21). Data visualization has the ability to help executives in terms of decision making by making sense of data and "build[ing] bridges and make[ing] approaches and/or results accessible and usable to others" (Hartung, 2018, para. 6). According to Boumans et al. (2020), data visualization and quantitative analysis can allow business executives to perform "more accurate 'what if' analyses" by "providing essential information to guide long-term sustainability analysis and planning" (para. 6).

Through the utilization of time-series analysis based on data visualizations and analytics, executives are able to "obtain an understanding of the underlying forces and structure that produced the observed data" (NIST, n.d., para. 3). Furthermore, by looking at "a set of observations taken over a series of equally spaced time periods," executives can look at the "dependence between observations to better predict what the series will look like in the future" (JMP, 2021, para. 1). They can assess the performance of different time-series models in order to determine which model is best suited to predict future years of data breach incidents based on this data.

Executive Dashboards

Resnick (2003) defined executive dashboards as "systems that provide business intelligence to company executives and managers by presenting data from a wide variety of sources in ways that support effective monitoring and decision making" (p. 1639). Executive dashboards allow business executives to identify problems and trends in data early enough to make decisions accordingly. Thus, executives are able to "recognize [the] situation and diagnose the cause and then [support] the development of solutions" (Resnick, 2003, p. 1639). For each executive, the dashboards can be customized to fit their specific needs. In this study, we conceive executive dashboards that will expand the time-series visualizations we've done here to significantly help them make better and faster decisions assisted by the historic data breach trends over the past 15-years. Additionally, according to Person (2013), "surveys have shown that two of the key benefits of implementing dashboards are faster decision-making and reduced administrative work in research and analysis" (para. 1).

Methodology

The methodology used in this research study is quantitative time-series analysis following traditional big data visualization, with emphasis on visual pattern recognition from the time-series analyzed. Quantitative time-series analysis helps us visualize larger volumes of data over time. The visualizations are not precise, but rather they provide visual representation to extrapolate and understand trends in the data. The dataset for the visualizations was obtained from The Privacy Rights Clearinghouse in order to develop the time-series graphs.

Table 1. Acronyms and Descriptions for Data Breach Types from the Privacy Rights Clearinghouse Dataset

Acronym	Description
CARD	Payment Card Fraud
HACK	Hacking or Malware
INSD	Insider
PHYS	Physical Loss
PORT	Portable Device
STAT	Stationary Device
DISC	Unintended Disclosure
UNKN	Unknown

The dataset contained 9,015 total recorded cybersecurity data breaches between 2005 and 2019 (complete years). The year 2019 was the last complete year available in the database, and therefore, it was the last data year used in this study. The Privacy Rights Clearinghouse first organizes data breaches by breach type. The eight types of breaches documented are: Payment Card Fraud (CARD), Hacking or Malware (HACK), Insider (INSD), Physical Loss (PHYS), Portable Device (PORT), Stationary Device (STAT), Unintended Disclosure (DISC), and Unknown (UNKN). Payment Card Fraud (CARD) refers to any fraud that is done using debit and credit cards, not through hacking. Hacking or Malware (HACK) can be accomplished through a third-party hacker or being infected by the malware. Insider (INSD) breaches happen when an authorized user from the organization accesses information or systems to conduct malicious activities. Physical Loss (PHYS) refers to the loss of any paper documents, meaning they are discarded or stolen. Portable Device (PORT) refers to the loss, whether it be discarded or stolen, of a device that contains organizational information and/or access to organizational systems. Stationary Device (STAT) refers to the loss of a stationary computer, whether it be discarded, illegally accessed, or stolen. Unintended Disclosure (DISC) breaches happen when sensitive information is released to the wrong party. Unknown (UNKN) breaches are those which do not fit into any of the previously mentioned seven breach types. Furthermore, the data breach records were subdivided by industry type. These eight industry types are: Business- Financial and Insurance Services (BSF), Business-Other (BSO), Business- Retail/Merchant- Including Online Retail (BSR), Educational Institutions

(EDU), Government & Military (GOV), Healthcare, Medical Providers & Medical Insurance Services (MED), Nonprofits (NGO), and Unknown (UNKN).

Results

Visuals

To initiate the visualization process for the data, basic numbers and breakdowns were calculated. Of the total 9,015 recorded breaches, the types of data breach incidents (in order of size) were due to: 28.10% HACK, 20.64% DISC, 19.22% PHYS, 13.00% PORT, 7.81% UNKN, 6.72% INSD, 2.76% STAT, and 0.75% CARD (see Figure 1a). Moreover, when assessed via the breakdown of records by industry type, the overall data breaches were across (in order of size): 48.18% MED, 11.59% BSO, 9.41% EDU, 8.73% BSF, 8.66% GOV, 6.91% BSR, 5.20% Unknown, and 1.32% NGO (see Figure 1b). As the data indicates, an overwhelming amount of data breach incidents (4,343) stem from Healthcare, Medical Providers, and Medical Insurance Services.

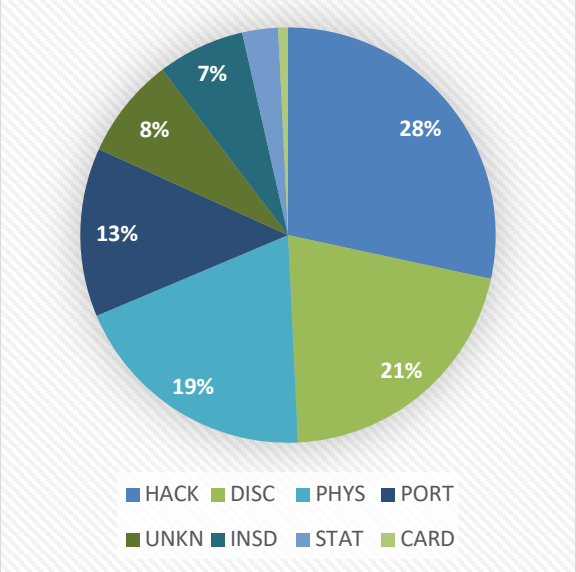

Figure 1a. Types of Data Breach Incidents Recorded (N=9,015)

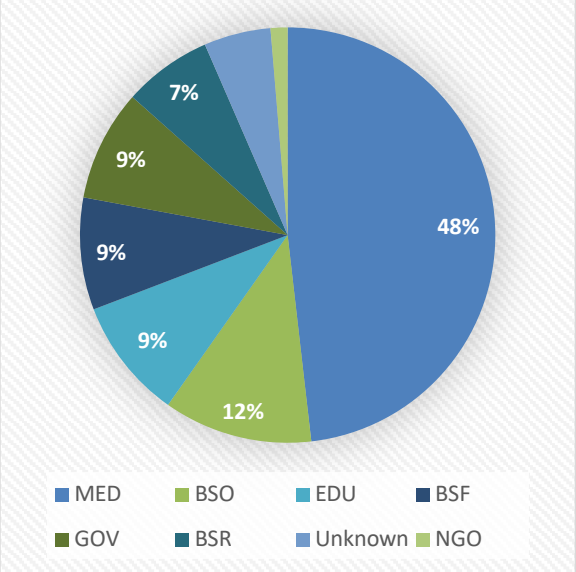

Figure 1b. Breakdown of Records by Industry Type (N=9,015)

The significance of the study is to help understand the trends in data breaches, especially for executives as it pertains to their industry, and the different types of cyber-attacks. Following extensive data manipulations using time-series analysis, it was made clear that the most important aspect of the data to visualize was a breakdown of a separate plot for each data breach type showing the number of breaches recorded for the particular breach type over the 15-years (2005-2019). As an overall picture of the big data, we have also included a visual (See Figure 2) representing the total number of breach incidents at each given year. The next eight figures (See Figure 3 to Figure 10) are the time-series analyses for business intelligence for each specific type of data breach, following the same format as the overall one in Figure 2.

Using advanced Microsoft Excel visualizations, we manipulated the dataset of over 9,000 rows into the relevant subcategories: *data breach type* and *industry type*. From there, we further broke down the data of interest into subcategories and developed the time-series displays of our findings. The data analysis comes from the overall observation of the eight different figures separated by type of breach (See Figure 3 to Figure 10). Figures 3, 5, and 6 are similarly shaped, with the years of highest number of records in the middle interval of years and less on either tail nearing towards 2005 and 2019, which may indicate that when recording of data breach incidents started and in recent years, these overall number of records were reduced in the tail ends of the 15-years internal investigated. Figures 4, 9, and 10 are all skewed to the left indicating an overall increase in the data breach incidents over the 15-years period. Another general statement that can be made about Figures 4, 9, and 10 is that the years of highest number of records are more focused on the latter half of the 15-years reporting period. Figures 7 and 8 are both skewed to the right. Unlike the ones that are skewed to the left, Figures 7 and 8 have the years of highest number of records more heavily represented in the first half of the 15-years reporting period. This may indicate that either these types of attacks have reduced due to added information security tools or the use of such threat vectors demonstrated to be less "valuable" to cyber criminals, so they are focused on conducting the cyber-attacks that provide them more financial benefits (Tariq, 2018).

We see a big jump from 2009-2010 in Figures 2 and 6, and this is the same time that a U.S. Regulation was put into place. The Cybersecurity Act was designed in 2009 and was signed in 2010 (111th Congress, 2010). In Figure 5, we see the start of a dip in 2013, and this is the same year of the 2013 Cybersecurity Executive Order (Fischer et. at., 2014). In 2015 we see a major dip in Figure 2. This may be due to the Cybersecurity and Information sharing act, which was introduced in the U.S. Senate in 2014 and signed in 2015. Finally, we see low numbers of reported data breaches in 2019 across Figures 2 to 10. We might be able to justify this dip due to the establishment a new federal agency, the Cybersecurity and Infrastructure Security Agency (CISA), in November 2018 (U.S. Department of Homeland Security, 2018).

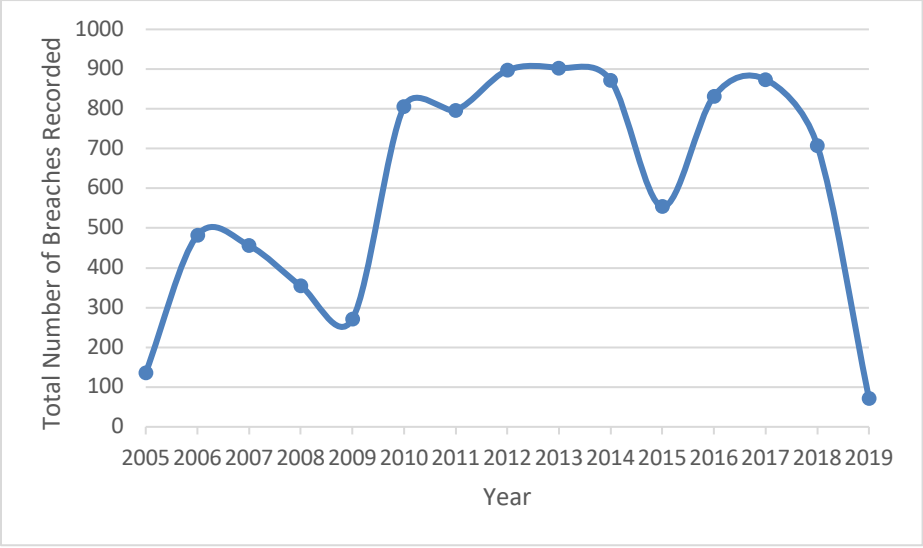

Figure 2. Total Number of Breach Incidents Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

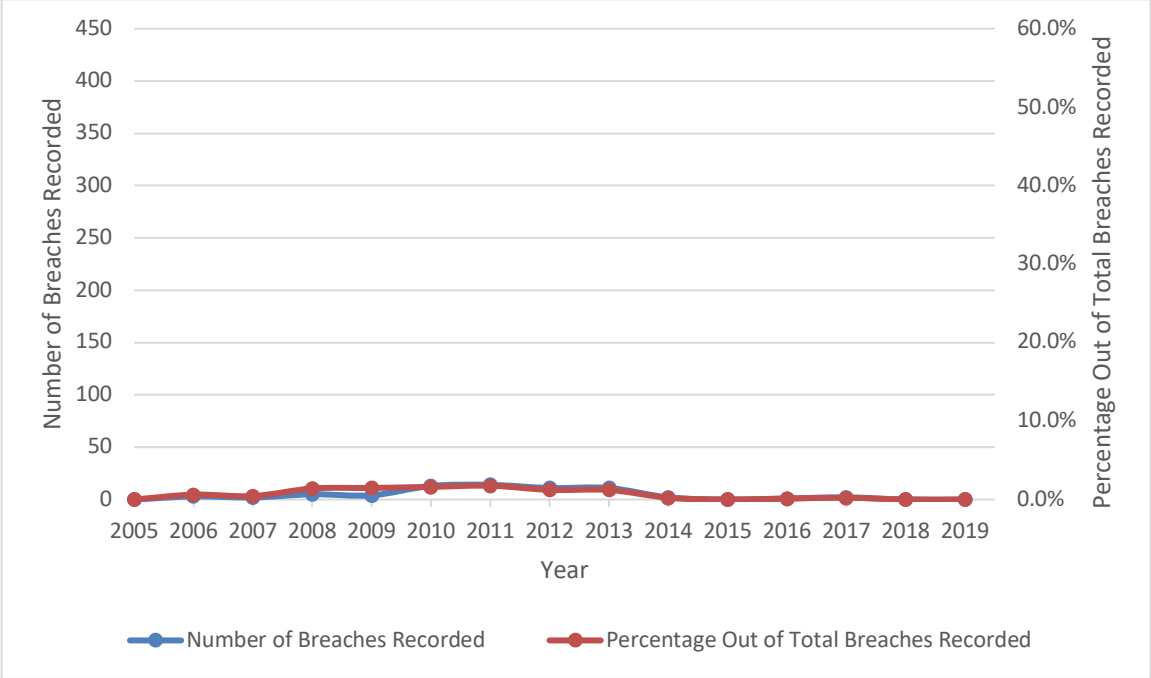

Figure 3. Payment Card Fraud Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

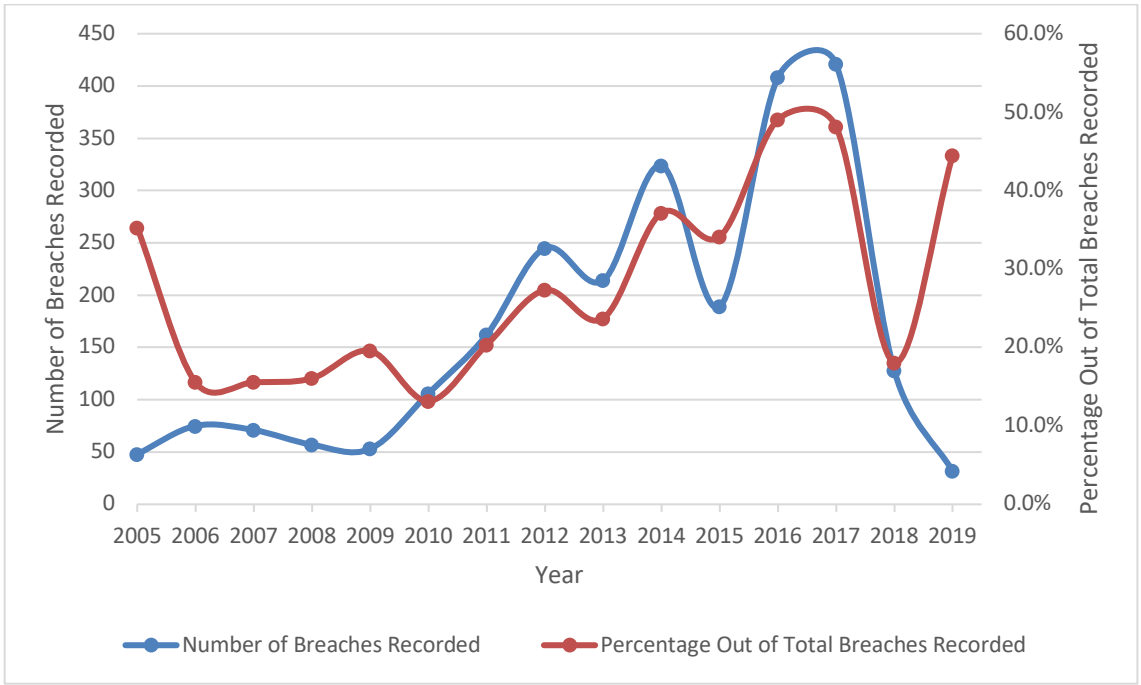

Figure 4. Hacking or Malware Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

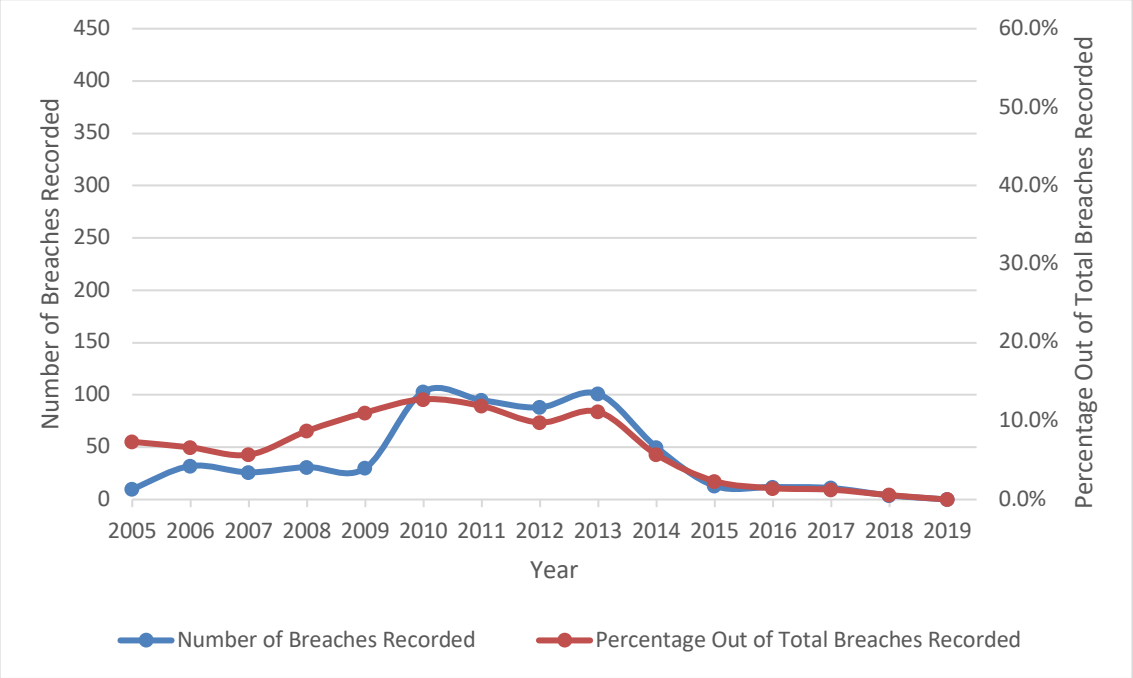

Figure 5. Insider Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

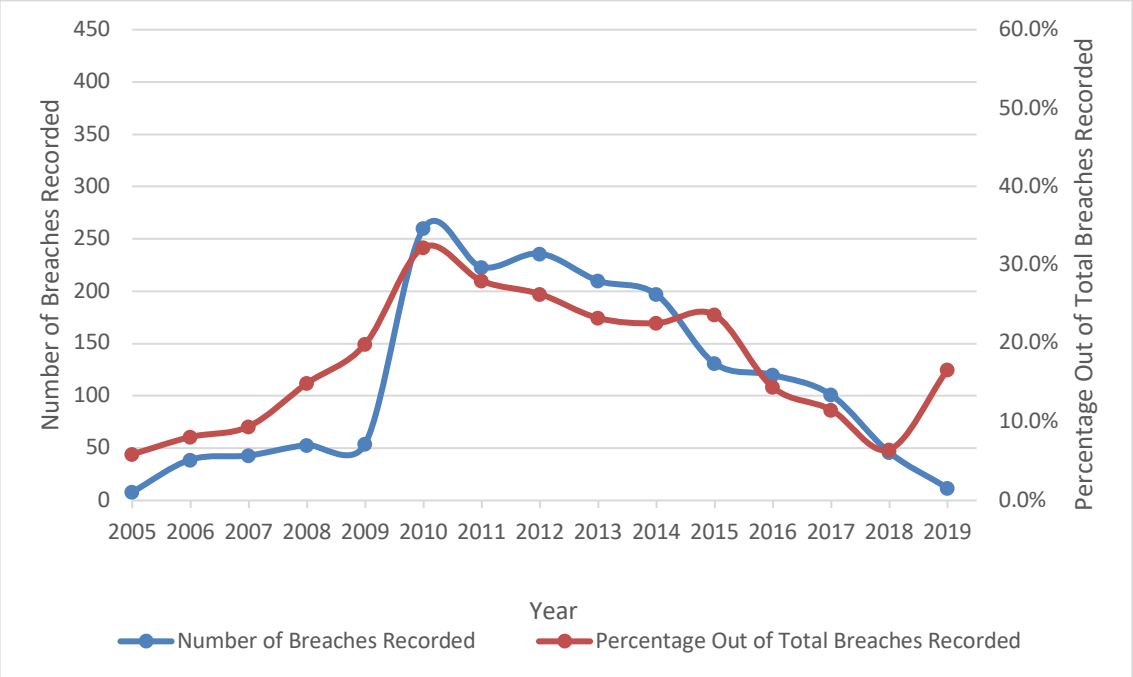

Figure 6. Physical Loss Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

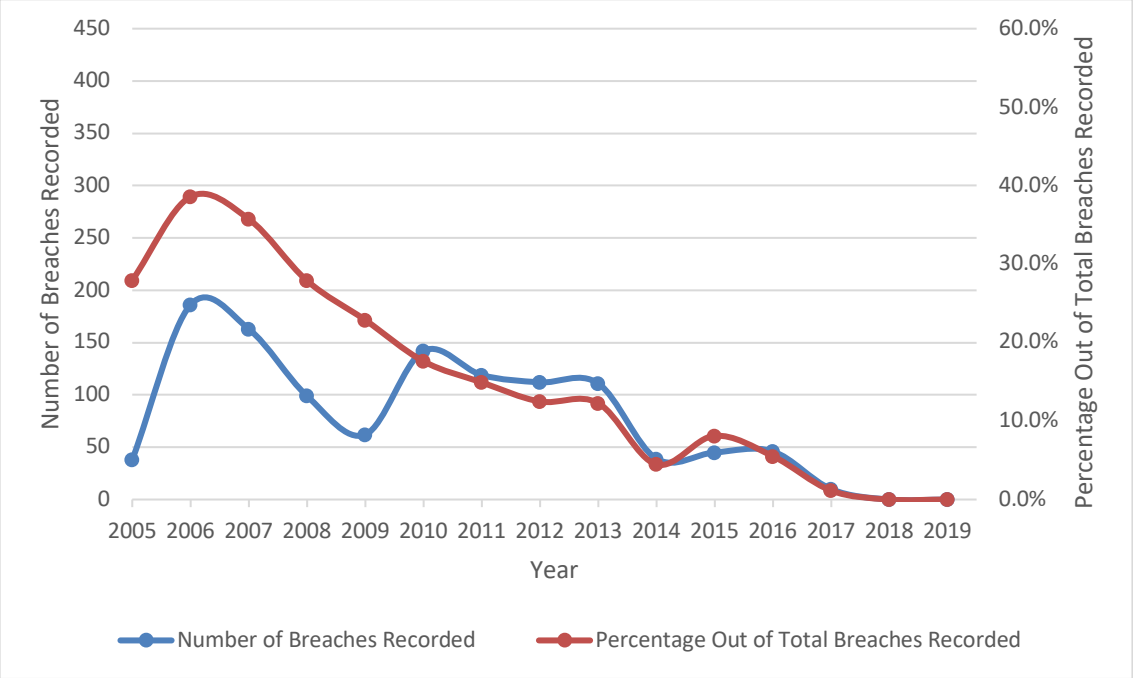

Figure 7. Portable Device Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

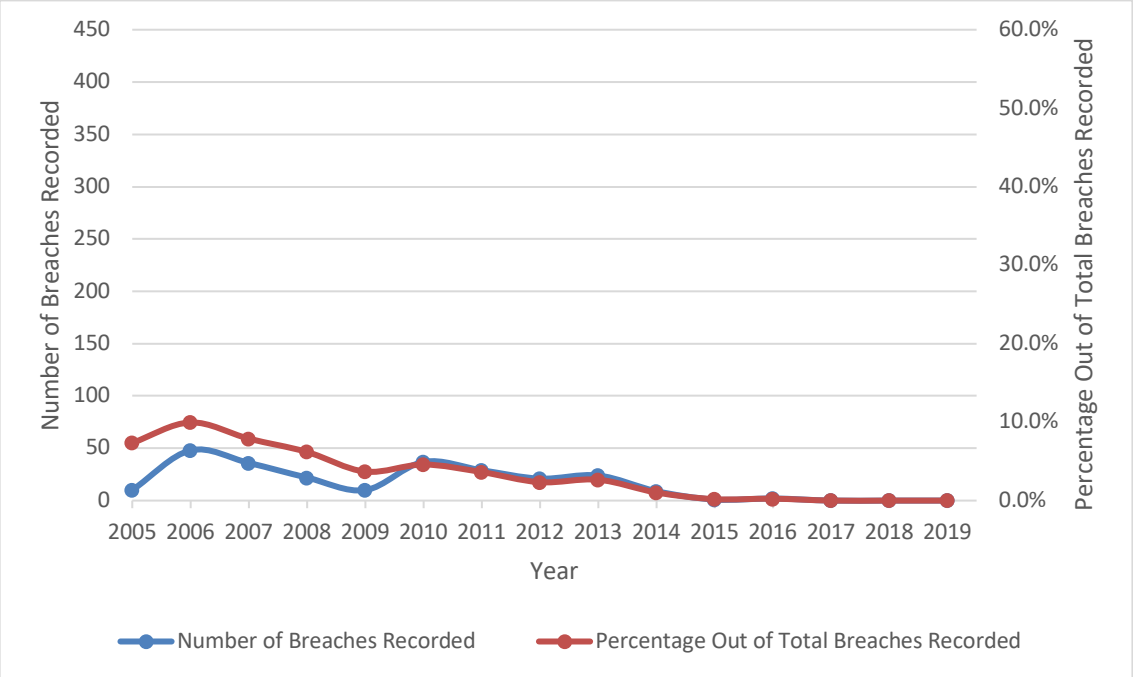

Figure 8. Stationary Device Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

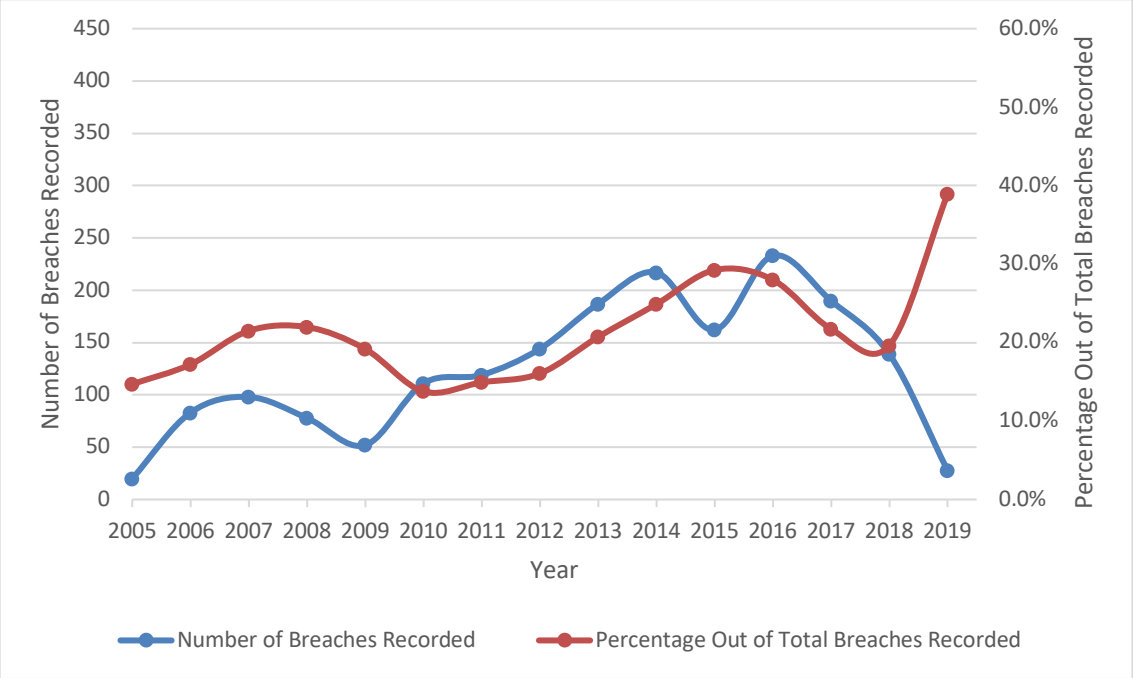

Figure 9. Unintended Disclosure Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

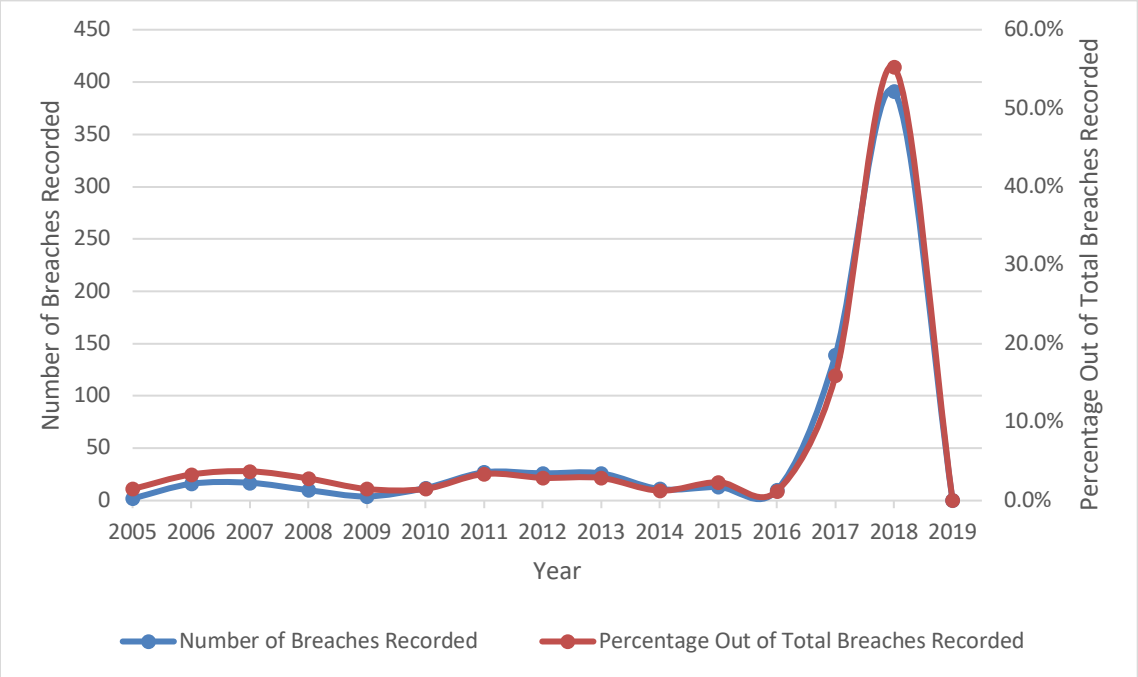

Figure 10. Unknown Related Incidents Reported Documented on the Privacy Rights Clearinghouse Over the Period of 2005-2019 (N=9,015)

Conclusion & Discussion

The main goal of this research study was to develop a deeper understanding of the Privacy Rights Clearinghouse data breach incidents database using quantitative time-series analyses for business intelligence. The visualizations can tell business professionals many different things depending on what the person is interested in. For example, the time-series visualizations can provide implications for practice and how it can help organizations in the different types within the dataset in their industry. According to Liu et al. (2012), there are five possible directions for future research when it comes to data breaches: control system security, power system security, accountability, integrity and confidentiality, and privacy. Nurse et al. (2011) presented another direction for future research in data breaches, being "the further examination of the support for and importance of specific usability guidelines" (p. 25). While there is still so much more to discover about data breach incidents, our results provide a basic understanding of how many recorded breaches there were over a 15-year time period. By doing so, we have addressed the main research question set for this study, which is: What are the overall big data trends emerging from 15 years of data breach incidents as documented by the Privacy Rights Clearinghouse? Furthermore, our results indicated that the number of documented data breach incidents within the Privacy Rights Clearinghouse investigated in this study appears to be dependent on the type of data breach incident of interest. Specifically, some are increasing pattern overtime, while others demonstrate a general declining pattern in some of the types of data breach incidents investigated. In different types of incidents where there appears to be an increase in data breaches, in following years it has reduced back to prior numbers. This may indicate that industry may have figured out security controls to deal with these data breach incidents, hence, the reduction pattern after a larger increase. This may be further evidence that most organizations that have been breached for these types of incidents appear to have implemented disaster recovery and business continuity planning in an effort to strengthen their cybersecurity posture, which in turn assisted in the mitigation of and reductions of such data breach incident types.

Study Limitations

Like every study, this study presents several limitations. The first limitation is due to the origin of the data. The data only comes from U.S. institutions. Thus, we are unable to generalize the information and provide any indications from our data to what is going on around the world, given that the data is assumed to be different. Additionally, data may be skewed due to reporting bias. Some industries that were reported in the dataset are under government regulation, such as healthcare and finance, who are required by law to report data breach incidents, while other industry types are either less regulated (e.g., business-retail, education, etc.) or not regulated at all (e.g., nonprofits). Reporting bias may also present itself because businesses are reluctant to report their data breaches, especially small to medium sized businesses. Many of them tend not to report at all, so the data may be more skewed towards larger organizations. Furthermore, the timing of this study may present a limitation. The dataset only covers 15 years of information, and we do not know what happened before 2005 (the first year of data). Finally, we must take into account the volume of devices and number of people who are on the Internet over time. A factor that was not accounted for within this particular study was the increased volume of devices and users on the Internet.

Future Research

Future research may present the visualizations provided in this paper to a sample of business executives and record their responses about whether or not the trends are important for their company. Additionally, future research may also look into mitigation strategies that are put into place and how they might impact industries in the next 10-15 years using similar big data visualizations and analytics. For example, implementing the Cybersecurity Maturity Model Certification (CMMC) (n.d.) may impact the long-term volume of cybersecurity incidents within certain industries, especially within the 16 critical infrastructure sectors (Cybersecurity & Infrastructure Security Agency, n.d.). Additional future research is recommended to conduct assessments related to business continuity and disaster recovery planning in the context of post-data breach incidents and looking at the differences between companies who have reported the data breach incidents and those who have not. Finally, another investigation may also look into the trends during the 2020-2021 COVID19 pandemic data.

Acknowledgement

We would like to thank Professor Meir Russ and the outstanding reviewers for their valuable comments and suggestions in helping us improve our manuscript throughout the review process. We thank the Privacy Rights Clearinghouse for enabling access to their database. Moreover, we thank the rest of the research lab team for their assistance with the ideas leading to this paper.

References

111th Congress. (2010). Cybersecurity act of 2010. https://www.congress.gov/bill/111th-congress/senate-bill/773

Bajaj, C. (1998). Data visualization techniques. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=FEC7925566383AA86FBFDF636B978F8B?doi=10.1.1.39.6660&rep=rep1&type=pdf

Cybersecurity Maturity Model Certification. (n.d.). *CMMC accreditation body cybersecurity maturity model certification*. Cybersecurity Maturity Model Certification Accreditation Body. https://cmmcab.org/

Cybersecurity & Infrastructure Security Agency. (n.d.). *Critical infrastructure sectors*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/critical-infrastructure-sectors

Emmert-Streib, F., Yli-Harja, O. P., & Dehmer, M. (2018). Data analytics applications for streaming data from social media: What to predict? *Frontiers in Big Data, 1*(2). https://doi.org/10.3389/fdata.2018.00002

Federal Bureau of Investigation (FBI). (2018). *Business e-mail compromise the 12 billion dollar scam.* Internet Crime Complaint Center (IC3). https://www.ic3.gov/media/2018/180712.aspx

Fishcer, E. A., Liu, E. C., Rollings, J. W., & Theohary, C. A. (2014). The 2013 cybersecurity executive order: Overview and considerations for congress. https://fas.org/sgp/crs/misc/R42984.pdf

Goode, J., & Levy, Y. (2017). Towards empirical exploration of employee's cybersecurity countermeasures awareness and skills: Differences in training delivery method and program type. *KM Conference 2017,* 18-30. http://www.iiakm.org/conference/proceedings/KM2017_RefereedProceedingsPapers.pdf

Hartung, T. (2018). Making big sense from big data. *Frontiers in Big Data, 1*(5). https://doi.org/10.3389/fdata.2018.00005

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems, 34*(50), 893-912. https://doi.org/10.17705/1CAIS.03450

JMP. (2021). *Time series analysis: Fit time series models and transfer functions*. https://www.jmp.com/support/help/en/16.0/index.shtml#page/jmp/time-series-analysis.shtml

Karunakaran, S., Thomas, K., Bursztein, E., & Comanescu, O. (2018). Data breaches: User comprehension, expectations, and concerns with handling exposed data. *Proceedings of the Fourteenth Symposium on Usable Privacy and Security.* https://elie.net/static/files/data-breaches-user-comprehension-expectations-and-concerns-with-handling-exposed-data/data-breaches-user-comprehension-expectations-and-concerns-with-handling-exposed-data-paper.pdf

Kaushik, S., Choudhury, A., Sheron, P. K., Dasgupta, N., Natarajan, S., Pickett, L. A., & Dutt, V. (2020). AI in healthcare: Time-series forecasting using statistical, neural, and ensemble architectures. *Frontiers in Big Data,* 3, Article 4. https://doi.org/10.3389/fdata.2020.00004

Keim, D., Qu, H., & Ma, K. (2013). Big-data visualization. *IEEE Computer Graphics and Applications, 33*(4), 20-21. https://doi.org/10.1109/MCG.2013.54

Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials*, *14*(4), 981-997. https://ieeexplore.ieee.org/abstract/document/6129371

Moore, J. (2017). Data visualization in support of executive decision making. *Interdisciplinary Journal of Information, Knowledge, and Management*, *12*, 125-138. http://www.ijikm.org/Volume12/IJIKMv12p125-138Moore2889.pdf

National Institute of Standards and Technology. (n.d.). *Definitions, applications and techniques*. https://www.itl.nist.gov/div898/handbook/pmc/section4/pmc41.htm

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. *Proceedings of the 2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, 21-26. https://ieeexplore.ieee.org/abstract/document/6058566

Peretti, K. (2009). Data breaches: What the underground world of carding reveals. *Santa Clara High Technology Law Journal, 25*(2), 375-413. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1472&context=chtlj

Person, R. (2014). Developing executive and operational dashboards. *Balanced Scorecards & Operational Dashboards with Microsoft® Excel®, Second Edition,* 101-108. https://doi.org/10.1002/9781118984000.ch9

Pitts J., Gopal S., Ma, Y., Koch, M., Boumans, R. M., & Kaufman, L. (2020). Leveraging big data and analytics to improve food, energy, and water system sustainability. *Frontiers in Big Data, 3*(13). https://doi.org/10.3389/fdata.2020.00013

Privacy Rights Clearinghouse. (2018). *Data breach database*. https://www.privacyrights.org/data-breaches

Privacy Rights Clearinghouse. (2019). *What's a data breach?*. https://privacyrights.org/resources/whats-data-breach

Resnick, M. L. (2003). Buildings the executive dashboard. *SAGE Journals, 47*(13), 1639-1643. https://doi.org/10.1177/154193120304701311

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce, 23*(2), 1-11. http://www.icommercecentral.com/open-access/impact-of-cyberattacks-on-financial-institutions.pdf

Telea, A. C. (2007). *Data visualization principles and practice*. CRC Press.

U.S. Department of Homeland Security. (2018). Congress passes legislation standing up cybersecurity agency in DHS. https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs

Authors Biographies

Emily Africk graduated from the University of Michigan with a Bachelor of Science in Statistics and a minor in Entrepreneurship. She works as a Technologist/Consultant, leveraging her skills and expertise in statistics and data analysis, statistical computing, probability, and regression analysis in support of risk assessments. Emily's current research interests include cybersecurity, data visualization, data analytics, risk analysis, as well as supply chain risk management.

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Computing and Engineering at Nova Southeastern University, the Director of the Center for Information Protection, Education, and Research (CIPhER) (http://infosec.nova.edu/), and chair of the Cybersecurity curriculum committee at the college along with serving as the director of the M.S. and Ph.D. programs in Cybersecurity. He heads the Levy CyLab (http://CyLab.nova.edu/), which conducts innovative research from the 'human factor' in cybersecurity, including social engineering. Levy authored numerous peer reviewed journal, conference proceedings, book

chapters, and other publications. His scholarly research has been cited over 6,000 times. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and FDLE South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics and actively serves as a board member on the South Florida FBI/InfraGard. He consults federal agencies, state and local government groups on cybersecurity topics. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy via: https://sites.nova.edu/levyy/