Issues in Information Systems
Volume 20, Issue 2, pp. 162-171, 2019

ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES

Ping Wang, Robert Morris University, wangp@rmu.edu
Hubert D'Cruze, University of Maryland, hubert.dcruze@yahoo.com
David Wood, Robert Morris University, wood@rmu.edu

ABSTRACT

A data breach is a consequential cybersecurity attack or incident that may bring substantial impacts and losses to organizational and individual victims. Unauthorized disclosure of sensitive information as a result of data breaches has been on the rise. The number of records breached in commercial business organizations has been the highest among all types of victims, which bring various harms and impacts including economic costs and monetary losses to businesses and consumers. It has been a research challenge for the cybersecurity field to establish an adequate and reliable method for measuring the true costs of cybercrimes and data breaches. A comprehensive model for identifying the factors and extent of economic costs of data breaches is essential to accurate measurement of data breach costs and valuable to cybersecurity decisions and investments for data protection. This paper explores the direct and indirect cost factors of data breach and proposes a comprehensive taxonomy of economic cost and impact factors for analyzing business data breaches. This paper uses the case study of the recent data breach at Target to illustrate direct and indirect cost factors in the proposed model.

Keywords: Data breach, taxonomy, cost factors, direct cost, indirect cost, business, consumer

INTRODUCTION

Data breaches have become common instances of cybersecurity attacks or incidents that victimize various organizations and individuals. A data breach is an "unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information" (NICCS, 2019, section D, para. 3). Recent research shows that data breaches continue to grow year after year in cost and in the number of lost or stolen consumer records (Ponemon Institute, 2018). However, there is no consensus on an adequate and reliable method for measuring the true costs of cybersecurity incidents such as data breaches (Riek & Böhme, 2018; Romanosky, 2016). An essential part of the challenge is that there is no consensus on the cost factors for measurement as cyber attacks and data breaches may bring various types of harms and impacts, including physical harm, monetary and economic harm, psychological harm, and social harm as well as indirect and hidden costs (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018; Anderson et al., 2012; Sidaway, 2016). Therefore, a comprehensive model for identifying the factors and extent of economic costs of data breaches is essential to adequate measurement of data breach costs and valuable to sound cybersecurity decisions and investments for data protection.

This research focuses on the costs of data breaches at commercial business organizations, which involve the majority of data records breached. According to the latest data retrieved on April 22, 2019 from Privacy Rights Clearinghouse (PRC), a nonprofit consumer education and advocacy organization, there have been a total of 8,804 data breach cases known to the public since 2005 with a total of 11,575,804,706 records breached. Among all the known data breach cases so far, 2,429 cases occurred at commercial business organizations, including online retail, financial and insurance services and other businesses but the number of records breached at business organizations have reached a total of 11,016,918,790 of all records breached (PRC, 2018). The commercial data breach cases are far more substantial than in other sectors as the number of records breached make up an overwhelming 95.17% of all records breached, whereas the commercial data breach cases only account for 27.59% of all data breach cases. The average direct financial cost of a typical data breach is $3.86 million according to the 2018 study report by IBM Security and Ponemon Institute (Ponemon Institute, 2018). However, the methodology for understanding and calculating typical

data breach incidents that do not exceed 100,000 records does not apply to mega data breaches that involve one million records or more (Ponemon Institute, 2018). In addition, there may also be various cost factors including hidden and indirect costs such as damage to corporate reputation and loss of customer confidence as a result of the data breach (Agrafiotis et al., 2018; Anderson et al., 2012). For example, the recent Equifax data breach not only costs hundreds of millions of dollars for the company but also may create problems that could impact hundreds of millions of consumers in the US for decades (U.S. News, 2017). Therefore, identifying various cost factors is essential to adequate recognition and measurement of the true costs of business data breaches.

The indirect and hidden cost factors are usually not easy to recognize and difficult to measure. However, these factors are significant to business survival and competitiveness. Hidden costs such as lost business, negative impact on business reputation and employee time spent on recovery increase business expenses and the level of difficulty for business management, and lost business alone accounted for one-third of the cost of mega data breaches (IBM Security, 2018). This study will explore various cost factors, including direct, indirect and hidden factors that contribute to the costs of data breaches. A comprehensive view of the data breach cost factors will not only improve the measurement methodology for data breach costs but also provide more accurate data for decision making in business management and cybersecurity planning. Since the costs of mega data breaches are especially challenging to measure, this study will uncover cost factors that apply to mega breaches as well and will conduct a comprehensive case study of the recent mega data breach at the retail giant Target.

The goal of this research is not to reach exact cost numbers of data breaches but to uncover various types of economic cost and impact factors for business data breaches and propose a comprehensive taxonomy to map out the cost factors that apply to various sizes of business data breaches especially the hard-to-measure mega data breaches. To illustrate the proposed taxonomy of cost factors, this paper uses the case study method to identify, examine and analyze the various cost factors for the mega data breach case that occurred at Target in 2013. The following sections of this paper will review relevant background theories and methods, formulate and define the proposed taxonomy, describe the data breach case used for the case study, and discuss the findings based on the case study.

BACKGROUND

Cybercrimes are a frequent cause for data breaches that result in unauthorized disclosures or theft of sensitive personal and financial information. Research efforts on measuring the costs of cybercrimes may shed light on the costs of data breaches. The research by Anderson et al. (2012) was believed to be the first systematic study on the costs of cybercrime. The key cost categories identified by Anderson et al. (2012) in their framework for analyzing the costs of cybercrime include direct losses, indirect losses, defense costs, and cost to society. Anderson et al. (2012) define these cost categories as follows: (1) Direct loss is the monetary equivalent of losses, damage or other suffering felt by the individual victim as a result of the cybercrime, which includes loss of monetary value and associated inconveniences, loss of time and effort spent on data recovery, emotional distress, and lost attention and bandwidth; (2) Indirect loss is the monetary equivalent of losses and opportunity costs to the society or institutions in general, which includes loss of consumer trust in online businesses leading to reduced revenues and higher business costs, missed business opportunities, and cost of efforts to respond and recover from cyber attacks such as malware infections from botnets; (3) Defense cost is the monetary equivalent of prevention measures, including the costs of developing, deploying and maintaining security products and services, training and awareness measures, fraud detection and recovery as well as costs of law enforcement, inconvenience and missed opportunities; and (4) Cost to society, which is the total of the direct losses, indirect losses, and defense costs. The study by Anderson et al. (2012) found that the direct costs of cybercrimes are relatively low but the indirect costs and defense costs for cybercrimes are much higher compared to the costs of traditional crimes. The study also acknowledged that estimates of the costs of cybercrimes may vary globally due to different measures used in different countries.

Krausz and Walker (2013) classify the costs of a data breach into two major categories: (1) Direct and indirect financial costs; and (2) Reputational cost, third-party risks and associated costs. According to Krausz and Walker (2013), direct financial cost is any cost directly attributed to the breach, including all work time, overtime, external cost, and equipment and legal costs, whereas indirect financial cost is not directly related to the breach but incurs as a result of the breach, such as costs of lost productivity and penalties from clients in the case of a denial-of-service attack.

Reputational cost is all damages to business in a data breach as a result of a loss of trust and credibility with the customers and general public, and third-party risks mainly refer to the security risks and associated costs in hosting applications, services and infrastructure components with third-party cloud service providers (Krausz &Walker, 2013). The study acknowledges that direct and indirect financial costs of data breaches can be estimated or calculated while reputational costs and third-party risks and costs are hard to measure and "can only be guesstimated, at best" (Krausz &Walker, 2013, p.29). The study by Cavusoglu, Mishra, and Raghunathan (2004) indicates a negative cost impact of the public announcement of an Internet security breach on the stock market value of the announcing firm: "The breached firms in the sample lost, on average, 2.1 percent of their market value within two days of the announcement - an average loss in market capitalization of $1.65 billion per breach" (p.69). This negative cost impact on the stock value is seen as an example of indirect costs as a result of anticipated loss of the customer confidence and trust, which may exceed the direct costs as the security breach unfolds (Laube & Böhme, 2016).

Several other studies have identified similar or diverse cost factors for cybercrimes and data breaches. Negrea (2015) identified several hard cost items in response to data breaches at colleges and universities regardless of the number of records exposed: hiring a forensics team, contracting for legal services, providing notifications and credit protection services for potential victims, and hardening computer and network systems. Sidaway (2016) highlighted a list of remediation costs to businesses and their average percentages in the case of a security breach: legal costs (19%), compensation costs to customers (18%), third party remediation resources (15%), fines/compliance costs (15%), PR/corporate communication costs (13%), compensation costs to suppliers (10%), and compensation costs to employees (9%). The study by Romanosky (2016) finds that the average cost of a typical cyber incident is less than $200,000 or only 0.4% of a company's annual revenue, but the concept of a cyber incident includes various types of events with no specific cost analysis for data breaches. The cost estimate model by Riek and Böhme (2018) is limited to the factors of monetary losses, time spent and protection expenses in handling cybercrimes, and the study focus is on mathematical formulas for consumers' losses with no inclusion of business spending.

The latest global study report on the cost of a data breach sponsored by IBM Security and independently conducted by Ponemon Institute provides specific average cost estimates: (1) The average total cost of a data breach is $3.86 million, an increase of 6.4 percent over 2017; (2) The average cost per lost or stolen record is $148, an increase of 4.8 percent over 2017; (3) The average size of data breaches has increased by 2.2 percent from 2017 (Ponemon Institute, 2018). The accounting methodology behind this study is activity-based costing (ABC) that identifies and assigns direct, indirect and opportunity costs to a range of activities following a data breach that include detection and internal reporting of breach, notification to data subjects and regulatory activities, post data breach response and reparation with data subjects and regulators, and lost business activities such as business disruption and system downtime. Hidden costs from lost business significantly increase business expenses and account for one-third of the cost of mega breaches (IBM Security, 2018). However, a major limitation acknowledged in the study is that it only targets typical data breach cases not exceeding 100,000 records and the method does not apply to mega data breaches involving a million records or more. The study does provide an alternative Monte Carlo simulation method for mega breaches, which estimates possible outcomes based on repeated simulation trials, but the mega breach sample size for the study is too small and the simulation approach needs further testing and validation.

Using the case studies of the recent data breaches at Sony, JPMorgan and Ashley Madison, the study by Agrafiotis et al. (2018) provides a comprehensive taxonomy of harms and impacts from cyber attacks to help organizations in managing risks and security controls. The main types of cyber harms are: (1) Physical or Digital harm, which is a negative physical or digital effect on a person or asset such as damaged systems or data theft; (2) Economic harm that refers to negative financial or economic consequences; (3) Psychological harm that affects individual mental well-being and psyche; (4) Reputational harm that relates to the public opinion about an organization; and (5) Social and Societal harm that may impact a social group or the general society (Agrafiotis et al., 2018). The major advantage of this study is its identification and mapping of key types and sub-types of harms and negative impacts from cyber attacks, including some sub-types of economic harms. However, the scope of the taxonomy is too broad and does not focus on economic impacts with in-depth analysis of the costs of data breaches.

PROPOSED TAXONOMY

This section proposes a comprehensive taxonomy and definitions of direct and indirect cost factors of data breaches for business organizations and consumer individuals. Direct cost factors are items of financial loss, damages, or monetary equivalent that arise directly as a result of a data breach. Indirect cost factors are items of financial loss, damages, or monetary equivalent that occur as a result of one or more additional factors, such as lost customer loyalty, caused by the data breach. Indirect costs would not have happened without the original data breach (Krausz &Walker, 2013). Indirect costs are often latent, hidden, and difficult to recognize and measure. For example, research shows that the probability of banking customers ending business relationship with their banks increases significantly in the six months following a fraudulent transaction or security breach (Somanchi & Telang, 2017). The banks will suffer indirect business and financial losses from the security breach due to decreased customer loyalty. This example also shows that it is important to map data breach cost factors for both businesses and consumers as they may be related to each other. Table 1 below presents the proposed taxonomy of this study to map the direct and indirect cost factors of data breaches for business and consumer victims.

Table 1. Proposed Taxonomy of Data Breach Cost Factors

	Direct Costs	**Indirect Costs**
Businesses	Financial theft	Profit decline
	Sales disruption	Productivity decline
	Operation disruption	Loss of customers
	Stock price drop	Loss of market share
	Legal cost	Reduced growth
	Investigation cost	Loss of investments
	Work time cost	System downtime
	Regulatory fines	Loss of competitiveness
	PR cost	Loss of talent
	Credit monitoring and reimbursement costs	Loss of consumer confidence
	Extortion payments	Reduced credit rating
	Settlement cost	Insurance cost
		Reputational cost
Consumers	Financial theft	Loss of time
	Legal cost	Loss of wages
	Stock price drop	Identity theft
	Extortion payments	Loss of convenience
	Credit monitoring cost	Credit loss
		Loss of employment opportunities
		Price increase
		Emotional stress

Direct Costs for Businesses

The direct cost factors for businesses as a result of a data breach are defined below. Some of the cost factors are similar to the cyber-harm sub-types in the taxonomy of the economic harm type by Agrafiotis et al. (2018) but are more accurately defined here in terms of their relationship to the data breach:

- Financial theft: Financial or monetary assets have been stolen in the data breach (Agrafiotis et al., 2018).
- Sales disruption: The normal sales revenue has been disrupted and reduced as a result of the breach.
- Operation disruption: The normal business operations and productivity have been disrupted by the breach.
- Stock price drop: The stock price falls soon after the breach (Cavusoglu, Mishra, & Raghunathan, 2004).
- Legal cost: Fees for lawyers specializing in cybersecurity to advise on applicable breach laws and handle litigations as a result of the breach (Negrea, 2015).
- Investigation cost: The cost for hiring a digital forensics team to determine how the breach happened and how to recover from the breach and prevent future breaches (Negrea, 2015).
- Work time cost: Costs of work time and overtime for staff to investigate a breach (Krausz &Walker, 2013).

- Regulatory fines: Fines and penalties charged by regulatory bodies for the business's liability (Agrafiotis et al., 2018). For example, the minimum fine for neglect in a HIPAA (Health Insurance Portability and Accountability Act) violation is $1.5 million (Chaput, 2015).
- PR cost: The cost of engaging in public relations and communication activities in response to a data breach (Agrafiotis et al., 2018; Negrea, 2015).
- Credit monitoring and reimbursement costs: The business has to spend money notifying potential victims and pay for credit monitoring and cover losses for those affected by the breach. In addition, reimbursing credit card companies for fraudulent transactions involving credit card data stolen from the breach can be a "staggering expense" (Iram, 2017).
- Extortion payments: The cost for the organization to pay to restore data and operations such as in a ransomware related attack (Agrafiotis et al., 2018).
- Settlement cost: The payments to settle lawsuits from parties affected by the data breach.

Indirect Costs for Businesses

The indirect cost factors for businesses as a result of a data breach are defined and explained as follows. These indirect factors are intermediary factors caused by the breach and cause subsequent financial loss to the organization:

- Profit decline: The business profit decreases after the breach due to intermediary factors, such as lost business opportunities and market shares as a result of the data breach. Consumers prefer to migrate to non-breached channels for purchases after an announced data breach (Janakiraman, Lim, & Rishika, 2018).
- Productivity decline: Productivity decreases after the breach due to intermediary factors caused by the breach.
- Loss of customers: Customers turn to competitors as a result of the breach (Chaput, 2015; Somanchi & Telang, 2017). Loss of customers in turn will cost the business in sales and revenue.
- Loss of market share: Decreased share in the market due to the breach will incur costs to the business.
- Reduced growth: The business growth will slow down after the breach.
- Loss of investments: The organization may lose investments from external parties (Agrafiotis et al., 2018).
- System downtime: Unavailable services caused by the breach will incur financial cost to the business.
- Loss of competitiveness: The business becomes less competitive due to intermediary factors such as loss of talent and reputation caused by the breach, which incurs subsequent financial costs to the organization.
- Loss of talent: Talented employees may be concerned about the business image and prospects after the breach and leave the organization, which may cause subsequent loss of productivity and competitiveness.
- Loss of consumer confidence: Consumer trust, confidence and loyalty may drop due to the breach.
- Reduced credit rating: The organization's credit rating is reduced due to the breach, which may cause loss of competitiveness and loss of profit.
- Insurance cost: Cost of insurance protection is a factor in the cost of a data breach (Ponemon Institute, 2018). Data breach incidents may drive up future insurance costs for the business.
- Reputational cost: Data breaches pose serious challenges to corporate reputation, which is an important asset related to corporate financial health (Gwebu, Wang, & Wang, 2018). The organization loses consumer trust and public confidence due to the breach, which may translate into financial or monetary loss (Krishan, 2018).

Direct Costs for Consumers

The direct cost factors for consumer victims of data breaches are defined and explained as follows:

- Financial theft: Consumers' loss of cash or financial assets such as unreimbursed theft of monetary assets from checking or savings accounts as a direct result of the data breach (Ablon, Heaton, Lavery & Romanosky, 2016).
- Legal cost: Consumers may have to spend money on their own to obtain legal help to recover their lost sensitive information or financial assets.
- Stock price drop: Consumers who are stock holders may suffer direct financial losses when the stock price falls soon after the breach.
- Extortion payments: Possible payments by individual consumers to attackers in a data breach to unlock critical systems or data hijacked or locked in a ransom related data breach.
- Credit monitoring cost: Consumers may have to spend money purchasing credit monitoring for protection if there is no or inadequate offer of credit monitoring services from the breached company.

Indirect Costs for Consumers

The indirect cost factors for consumers are defined and explained as follows:

- Loss of time: Consumers may have to spend time on repairing damaged credit accounts (Ablon et al., 2016). Loss of time is common and substantial cost factor for individuals affected by the breach (Riek & Böhme, 2018).
- Loss of wages: Consumers affected by a data breach may lose their wages due to work time spent on dealing with the ramifications of the breach.
- Identity theft: Theft of PII (personal identifiable information) from a data breach may cause damage to consumer credit or loss of financial assets.
- Loss of convenience: A data breach may cause serious inconveniences to individual consumers such as switching services and consumer accounts. The median estimated dollar value for inconveniences from a data breach from a survey study is $500 per person (Ablon et al., 2016).
- Credit loss: Consumers may lose credit ratings or scores due to identity theft and fraudulent transactions facilitated by stolen sensitive personal data from a data breach.
- Loss of employment: Consumers may lose employment opportunities and subsequent loss of financial income due to credit damage and identity theft from a data breach.
- Price increase: Consumers have to pay extra for services and products when breached vendors hike their prices to stay profitable.
- Emotional stress: The harmful effects from cyber attacks and data breaches include psychological harms to affected individuals, such as confusion, frustration, anxiety, depression, loss of self-confidence, and negative changes in perception (Agrafiotis et al., 2018). Other research also found that data breaches may trigger an enhanced perception of vulnerability and harm among consumers affected by a data breach leading to negative outcomes (Janakiraman et al., 2018).

CASE STUDY: THE TARGET DATA BREACH

The case study method provides realistic illustrations of the proposed taxonomy of economic cost and impact factors based on a real case of data breach. The case for this study is the data breach of late 2013 at the Target Corporation, one of the largest retail chains in the United States. The Target breach case is selected for this study because the breach involves multiple victims and parties affected and a variety of direct and indirect cost factors that fit the proposed taxonomy for this study.

Here is a brief synopsis of the Target data breach based on a Congressional Research Service Report by Weiss and Miller (2015). In November and December of 2013, cybercriminals breached the data security of Target and stole the personal and financial data for millions of customers. Target officially confirmed in a public announcement on December 19, 2013 that about 40 million credit and debit card account numbers were stolen, and on January 10, 2014 Target announced that PII (personal identifiable information) including the names, addresses, phone numbers and email addresses of up to 70 million customers was also stolen during the data breach (Weiss & Miller, 2015).

The specific timeline of the Target breach is as follows:

- September 2013: Hackers from unknown location conducted an email phishing attack against Fazio Mechanical Services, which was a third-party heating and ventilation provider for Target (Srinivasan, Paine, & Goyal, 2019).
- November 15, 2013: Hackers gained access to Target's network by using stolen credentials from Fazio Mechanical Services (Srinivasan et al., 2019).
- By November 30, 2013: Most of Target's POS (Point-of-Sale) system was compromised by hackers who installed the "Citadel" Trojan malware to collect payment card data from POS systems (Shu, Tian, Ciambone, & Yao, 2017; Srinivasan et al., 2019).
- December 12, 2013: The Department of Justice (DOJ) notified Target of suspicious activity involving payment cards that had been used at Target (Weiss & Miller, 2015).
- December 14, 2013: Target hired outside experts to conduct a forensic investigation (Weiss & Miller, 2015).
- December 16 and 17, 2013: Target notified payment processors and card networks that a breach had occurred (Weiss & Miller, 2015).

- December 19, 2013: Target made a public announcement of the breach and confirmed the theft of 40 million payment card information (Weiss & Miller, 2015).
- January 10, 2014: Target announced the PII theft of about 70 million customers (Weiss & Miller, 2015).

The direct cost factors for the Target organization from the data breach include sales disruption, operation disruption, stock price drop, legal cost, investigation cost, work time cost, regulatory fines, PR cost, credit monitoring and reimbursement costs, and settlement cost. Target reported a total of $248 million in expenses related to the breach by November 1, 2014, including the costs of the breach investigation, credit monitoring, increased call center staffing, and accrual payments for fraud losses and operating costs from payment card networks and allowances for defending and settling over 100 lawsuits against the Target as a result of the breach (Weiss & Miller, 2015). Target's total sales decreased by 6.6% for the fourth quarter of 2013 compared with the previous year, and Target stock price went down 8.8% six weeks after the breach announcement (Srinivasan et al., 2019). Target could also face a fine between $400 million and $1.1 billion for non-compliance with the Payment Card Industry Data Security Standard (PCI-DSS) which requires two-step authentication for remote access to payment networks (Dube, 2016; Srinivasan et al., 2019; Weiss & Miller, 2015). Target had to pay large sums of settlement costs in response to lawsuits from customers and banks. Target agreed to a $10 million settlement to compensate for consumer losses in November 2015 and settled the complaint from Visa for $67 million in August 2015 and approximately $40 million with MasterCard and other banks in December 2015 (Srinivasan et al., 2019). In addition, crisis communication is an important part of corporate response to a data breach incident (Wang & Johnson, 2018; Wang & Park, 2017). By January 2016, Target had spent $291 million in breach-related costs including legal fees, crisis communications and forensics costs, and less than one-third of that amount was expected to be covered by cyber insurance (Newman, 2016).

In addition to the direct costs, there were indirect cost items to the Target organization caused by intermediary impacts and factors as a result of the breach. Target announced a 46% drop in profits and a 5.3% decrease in revenue for the fourth quarter of 2013, which was a result of fearful shoppers according to Target management (Dube, 2016). Target also suffered severe damage to its business brand and reputation, which could cause losses of customers, market share, profits, and competitiveness. The Target brand scored negatively in all surveys of consumer perceptions for the first time in late December 2013, and the exodus of its customers contributed to its poor quarterly and full-year business performance that dropped way below the targets expected by Wall Street (Dube, 2016). Target's brand plunged by 35 points on the BrandIndex's scale the day after the announcement of the breach (Picchi, 2013). Post-Target research of consumer attitude on data security shows that an overwhelming 85% of consumers expect a company processing personal and financial information online to keep the data safe from criminals, which is also the number one issue for consumers to reconsider using the company if it fails to keep the data safe (Deloitte, 2015). Consumer perception of Target reached the lowest since June 2007, and many of them vowed to avoid shopping at Target and others have cancelled their REDcards (Srinivasan et al., 2019). There was also significant damage to consumer confidence after the breach, and in terms of market share the percentage of customers shopping at Target was down to 33% in January 2014 from 43% in the same month of the previous year (Plachkinova & Maurer, 2018). Target did receive some insurance coverage of less than one-third of the total direct costs from the breach. However, the cyber insurance premium skyrocketed and was expected to go up further following the high profile data breaches, including the Target breach even though Target never disclosed the details of the premium increase (Finkle, 2015). These indirect cost factors will drive up the total economic costs and impacts from the data breach.

Consumer victims are an important part of the data breach incident as well, and the economic costs and impacts to consumers are often under-reported. Consumer victims in the Target case suffered both direct losses of financial or monetary assets and indirect losses that may be translated to financial costs or in some respects perceived more valuable than monetary assets. Some customers suffered direct financial loss as a result of the breach. For example, one customer found two unauthorized charges to her account while another customer "found her bank account depleted from $3,643.53 to $5.86, forcing her to borrow for food and for her son's tuition" (Srinivasan et al., 2019, p.6). The direct monetary loss from the breach in the latter part of this case also created subsequent inconveniences and additional financial difficulties for the customer victim. In addition to the monetary loss, consumer victims also experienced additional direct financial burdens of higher interest rates due to missed payments, cost of replacing government ID cards, and cost of hiring legal help (Srinivasan et al., 2019).

Consumer victims faced various indirect costs and losses from the Target breach as well. One customer cited from a lawsuit was a mother of five children, had two fraudulent charges on her bank card due to the breach, was locked out of her bank account, missed a rent payment and car loan payment and "had difficulty putting food on the table during

the holidays" (Srinivasan et al., 2019, p.8). Another customer had to delay his purchase of a much needed newer car because his credit score dropped about 20 to 50 points due to 35 fraudulent inquiries on this credit records (Srinivasan et al., 2019). These examples indicate the costs of identity theft, losses of credit and conveniences as well as emotional stress consumer victims had to experience in the aftermath of the breach. Obviously, the affected consumers had to spend substantial amount of time in dealing with various organizations and agencies to repair their damaged credit and restore their accounts. A study on the impacts of data breaches, including the Target breach, on financial institutions and customers shows that customers are indirectly and adversely impacted not only by not being able to use their payment cards during the lockout but also by the slow process of reactivating and re-registering cards with various merchants that could take several months (First Citizens' Federal Credit Union, 2015).

CONCLUSIONS

Cyber attacks and data breaches have become a frequent issue in the age of information technology. Data breaches involving commercial business organizations make up an overwhelming majority of data records breached. Data breaches cause various impacts including economic costs to both business organizations and individual consumers. The existing research literature has been primarily concerned with the costs and impacts to businesses with inadequate study on the economic impacts on consumer victims. In addition, there has been no reliable measures of the costs of data breaches. The goal of this study is to identify the cost factors essential to reliable measures of true costs of data breaches. This study proposes a comprehensive taxonomy of direct and indirect cost factors to both businesses and consumers in data breaches. The direct cost factors are financial costs or monetary losses that incur to organizations or individuals as a direct result of the data breach. The indirect cost factors are items of financial costs or monetary equivalents from one or more intermediary factors caused by the data breach. Identifying and defining comprehensive cost factors will contribute to more reliable measures of the economic costs and impacts of data breaches.

The case study of the Target data breach of late 2013 used in this research reveals that the Target Corporation suffered substantial direct financial losses from sales disruption, operation disruption, stock price fall, legal cost, investigation cost, work time cost, regulatory fines, PR cost, credit monitoring and reimbursement costs, and costs of settlement with customers and banks. In addition, Target suffered indirect costs and loss of profit from damage to corporate brand and reputation, loss of consumer trust and confidence, customer turnover, loss of market share, and probable increase in cyber insurance premium as a result of the massive data breach. The case study also reveals that consumers suffered direct financial losses of monetary thefts, unauthorized charges, higher interest rates, financial difficulties, and costs of replacing IDs and hiring legal help. In addition, consumers experienced a variety of indirect costs from the intermediary factors of financial difficulties, loss of identity, damaged credit, account lockout and recovery, loss of time, and inconveniences and emotional stress that were caused by the data breach.

This study is a preliminary effort toward reliable and accurate measures of the costs of data breaches and limited to the proposed taxonomy of economic cost factors. Future studies may include mapping of relationships between certain direct and indirect cost factors and developing an instrument for testing. Future case studies may also include more data breach cases and cases of varying sizes. With multiple studies of diverse and representative breach cases, it will be possible to yield more specific data on the probabilities, ranges and other statistical distributions of the cost factors identified in this research.

REFERENCES

Ablon, L., Heaton, P., Lavery, D.C., & Romanosky, S. (2016). Consumer attitudes toward data breach notifications and loss of personal information. Santa Monica, CA: RAND Corporation, 2016. Retrieved from https://www.rand.org/pubs/research_reports/RR1187.html

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1-15. https://doi.org/10.1093/cybsec/tyy006

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., & Savage, S. (2012). Measuring the cost of cybercrime. In *Proceedings of Workshop on Economics of Information Security (WEIS 2012)*, Berlin, Germany, June 2012, 1-31.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9(1),* 69-104.

Chaput, M.A. (2015, May). The colossal cost of a data breach. *CFO,* 22-23.

Deloitte. (2015). Consumer data under attack: The growing threat of cyber crime. *The Deloitte Consumer Review,* 1-28. Retrieved from https://www2.deloitte.com/content/campaigns/uk/consumer-review/consumer/consumer.html

Dube, L. (2016). Autopsy of a data breach: The Target case. *International Journal of Case Studies in Management, 14*(1), 1-8.

Finkle, J. (2015, October 12). Cyber insurance premiums rocket after high-profile attacks. Retrieved from https://www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012

First Citizens' Federal Credit Union. (2015). Data breaches: How it impacts the customer & the financial institution. Retrieved from https://www.firstcitizens.org/assets/files/IQqKfUZ0/r/DATA+BREACHES+-+RELATED+EXPENSES+FOR+FINANCIAL+INSTITUIONS+%283%29.pdf

Gwebu, K.L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems, 35*(2), 683–714.

IBM Security. (2018). IBM Study: Hidden costs of data breaches increase expenses for businesses. Retrieved from https://www.prnewswire.com/news-releases/ibm-study-hidden-costs-of-data-breaches-increase-expenses-for-businesses-300679124.html

Iram, R. (2017, September). How to curb the costs of a data breach. *CFO,* 14-15.

Janakiraman, R., Lim, J.H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing, 82*(March 2018), 85-105.

Krausz, M., & Walker, J. (2013). *The true cost of information security breaches and cyber crime.* Ely, UK: IT Governance Publishing.

Krishan, R. (2018, May). Corporate solutions to minimize expenses from cyber security attacks in the United States. *Journal of Internet Law,* May 2018, 16-19.

Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity, 2*(1), 29 – 41.

Negrea, S. (2015, June). Hard costs of a data breach. *Campus Finance.* 61-63.

Newman, C.A. (2016, April 7). Target's cyber insurance: A $100 million policy vs. $300 million (so far) in costs. Retrieved from https://www.pbwt.com/data-security-law-blog/targets-cyber-insurance-a-100-million-policy-vs-300-million-so-far-in-costs

NICCS (National Initiative for Cybersecurity Careers and Studies). (2019). Explore Terms: A Glossary of Common Cybersecurity Terminology. Retrieved from https://niccs.us-cert.gov/glossary

Picchi, A. (2013, December 27). After security breach, Target's brand takes a hit. Retrieved from https://www.cbsnews.com/news/after-security-breach-targets-brand-takes-a-body-blow/

Plachkinova, M. & Maurer, C. (2018). Teaching case: Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-20.

Ponemon Institute. (July 2018). 2018 Cost of data breach study: Global overview. Retrieved from https://www.ibm.com/security/data-breach

PRC (Privacy Rights Clearinghouse). (2019). Data breaches. Retrieved from https://www.privacyrights.org/data-breaches

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 4(1), 1-16. https://doi.org/10.1093/cybsec/tyy004

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Shu, X., Tian, K., Ciambone, A., & Yao, D. (2017). Breaking the Target: An analysis of Target data breach and lessons learned. Retrieved from https://arxiv.org/abs/1701.04940

Sidaway, G. (2016). Security breaches – What's the real cost to the business? *Credit Control,* 41-45.

Somanchi, S., & Telang, R. (2017). Impact of security events and fraudulent transactions on customer loyalty: A field study. *WEIS 2017*, 1-16. Retrieved from https://weis2017.econinfosec.org/program

Srinivasan, S., Paine, L., & Goyal, N. (2019). Cyber breach at Target. *Harvard Business School Case Studies.* Retrieved from www.hbsp.harvard.edu

U.S. News. (2017, September 8). Equifax breach could have 'decades of impact'. Retrieved from https://www.usnews.com/news/articles/2017-09-08/equifax-breach-could-have-decades-of-impact-on-consumers

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems, 19*(3), 150-159.

Wang, P., & Park, S. (2017). Communication in Cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems, 18*(2), 136-147.

Weiss, & Miller. (2015, February 4). The Target and other financial data breaches: Frequently asked questions. *Congressional Research Service,* 1-33. Retrieved from www.crs.gov