The Price of a Data Breach

In this modern age, the volume of data shared among different platforms has exponentially increased as technology becomes more prevalent across all industry sectors. Although technological advancements have improved efficiency, they have unintentionally increased the risk of confidential and other sensitive information becoming compromised. In 2017, the number of reported data breaches—incidents in which data are stolen or taken from a system without authorization and/or knowledge of their owner—reached a total of 1,579 in the United States, an almost 45 percent increase from the previous year.[1] Notable breach cases included the US Department of Homeland Security, LinkedIn and Yahoo. However, one of the most publicized cases involved Equifax's security breach. According to NBC News, Equifax admitted to a failure in remediation efforts after discovering a malicious infiltration caused by security weaknesses in March 2017. As a result of the infiltration, sensitive information such as names, dates of birth, Social Security numbers, and other personal identifiers of more than 143 million US consumers were compromised.[2]

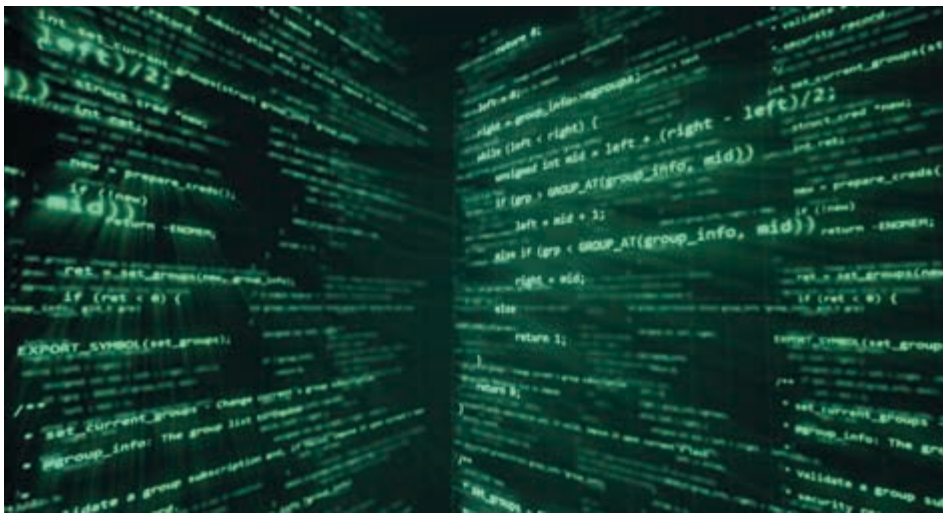
Approximately 82 percent of data breaches worldwide originate within the United States, whereas 12 percent originate from European countries (e.g., Ireland, Netherlands, the United Kingdom), Asian countries (e.g., China, India, Singapore) and Australia.[3] Although the United States accounts for a significant portion of data breaches, China experienced the highest volume of breached records, 3.8 billion within the first nine months of 2017.[4]

A common misconception is that data breaches, as in the case of Equifax, revolve around malicious hacking. However, these types of incidents account for less than half of reported breaches. Other data breach incidents occur due to unintended disclosure, negligence, insider leaks and physical hardware loss.[5] As organizations rely more heavily than ever on technology to carry out their missions, cybercriminals are also utilizing such advancements to fulfill their goals. Cybersecurity measures, such as implementing security controls and conducting assessments, should be prioritized by all organizations in the war against data breaches.

Investments in preventive controls (conducting security training and awareness and establishing information security policies, procedures and standards) and detective controls (performing continuous vulnerability assessment and testing, preparing an incident response plan) can possibly assist in minimizing the likelihood of a data breach.[6]

Impact of Data Breaches

The growing threat of data breaches has a rippling effect that impacts organizations, consumers and regulatory agencies. Once a data breach occurs, organizations are exposed to financial loss, reputation damage, legal fees, regulatory fines and loss of records. Consumers are subject to financial loss, fraud/identity theft and emotional distress. Data breaches may influence the creation of additional cybersecurity laws, cybersecurity funding and regulatory enforcement by regulatory agencies. Furthermore, regulatory agencies may look to



Van Ha Le
Is an associate within Williams Adley's IT risk management practice. Prior to joining the firm, she worked as a tax intern for UHY Advisors and was an audit intern for RSM. Le is a member of ISACA's Greater Washington DC Chapter.

Bianca Zamora
Is an associate in Williams Adley's IT risk management practice. Zamora is a member of ISACA's Greater Washington DC Chapter.

establishing new rules governing the appropriate actions an organization must take when disclosing a breach to its consumers.

Impact on Organizations

With more than 1,700 data breaches occurring around the world in 2017, organizations are becoming more vulnerable to cyberattacks as more data are stored digitally on cloud servers.[7] Although cloud services, such as Amazon Web Services, provide layers of infrastructure and software security, data breaches continue to occur due to human error. According to the IBM X-Force Threat Intelligence Index, "inadvertent activity such as misconfigured cloud infrastructure was responsible for the exposure of nearly 70 percent of compromised records."[8] Ultimately, any organizations with sensitive data, whether stored in the cloud or on-premise, are responsible for securing such data with proper configurations and access. However, even when actions are taken to actively safeguard sensitive information, the inherent risk of data breaches, and the threat of intentional hacking, will always remain. Based on a study of 5,500 companies across 26 countries, the direct cost of damage control related to incidents where confidential data were leaked averaged US $551,000 and US $69,000 for indirect spending.[9]

The most immediately felt impact for any organization is financial loss. Upon a data breach, organizations are faced with unexpected expenses in combatting the situation both internally and externally. Internally, time and money are poured into remediation efforts aimed at reducing the resulting damages. Activities commonly carried out upon discovery of a data breach include:[10]

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center procedures and specialized training

However, most breaches remain undetected for a long period of time. According to research conducted by the Ponemon Institute about the cost of data breaches, the mean time to identify (MTTI) a malicious attack is 214 days, with a mean time to contain (MTTC) of approximately 77 days. The study also suggests that the longer an organization takes to identify and contain a data breach, the higher the cost will be. If the MTTI was less than 100 days, the average data breach cost to resolve the situation was US $3.23 million. If it took more than 100 days, the cost was US $4.38 million.[11]

Within the estimated cost is the cost per lost record of information. For data breaches with evidence of malicious or criminal intent, the average cost per record to resolve such an attack runs higher, at approximately US $156, in comparison to US $128 from cases of system glitches or human error.[12] The increase in cost per record is associated with the potential of external hackers exploiting stolen confidential account information for personal gains.

A data breach may also signify the failure of a business process or the presence of an unqualified employee, either of which is likely to prompt an organization to equip itself with new technology and policies against potential future incidents. It is reported that organizations typically spend between US $3,500 and US $300,000 in new tools and services, awareness programs, administrative policies and additional staffing following a data breach. In cases of financial loss of less than US $1,000, investment in awareness programs is the most common response, while organizations with losses between US $1,000 and US $100,000 are more likely to invest in the development of administrative policies. Breaches resulting in the loss of more than US $1 million usually lead to administrative policy development, training and awareness, investment in technical tools, and additional staffing costs.[13]

While addressing the internal impact, organizations must also turn their attention to external matters in dealing with consumers and regulators. Public notification is one of the necessary upfront costs for organizations to consider. Forty-seven US states have enacted legislation mandating businesses to alert individuals of data breaches involving their personally identifiable information (PII). For example, the District of Columbia's Code § 28-3852 states that notifications are to be:

> *Made in the most expedient time possible and without unreasonable delay…with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.*[14]

Similarly, Costa Rica's Data Protection Law mandates the responsible party to report a data breach within five days following the incident. Such notification must include:

> *The nature of the incident; personal data that was subject to the data breach incident; corrective actions taken and the means or the place where appropriate/authorized personnel can get more information.*[15]

"IN THE WAKE OF PUBLIC NOTIFICATION, ORGANIZATIONS ARE ALSO VULNERABLE TO LITIGATION FROM CUSTOMERS, CLIENTS OR EMPLOYEES WHOSE INFORMATION WAS EXPOSED DURING THE BREACH."

Less stringent are the regulations in India where data breaches are not required to be reported unless they are categorized as a certain type of cybersecurity incidents.[16] The discrepancy in notification laws among different countries directly correlates to the costs for which each individual organization is responsible. For instance, since the US has more rigid laws, "notification costs for organizations in the US were the highest ($0.69 million), whereas India had the lowest ($0.02 million)."[17]

In the wake of public notification, organizations are also vulnerable to litigation from customers, clients or employees whose information was exposed during the breach. For example, in 2013, Target suffered a data breach in which cybercriminals compromised the information of 110 million of its consumers. Financial institutions such as Mutual Bank, Village Bank and CSE Federal Credit Union filed suit against Target in a Minnesota, USA, federal court demanding compensation for damages from the breach of leaked payment and contact information of millions of consumers' accounts. In 2016, Target agreed to pay the banks "$39 million plus costs and attorney's fees, and separately settled with Visa for $67 million."[18] Also, in May 2017, Target paid a US $18.5 million settlement for consumers' class action suits resulting from the same incident.[19]

Organizations may also face fines from government agencies such as the US Federal Trade Commission (FTC), the US Securities and Exchange Commission (SEC), or the US Department of Health and Human Services (HHS). Such government agencies establish regulations and guidelines to protect consumers' sensitive information. A recent (2016) example was the SEC's US $1 million imposed penalty charge on Morgan Stanley for its failure to design proper procedures against theft, which allowed an employee to copy 730,000 customers' account names and numbers to a personal server that was eventually hacked.[20] Even when the company released a statement reassuring the public that sensitive information such as account passwords and Social Security numbers was not compromised, client confidence was negatively impacted by the breach.

Organizations operating in the United Kingdom are potentially subject to fines from the independent authority known as Information Commissioner's Office (ICO), which oversees issues regarding individual information rights and privacy. An analysis from PricewaterhouseCoopers (PwC), a global consulting firm, revealed that breaches of UK's Data Protection Act during 2016 resulted in the ICO levying 35 fines totaling US $4.37 million.[21] On a wider scale, the European Union (EU) introduced a law known as the General Data Protection Regulation (GDPR) that became effective on 25 May 2018. The regulation mandates "businesses to protect the personal data and privacy of EU citizens for any transactions that occur within EU member states."[22] Included in the scope of such narrative are nearly any companies that have a web presence and market their products online, such as Amazon and eBay.[23] Another PwC survey detailed

that 92 percent of US companies are considering GDPR compliance a top priority, with 68 percent of such companies budgeting between US $1 million to $10 million to meet the requirements.[24] It is anticipated that once an organization violates the GDPR after it goes into effect, the penalty amount will drastically skyrocket as the fines can accumulate between 2-4 percent of the organization's worldwide annual revenue of prior financial year.[25] For example, as in the case of Hilton Domestic Operating Company, Inc. (Hilton), the hotel giant was charged in 2017 with a US $700,000 fine in response to two data breaches from 2015, exposing 350,000 customers' credit card and other information.[26] Since Hilton, just like numerous other US companies, has substantial operations in the EU, it is subject to the full effect of GDPR. By the same token, it is possible that the US $700,000 fines previously stated for Hilton would increase up to US $420 million under the new regulation.[27]

As a result of the implementation of GDPR, organizations face harsher penalties in cases of noncompliance to security requirements. Although Morgan Stanley's cost was approximately US $1.50 per record, future similar circumstances would render higher fines under the new GDPR. As mentioned previously, the cost for Hilton would have been US $1,200 per record if the regulation had been implemented at the time of the breach.

In addition to the financial impact of a data breach, organizations need to be aware of the hidden damages that can cause harm to their reputation and customer relationships. As reported by Ponemon Institute in 2017, US organizations exhibited the highest lost-business cost of US $4.13 million, which included abnormal turnover of customers, increased customer acquisition activities, tainted reputation and diminished goodwill.[28] Furthermore, established customer relationships may be faced with mistrust and uneasiness, and financial institutions and investors may become reluctant to provide capital to the breached entities because of the heightened risk. Although the hidden damages are difficult to quantify, it is important for businesses to recognize and prepare for their potential adverse impacts.

Impact on Consumers

Data breaches have a significant impact on consumers' daily lives. Once consumers become victim to the aftermath of a data breach, they are subject to financial setbacks and emotional distress, the result being that many consumers are reluctant to trust the organization again with their PII and other sensitive information. For example, after the 2013 Target data breach, the company stated net earnings in 2014 were US $520 million in the fourth quarter, down 46 percent from the same period a year earlier, when earnings were US $961 million.[29] This unfavorable change in consumers' shopping frequency exemplified their disapproval of the organization's lack of safety measures to protect their information. Usually when consumer perception is adversely impacted, it may be difficult to retain loyalty and trust. After a data breach, organizations can earn back consumers trust by being as responsive and transparent as possible. According to a survey conducted by PwC, 27 percent of consumers responded that trust can possibly be regained if organizations offer compensation for victims in the aftermath. Additionally, 22 percent of consumers stated they would like to know what happened and how it is being resolved.[30]

> "USUALLY WHEN CONSUMER PERCEPTION IS ADVERSELY IMPACTED, IT MAY BE DIFFICULT TO RETAIN LOYALTY AND TRUST."

When consumer information is compromised and personal information is stolen, many victims feel the need for compensation. According to a study conducted by the Ponemon Institute, 67 percent of consumers believe data breach victims should be compensated with cash or products. Additionally,

63 percent of consumers believe victims should be provided with identity theft protection services and 58 percent of consumers believe credit-monitoring services should be offered.[31] As reinforced by the statistics mentioned previously, consumers usually expect businesses to be accountable for any unexpected burden that may occur after a breach—even more so with the increasing number of cases of identity theft. According to the FTC's database of consumer complaints, consumers logged approximately 399,225 complaints of identity theft in 2016, placing it in one of the top-three complaint categories in the database.[32] Additionally, a Javelin Strategy and Research study stated identity thieves stole approximately US $16 billion from 15.4 million US consumers in 2016, an increase from the previous year when US $15.3 billion dollars was stolen from 13.1 million US consumers.[33] In addition, the median cost per US consumer incurred on each fraud-related complaint was US $450.[34] New research suggests that the cost of data breaches globally could increase up to US $2.1 trillion by 2019 because of the emerging digital economy.[35]

Most cases of identity theft are not resolved quickly and linger for months to years. After the Equifax breach in 2017, one of the 143 million data breach victims came forward with her personal identity theft story. According to a news article, Katie Van Fleet claimed her identity had been stolen more than 15 times and thieves had used her name to open several store credit cards and pay for hotel lodging in different states.[36] Van Fleet's case took several months to resolve even after she called the credit companies to dispute the use of her credit history. This example of identity theft highlights the frustration and violation data breach victims experience when their information is stolen. More disappointment ensues when organizations such as Equifax fall into the gray area of regulation because credit reporting agencies are much less regulated than other financial institutions.

Fraud and identity theft victims are subject to other financial setbacks as well, such as missing employment opportunities, taking time off from work or borrowing money. The lingering effects of fraud and identity theft leave consumers in a bind through financial uncertainty and distress. In a 2016 survey, the Identity Theft Resource Center (ITRC) found that 33.3 percent of US consumers closed existing financial accounts and used online accounts less frequently because of criminal identity theft. Additionally, 26 percent borrowed money from family/friends, and 6.7 percent obtained payday loans to pay expenses.[37] As a result of criminal identity theft, 22 percent took time off work, 15.3 percent sold possessions to pay for expenses and/or relocated or moved their location, and 11.3 percent applied for government benefits. The results of criminal identity thefts are numerous, but the long-term financial impact on consumers is astounding. Many of the respondents (38.2 percent) stated their ability to get credit cards was affected, and 34.2 percent of the respondents' ability to obtain loans was affected and/or denied post-incident. As shown by these statistics, the risk of criminal identity theft is mostly financial burden and uncertainty.

Along with financial setbacks, emotional distress is another concrete side effect of a data breach for consumers. ITRC also surveyed consumers on how distressing the misuse or attempted misuse of their personal information was and the response was an overwhelming 75.5 percent indicating that the event was severely distressing.[38] Once consumers fall victim to a data breach, there is usually a constant worry about the incident repeating itself. The perpetual threat of having their private information exposed leaves consumers with unwanted mental distress, especially individuals who were financially responsible and stable for most of their lives. Because of the amount of time and research they must do on their own to repair their credit, getting back on track post breach can be stressful for those individuals who were once financially stable. In the end, the emotional and financial impact consumers face can be substantial. If organizations do little to nothing to help consumers after damage is done, consumers may lose faith and eventually cut ties with a company.

Impact on Regulators

Because the volume and cost of data breaches have grown rapidly, many laws and regulations have been developed in the past 20 years to strengthen organizations' cybersecurity to protect affected parties and prevent cyberthreats. Countries

are making strides internationally to improve information security. For example, the EU introduced the Directive on Security of Network and Information Systems (NIS), which requires companies in critical industry sectors such as healthcare, transportation, energy and banking to adopt risk management practices and report incidents that can affect the Digital Single Market to their national authorities.[39] This law would also apply to online stores and cloud computing services to ensure that necessary security measures are taken.

> "THE INCREASE IN CYBERSECURITY LAWS INDICATES THE RECOGNITION OF THE IMPORTANCE OF PROPER IT INFRASTRUCTURE TO REDUCE THE OCCURRENCE OF DATA BREACHES."

In the United States, various states have taken measures to improve information security by mandating that government agencies and businesses implement certain security practices and promote cybersecurity infrastructure. The US National Conference of State Legislatures reports that 42 US states have introduced more than 240 bills in relation to cybersecurity with at least 28 states ultimately enacting such legislation in 2017. The new legislation in 2017 was noted as an increase in a 2016 report that stated only 28 states considered cybersecurity laws and 15 states enacted those laws.[40] The increase in cybersecurity laws indicates the recognition of the importance of proper IT infrastructure to reduce the occurrence of data breaches. The new laws mentioned previously aim to influence organizations by mandating the creation of cybersecurity commissions, studies or task forces, and establishment of cybersecurity training and education.

One example of these measures is Michigan's enacted house bill 4323, which aims to appropriate a portion of state funds for cybersecurity staffing, hardware and support costs. It requires departments to identify specific outcomes and performance measures, including, but not limited to, the following during the fiscal year ending 30 September 2018:[41]

- Reducing the number of cyberthreats based on the daily attacks to prevent data breaches
- Reducing the risk of cybervulnerabilities for application, data and network
- Increasing awareness of cyberthreats and the preventive steps for citizens, businesses and employees

The requirements of new legislation enable government agencies to act when addressing cyberthreats in the hope of alleviating the impacts of a data breach incident. Another example of states acting to address threats is when the state of New York proposed to modify banking laws by requiring lending institutions to provide customers with personal identification numbers (PINs) to use in combination with any chip-embedded credit card.[42] Although the bill currently holds a pending status, New York is making progress in mitigating the risk of data breaches.

The US federal government is also working to pass laws to combat cyberthreats. For example, the US Cyber Security Education and Federal Workforce Enhancement Act was introduced in February 2017 to:

> *Codify an office within the Department of Homeland Security (DHS) with the mission of strengthening the capacity of the agency to attract and retain highly trained computer and information security professionals.*[43]

The push toward cybersecurity education showcases the need for an enriched knowledge base to prevent future data breaches. In March 2017, changes were also suggested to the US National Institute of Standards and Technology (NIST) framework to "implement a framework, assessment, and audits for improving US cybersecurity" within the proposed NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017.[44] Most of the new and

existing legislation geared toward cybersecurity is developed and revised regularly to tackle potential effects caused by data breaches. In addition, several countries have announced initiatives to take action against cybersecurity threats internationally and locally. For example, Australia opened the Australian Cyber Security Center in November 2014 to help raise awareness of cybersecurity trends, report on the nature and extent of cyberthreats, and lead the Australian government's response to cyberthreats. Another example lies in the Middle East, where there has been more emphasis on cybersecurity education training in the past five years. A global cybereducation program introduced by Raytheon, a defense organization, was brought to Khalifa University (Abu Dhabi, United Arab Emirates). The program will focus on enhancing cybersecurity skills at the Cyber Operations Center of Excellence.[45]

> "US CONSUMERS AND BUSINESS GROUPS, HOWEVER, ARE DEMANDING A UNIFORM DATA BREACH NOTIFICATION LAW THAT IS INCLUSIVE OF ALL INDUSTRY SECTORS THAT HANDLE CONSUMER DATA."

In some cases, regardless of the cybersecurity efforts geared toward preventing data breaches, cybercriminals still manage to infiltrate sensitive data. For this reason, states in the US have begun implementing concise notification laws since it has become a primary concern for many states, as indicated by the approval of numerous bills across 47 states. US consumers and business groups, however, are demanding a uniform data breach notification law that is inclusive of all industry sectors that handle consumer data. The US National Retail Federation (NRF) petitioned Congress to pass federal legislation that requires any industry affected by data breaches to notify the public in a timely manner.[46] The NRF argues that no industry should be able to keep secret from the public any data breaches that create a risk of identity theft or financial harm. Since the Equifax breach, the pressure is on for the US Congress to act on a universal federal data breach notification law before another massive data breach hits another institution with sensitive consumer data. Internationally, countries have also created laws to notify the public in the case of a data breach. One example to consider is Israel's new Privacy Protection Regulations (Data Security) that took effect in May 2018. The new law imposes mandatory data security requirements and data breach notification requirements on organizations or individuals who own, manage and maintain information or personal data from citizens of Israel.[47] Similarly, the EU's GDPR requires every company that does business with citizens of EU member countries to notify authorities of a data breach within 72 hours of discovering the event or the organization will face steep fines.[48]

Impact on the Future

Organizations are increasing funding of IT security solutions to mitigate the potential impact of data breaches. After Target's experience with compromised payment methods, Target made improvements to its network to combat future security issues. Similar to New York's proposal to modify banking laws for credit/debit cards, Target implemented chip and PIN technology on its store cards to encrypt customers' transaction data with unique codes, making it difficult for hackers to use and/or duplicate.[49]

Other organizations and businesses are allocating additional resources to their cybersecurity budgets. For example, within a quarterly report issued on 3 August 2015, financial services giant JPMorgan Chase announced that it was increasing its cybersecurity research and development budget from US $250 million to US $500 million.[50] Commensurately, US federal agencies are ramping up cybersecurity funding, as shown by the White House's Cybersecurity National Action Plan. The plan proposed an investment of US $19 billion within the fiscal year 2017 budget for cybersecurity, representing

an increase of approximately 35 percent over fiscal year 2016.[51] The United States is not the only country making strides in strengthening its cybersecurity posture. According to the 2017 Global Cybersecurity Index report, the top 10 countries most committed to tackling cybercrimes are Australia, Canada, Estonia, France, Georgia, Malaysia, Mauritius, Oman, Singapore, and the United States.[52] Each country's ranking is assessed on its level of development within five categories: legal measures, technical measures, organizational measures, capacity building and cooperation. For example, Singapore's Cyber Security Agency established a fund of US $141 million for spending on cybersecurity research over the period from 2015 to 2020.[53] Singapore is one of the leaders in coordinating cybersecurity cooperation through codeveloping the Association of Southeast Asian Nations (ASEAN) Cyber Capacity Program, an initiative to "build capabilities across the region through tailored training programs, public-private partnerships, and discussions on policy and legislation."[54]

> "ORGANIZATIONS ARE PLACING MORE IMPORTANCE ON CYBERSECURITY BUDGETS TO BE BETTER PREPARED IF A BREACH DOES OCCUR."

It is evident that cybersecurity has become imperative to organizations' budgets in recent years. Many organizations align their security spending on practical operational areas, while ensuring compliance and continuous development. Organizations primarily focus their efforts on protection and prevention (72.4 percent) and detection and response (62.8 percent). Spending is followed by audit and compliance, which serves to protect sensitive data and ensure regulatory compliance.[55] Organizations are placing more importance on cybersecurity budgets to be better prepared if a breach does occur.

Conclusion

Increasingly, cybersecurity is becoming one of the top priorities within any organization globally. The frequency of data breaches has been escalating in recent years ever since sharing data across various platforms has become embedded in almost all areas of every industry sector. The overall impact data breaches have on businesses is significant in relation to their financials, reputation and customer retention. When it comes to consumers who are victims of identity theft, the impact is geared toward emotional and financial distress. As a result, the consumer backlash toward massive data breaches in organizations has led to petitions to the US Congress to act for tighter regulations and federal data privacy laws to protect and notify consumers in a timely manner when a data breach occurs. In addition, countries around the world are introducing stringent cybersecurity laws to hold certain organizations accountable for securing consumer information. Cybersecurity laws are being developed globally in response to the emerging digital economy and recognition of improving information security to combat cybercrimes that cost billions to consumers as well as organizations to remediate. It is crucial for businesses and organizations to increase cybersecurity efforts to reduce the occurrence and impact of data breaches.

Authors' Note

The authors would like to thank their reviewers, Jocelyn Hill and Charbet Duckett, and would like to give special thanks to Edwen Delcid and Tony Wang for giving them this opportunity.

Endnotes

1 Identity Theft Resource Center, "2017 Annual Data Breach Year-End Review," *https://www.idtheftcenter.org/2017-data-breaches*
2 Johnson, A.; "Equifax Breaks Down Just How Bad Last Year's Data Breach Was," NBC News, 8 May 2018, *https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496*
3 Gemalto NV, "The Reality of Data Breaches: Data Records Compromised in 2017," *https://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg*

4 Online Trust Alliance, *Cyber Incident and Breach Trends Report: Review and Analysis of 2017 Cyber Incidents, Trends, and Key Issues to Address*, 25 January 2018, *https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf*

5 TrendMicro, "Data Breach," *https://www.trendmicro.com/vinfo/us/security/definition/data-breach*

6 Clean Energy State Alliance, "Cyber Security and Information Assurance Controls Prevention and Reaction," November 2013, *www.cesa10.k12.wi.us/upload/document/362/cesasecurityawarenessandtraining-november2013.pdf*

7 Gemalto NV, "2017, The Year of Internal Threats and Accidental Data Breaches," *https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf*

8 IBM, "IBM X-Force Report: Fewer Records Breached in 2017 as Cybercriminals Focused on Ransomware and Destructive Attacks," IBM News Room, 4 April 2018, *http://newsroom.ibm.com/2018-04-04-IBM-X-Force-Report-Fewer-Records-Breached-In-2017-As-Cybercriminals-Focused-On-Ransomware-And-Destructive-Attacks*

9 Kaspersky Lab, "Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series," 2015, *https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf*

10 Ponemon Institute, *2016 Cost of Data Breach Study: Global Study*, June 2016, p. 26

11 Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, June 2017, p. 26-28

12 *Ibid*., p. 6

13 Filkins, B.; *Cleaning Up After a Breach, Post-Breach Impact: A Cost Compendium*, SANS Institute, December 2015, p. 19-20, *https://www.sans.org/reading-room/whitepapers/analyst/cleaning-breach-post-breach-impact-cost-compendium-36517*

14 Code of the District of Columbia, "§ 28-3852. Notification of Security Breach," 8 March 2007, *https://code.dccouncil.us/dc/council/code/sections/28-3852.html*

15 World Law Group, *Global Guide to Data Breach Notifications*, 2016, p. 43

16 *Ibid*., p. 80

17 *Op cit* Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, p. 5

18 Carter Ledyard & Milburn LLP, "Cybersecurity: Regulatory and Litigation Consequences of a Data Breach," 26 April 2017, *www.clm.com/docs/7942385_1.pdf*

19 McCoy, K.; "Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers," *USA Today*, 23 May 2017, *https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/*

20 Securities and Exchange Commission, "SEC: Morgan Stanley Failed to Safeguard Customer Data," USA, 8 June 2016, *https://www.sec.gov/news/pressrelease/2016-112.html*

21 PricewaterhouseCoopers, "Number of Fines for UK Data Privacy Issues Doubles and Totals £3.2m," 1 June 2017, *https://www.pwc.co.uk/press-room/press-releases/number-of-fines-for-UK-data-privacy-issues-doubles.html*

22 Nadeau, M.; "General Data Protection Regulation (GDPR) Requirements, Deadlines and Facts," *CSO*, 23 April 2018, *https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html*

23 Faitelson, Y.; "Yes, the GDPR Will Affect Your US-Based Business," *Forbes*, 4 December 2017, *https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/#1e771ed16ff2*

24 PricewaterhouseCoopers, "Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets," *https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html*

25 GDPR EU.org, "Fines and Penalties," *https://www.gdpreu.org/compliance/fines-and-penalties/*

26 Stempel, J.; "Hilton to Pay $700,000 Over Credit Card Data Breaches," *Reuters*, 31 October 2017, *https://www.reuters.com/article/us-hilton-wrldwide-settlement/hilton-to-pay-700000-over-credit-card-data-breaches-idUSKBN1D02L3*

27 Roberts, P.; "Hilton Was Fined $700K for a Data Breach. Under GDPR It Would Be $420M," *Digital Guardian*, 2 November 2017, *https://digitalguardian.com/blog/hilton-was-fined-700k-data-breach-under-gdpr-it-would-be-420m*

28 *Op cit* Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*

29 Target, "Target Reports Fourth Quarter and Full-Year Earnings," 26 February 2014, *https://corporate.target.com/press/releases/2014/02/target-reports-fourth-quarter-and-full-year-2013-e*

30 PricewaterhouseCoopers, "Consumer Intelligence Series: ProtectMe," *https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html*

31 Ponemon Institute, *The Aftermath of a Data Breach: Consumer Sentiment*, April 2014, p. 22, *https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf*

32 Federal Trade Commission, "FTC Releases Annual Summary of Consumer Complaints," USA, 3 March 2017, *https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints*

33 Javelin Strategy & Research, "Identity Fraud Hits Record High With 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study," 1 February 2017, *https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new*

34 Insurance Information Institute, "Facts + Statistics: Identity Theft and Cybercrime," *https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime*

35 Juniper Research, "Cybercrime Will Cost Business Over $2 Trillion by 2019," *https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion*

36 Mosbergen, D.; "Seattle Woman Says Her Identity Has Been Stolen 15 Times Since Equifax Data Breach," Huffpost, 30 October 2017, *https://www.huffingtonpost.com/entry/katie-van-fleet-equifax-stolen-identity_us_59f71d08e4b07fdc5fbf782d*

37 Identity Theft Resource Center, "Identity Theft: The Aftermath 2017," p. 7, *https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf*

38 *Ibid*.

39 European Parliament, "Cybersecurity: MEPs Back Rules to Help Vital Services Resist Online Threats," 7 June 2016, *www.europarl.europa.eu/news/en/press-room/20160701IPR34481/cybersecurity-meps-back-rules-to-help-vital-services-resist-online-threats*

40 National Conference of State Legislature, "Cybersecurity Legislation 2016," 8 December 2016, *www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx*

41 National Conference of State Legislature, "Cybersecurity Legislation 2017," USA, 29 December 2017, *www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx*

42 *Ibid*.

43 National Conference of State Legislature, "Federal Cybersecurity Legislation Proposed in the House and Senate," USA, *www.ncsl.org/Portals/1/Documents/Task_Forces/Cybersecurity_Legislation_in_115_Congress.pdf*

44 *Ibid*.

45 RadioResource International, "Cybersecurity Efforts Accelerate Around the World," 14 March 2016, *https://www.rrmediagroup.com/Features/FeaturesDetails/FID/648*

46 Shearman, J. C.; "Retailers Say Data Breach Notification Law Should Cover All Affected Businesses and 'Leave No Holes'," National Retail Federation, 13 February 2018, *https://nrf.com/media/press-releases/retailers-say-data-breach-notification-law-should-cover-all-affected-businesses*

47 Merken, S.; "Companies in Israel Facing New Data Security Regulations," *Bloomberg*, *https://www.bna.com/companies-israel-facing-n57982092558/*

48 European Union, General Data Protection Regulation, *https://www.eugdpr.org/*

49 Vasel, K.; "Target Just Made Its Credit Card a Lot Safer," *CNN Money*, 14 October 2015, *http://money.cnn.com/2015/10/14/pf/target-pin-credit-card/index.html*

50 Morgan, S.; "Why J.P. Morgan Chase & Co. Is Spending a Half Billion Dollars on Cybersecurity," *Forbes*, 30 January 2016, *https://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#5b4fd7422599*

51 The White House, Office of the Press Secretary, "Fact Sheet Cybersecurity National Action Plan," USA, 9 February 2016, *https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan*

52 International Telecommunication Union (ITU), *Global Cybersecurity Index 2017*, *https://www.itu.int/en/mediacentre/Pages/2017-PR29.aspx*

53 A.T. Kearney; *Cybersecurity in ASEAN: An Urgent Call to Action*, *https://www.atkearney.com/communications-media-technology/article?/a/cybersecurtity-in-asean-an-urgent-call-to-action-article*, p. 43,

54 *Ibid*.

55 Filkins, B.; "IT Security Spending Trends," SANS Institute, February 2016, p. 8, *https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697*