International Journal of Emerging Trends in Social Sciences
ISSN: 2521-3539
Vol. 8, No. 1, pp. 33-41, 2020
DOI: 10.20448/2001.81.33.41

Cost and Effects of Data Breaches, Precautions, and Disclosure Laws

Narendra Sharma[1]
Ebere A. Oriaku[2]
Ngozi Oriaku[3]

[1]*Associate Professor of Accounting, Department of Business, Accounting, and Sport Management, Elizabeth City State University, NC, USA.*
Email: nsharma@ecsu.edu
[2]*Endowed Professor of Economics, Department of Business, Accounting, and Sport Management, Elizabeth City State University, NC, USA.*
[3]*Professor of Management and Chair, Department of Business, Accounting, and Sport Management, Elizabeth City State University, NC, USA.*

Abstract

In recent times the breach of security systems or cyber-attacks leading to unauthorized acquisitions of computerized data that compromises the security, confidentiality, and integrity of personally identifiable information by many organizations has grown. There is a general belief that data breaches and today's organizational practices are axiomatically regarded as cause and effect. This paper addresses the cost of data breaches, disclosure laws, and precautions that have been instituted for many organizations and concludes that cybersecurity and data breach question is not "if" but "when" it might happen. Data has grown as one of the critical assets, and the absence of security protocols creates a vulnerability that can be misused by bad actors engaged in hacking and other forms of the data breach. This paper documents that the last decade experienced a phenomenal rise in the number of data breaches caused by hacking and the efficacy of disclosure laws that have been instituted by 48 states in the US. The frequency of data breach incidents has been alarming as billions of records have been breached and billions of dollars have been spent to mitigate those breaches, which could have been allocated for other projects. It is recommended that all organizations, big or small, have cybersecurity policies and a business continuity plan in place to deal with data breaches.

Keywords:
Data breach
Causes of a data breach
Data breach disclosure laws
Activity-based costing
Costing data breaches.

Publisher:
Scientific Publishing Institute

Accepted: *30 December 2019*
Published: *21 January 2020*

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.

1. What is a Data Breach?

The release of confidential data, commonly known as personally identifiable information, from a secured location in a computer or an electronic device to an unsecured site is a data breach. US Department of Health and Human Services (DHHS) for their purposes defines a breach as "generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information (US Department of Health and Human Services, 2009). Hence, DHHS considers not only the disclosure of protected information but also the impermissible use as a breach. California's data breach notification law defines a data breach as "breach of the security of the system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business" (State of California, 1988). Similarly, US National Initiative for Cybersecurity Careers and Studies (NICCS) (2018) in their glossary define data breach as "the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information." After the farming of Facebook data by Cambridge Analytica, there has been a growing demand to extend the definition of a data breach to include manipulation of data through

social engineering (Kilovaty, 2018). Howsoever is it defined; release of confidential data creates severe legal implications and public relation problems to the companies hosting and managing the data. Organizations are viewed suspiciously because of the general belief that it has been negligent in safeguarding the entrusted information by customers, employees, vendors, and others interacting with the company. Apart from the public image and legal implications, there is also a significant cost emanating from instances of such data breaches. Goldberg (2013) concluded that the lack of adequate mitigation and responses are more consequential and costly than the cost incurred for data protection.

Similarly, there are federal and state laws that require the breached company to notify affected individuals and government officials (Callahan, 2017). At the same time, the individuals whose confidential information has been compromised are adversely impacted and will have to take several measures to mitigate the release of their confidential information and subsequently possible identity thefts. Such individuals usually look upon the breached company to make reasonable the actual and any anticipated losses, they might suffer.

2. Causes of Data Breaches

Generally, a data breach occurs because of a lack of security, elimination of security, and a breach of security. Lack of security may be as a result of unwillingness on the part of the organization to consider itself to be prone to data breaches or is considered too cost-prohibitive to secure the information. Elimination of security may be as a result of slackness on the part of the organization to beef-up the data security, and either insiders or outsiders purposefully eliminate the security protocols to make the data vulnerable. Such elimination may also be because of accidental loss of privileges and equipment or some state-sponsored actors purposefully removing the security to create vulnerability - for e.g., Desjardins Group data breach exposing 2.9 million members was caused by an employee (Smith, 2019). Breach of security is intentional on the part of actors to steal the data using malware, hacking, virus, social engineering, cyber espionage, and sabotage. It could be accidental when sensitive information is leaked inadvertently by accidentally publication, configuration errors, improper encryption, lost computer, and privilege abuse (Cheng, Liu, & Yao, 2017).

A survey by Clearswift (2013) in the UK showed 42% of data breaches were targeted from outsiders, 58% were from insiders - extended enterprise (33% employees, 7% Ex-employees, and 18% third parties) -majority of internal security threats were as a result of inadvertent human error, lack of awareness, and malware via personal devices. McAfee (2017) reported a 43% -57% split between internal and external actors for data loss. The internal actors included employees, contractors, and third-party suppliers - half of the data loss was attributable as accidental. Wikina (2014) reported that data breaches involved computer systems and networks, desktop, laptops, paper records, emails, electronic health records, and portable devices. The researcher also reported that theft (47%) and loss (27%) - not hacking (7%) was the major type of data breaches reported. Table 1 shows the method data for the last five years:

The data in Table 1 shows that hacking came down from 17.2% to 9.2% in 2017 as compared to 2016, which may have been because of intervention strategies but it has slowly but surely climbed to 2016 level in the year 2019. It may have been very well that the hackers have found new ways, or the precautions taken by entities have slackened off over the years. Since hacking is one of the highest contributing methods with 69.5% instances followed by poor security of about 23%, a combination of laws, investment in precautionary measures, and training the cybersecurity personnel may be a better strategy (Ayyagari, 2012). Lost devices are some of the most interesting as many devices these days have a hard drive; a protocol for their disposal is a must. For e.g., a stolen digital camera belonging to the University of Arkansas for Medical Sciences (UAMS) in Little Rock contained photographs of new-borns and their information which was responsible for the data breach (Stolen Camera Creates Privacy Breach for Arkansas Hospital, 2011). The same is possible from copy machines, fax machines, and biomedical equipment.

The data in Table 2 shows the top 15 entities prone to data breaches and the number of records breached. It clearly indicated that technology and web-related entities are more prone to data breaches followed by government entities, and the financial sector. The data- points report worldwide figures and are not necessarily US-based entities only.

Table-1. Method of data breach in last 5 years.

	2015		2016		2017		2018		2019		Total Count	Total Percent
Method	**Count**	**Percent**	**Count**	**Percent**	**Count**	**Percent**	**Count**	**Percent**	**Count**	**Percent**		
Hacked	21	12.7%	30	17.2%	16	9.20%	24	13.8%	30	17.2%	121	69.5%
Inside job		0.00%	1	0.57%		0.00%	1	0.57%	1	0.57%	3	1.72%
Lost device		0.00%		0.00%	1	0.57%		0.00%		0.00%	1	0.57%
Oops!	1	0.57%	1	0.57%	2	1.15%	4	2.30%	1	0.57%	9	5.17%
Poor security	3	1.72%	1	0.57%	6	3.45%	17	9.77%	13	7.47%	40	22.99%
Grand total	25	14.37%	33	18.97%	25	14.37%	46	26.44%	45	25.86%	174	100.00%

Source: McCandless (2019)

Table-2. *Sector-wise data breaches methods and records lost.*

Sector/ Method	Hacked	Inside Job	Lost Device	Oops!	Poor Security	Grand Total
Tech	113,075,000		200,000	14,767,232	12,407,950,000	12,535,992,232
Web	6,067,864,339	92,000,000		1,396,000,000	2,002,541,298	9,558,405,637
Government	169,117,025	4,192,000	61,094,500	1,021,240,396	1,103,000,000	2,358,643,921
Financial	522,420,083	237,688,000	22,534,000	150,000	899,125,000	1,681,917,083
App	390,300,000				587,849,000	978,149,000
Retail	749,644,025	8,637,405	897,000	7,000,000	39,300,000	805,478,430
Gaming	209,930,755					209,930,755
Healthcare	122,097,798	6,512,000	33,533,702	550,000	14,775,350	177,468,850
Telecoms	90,671,000	2,000,000	17,113,000	170,000	32,000,000	141,954,000
Transport	76,030,000			2,394,000	18,052,000	96,476,000
Military	935,000		76,131,000			77,066,000
Media	11,270,000				51,200,000	62,470,000
Energy	110,000	12,900,000				13,010,000
Legal	11,500,000					11,500,000
Academic	1,392,000		4,372,000	43,000	146,000	5,953,000
Grand total	8,536,357,025	363,929,405	215,875,202	2,442,314,628	17,155,938,648	28,714,414,908

Source: McCandless (2019)

Another devasting data breaches over the years have been caused by the use of ransomware when the hackers encrypt the data of the target organizations and demand ransom to decrypt the data. Commonly known ransom wares are Cryptologer in 2014, Teslacrypt in 2016, Wanacry in 2017, Cryptowall, and AlphaCrypt (Hammouchia, Cherqia, Mezzoura, Ghoghoa, & El Koutbib, 2019; Rashid, 2016).

The other causes of data breaches resulting in cyber frauds are phishing, spyware, pharming, and spoofing. There are also internal causes of data breaches. Intelligence and National Security Alliance (2013) have identified four insider threats: fraud, theft of intellectual property, IT sabotage and Espionage.

Due to several possibilities of data breaches, massive data breaches have been reported. Notable recent data breaches in 2019 are listed in Table 3. In some of the instances, data was farmed by legitimate users, others were breached using other methods discussed above.

Table-3. *Top 10 data breaches and number of records lost in 2019.*

Year	2019
Entity	**Number of Records Lost**
People Data Labs	3,000,000,000
First American Financial Corporation	885,000,000
Facebook	419,000,000
OxyData	380,000,000
Indian Jobseekers	275,265,298
Dubsmash	162,000,000
Canva	139,000,000
Capital One	100,000,000
Houzz	57,000,000
Chtrbox	49,000,000
Grand Total	5,466,265,298

Source: McCandless (2019)

Table-4. *Data breaches annual comparisons.*

Industry	2018		2017	
	Breaches	**Records**	**Breaches**	**Records**
Banking/Credit/Financial	135	1,709,013	134	3,230,308
Business	571	415,233,143	907	181,630,520
Education	76	1,408,670	128	1,418,455
Government/Military	99	18,236,710	79	6,030,619
Medical/Healthcare	363	9,927,798	384	5,302,846
Totals	1,244	446,515,334	1,632	197,612,748

Source: Identity Theft Resource Center (ITRC) (2019).

The data in Table 4 shows that the total number of breaches reported in 2018 as compared to 2017 has decreased but the number of records has increased substantially- more than 100%. The data clearly shows that data breaches have become prevalent, but also the impact has been enormous, with billions of records breached.

3. Effect of Data Breaches

Gatzlaff and McCullough (2010) examined the stock market's reaction to data breaches in publicly listed companies and concluded that data breaches negatively affected shareholder wealth, especially for those firms with higher market-to-book ratios. Garg, Curtis, and Halper (2003) reported a 0.5% -1.0% loss of revenue on an annual basis. They also said that the insurance-sector reacted favorably in anticipation of increased cyber-insurance sales and the higher premiums resulting from a heightened awareness of cyber-insurance. Supriya (2018) asserted that depending upon the organization and information breached, the affected organization may lose its financial sustainability in one extreme to not being an issue at all in another extreme of the spectrum. For organizations, like Health and Education, a data breach will lead to privacy concerns relating to the Health Insurance Portability and Accountability Act (HIPAA) and the Family Education Rights and Privacy Act (FERPA) violations. They may not face financial consequences unless the data is tampered with impacting the integrity of the information but will suffer punitive and compensatory damages when the breached data becomes available on the darknet. The impact is judged on confidentiality, integrity, and availability of the data breached. For example, a data breach at Facebook created its stock price to lose value but it was a minor issue for them in terms of confidentiality as no credit card information was stolen. Therefore, the effect could be explicit or implicit, and both. The outcome will be felt differently by the organization, and those impacted individuals whose personally identifiable information has been breached. The risk factor is more for companies

that store, process, and transmit sensitive information like a credit card, social security numbers, medical records, educational records, financial records, and other personally identifiable information.

Toe (2013) considered the three areas: organizational reputation, customer resentment, and possible lawsuits apart from immediate operating expenses for customer notification, upgrades in security infrastructure, and credit monitoring service costs and regulatory or industry-specific fines. All these have explicit and implicit financial implications (Confente, Siciliano, Gaudenzi, & Eickhoff, 2019). Some could result in the bankruptcy of the victim organizations like the American Medical Collection Agency (AMCA) whose data breach compromised 20 million records (Stone, 2019) and filed for bankruptcy immediately following the breach. On the other hand, Plachkinova and Maurer (2018) opined that despite one of the most significant data breaches in history, Target is still a successful business. The initial estimate of the costs to Target was reported $ 3.6 billion. The resiliency to come out of such an event could a business continuity plan which kicks in, and the crisis is managed.

Solove and Citron (2018b) laid out the concept of data breach harm as a result of risk and anxiety for those whose information has been compromised by the data breach. E.g., Marriott breach resulted in loss of hundreds of millions of customer details, including credit card and passport numbers which has ensued the risk of those information being misused by bad actors (Fruhlinger, 2019a) leading to possible class lawsuits citing three injuries: "(1) the cost of fraudulent transactions, (2) the increased risk of future identity theft resulting from the breach, and (3) the burden of closing affected accounts and opening new ones" (Richie, 2015). Berezina, Cobanoglu, Miller, and Kwansa (2012) concluded that data breaches in a hotel led to a decrease in customers' perceptions of reliability and assurance of quality services. Lending, Minnick, and Schorno (2018) found that banks with data breaches had significant declines in deposits and nonbanks had substantial decreases in sales in the long run. Furthermore, they reported companies were more likely to replace their chief executive officer and chief technology officer and invest more to improve in their corporate governance and social responsibilities. Fruhlinger (2019b) reported that Equifax had spent $1.4 billion on clean-up costs, including the cost for the transformation of technology to improve the application, network, and data security. On the other hand, there still is a lot of anxiety for almost 40% of Americans whose data was exfiltrated in the Equifax hack Fruhlinger (2019b).

4. What happens to the Breached Records?

Data breaches happen because the data stolen is of value as it can be used to defraud the businesses and steal the identities of those whose personal information was breached (Bellemare, 2017). Onaolapo, Mariconti, and Stringhini (2016) reported that criminals use the breached information to profit themselves, release them publicly, or sell them in the darknet. There are three segments of the internet: the surface net, the deep-net, and the darknet. The surface net is unprotected like a searchable website or news or open-source websites. The deep-net requires some identification and authorization to access websites like health care websites, utility websites, and banking websites. The darknet is that part of deep-net that consists of hidden websites that require special software to access where the sale of user IDs and other information takes place (Chertoff, 2017). The use of cryptocurrencies has made it difficult to track the illegal transactions for law enforcement agencies.

5. Precautions

There are two levels of precautions entities can take: basic and dedicated. The basic security mechanisms are primary security measures like firewalls, antivirus software, intrusion detection, authentication, access control, and encryption. The dedicated systems are more sophisticated and designed to deal with data breaches, and geared towards, identifying, monitoring, and protecting confidential data from unapproved access. Cheng et al. (2017) suggested a dedicated system that is both a content-based approach and a context-based approach. They summarized the existing techniques in Table 5.

Table-5. *Content and context techniques of dedicated system.*

Technique	Analysis	Pros	Cons
Fingerprinting	Content	Simple, Better coverage	Very sensitive to data modification
Regular expressions	Content	Simple, Tolerate certain noises	Limited data protection, High false positive
Collection intersection	Content	Wide data protection, Capture local features	High computation and storage cost, Inapplicable to evolved or obfuscated data
Machine learning	Content/ Context	Resilient to data modifications, High accuracy	Large training data, Complicated
Behavior analysis	Context	Mitigate insider threats	Large training data, High false positives
Watermarking	Context	Forensics analysis	Vulnerable to malicious removal or distortion
Honeypots	Context	Detect malicious insiders	Limited applications

Source: Cheng et al. (2017).

Researchers have also critically examined some of the important measures. Gritzalis (2004) argued that although the encryption of information exchanged between Web servers is one of the essential precautions one can take to deal with confidentiality of the data but encryption would not protect the privacy of the client from the server since it is limited to maintaining the confidentiality of the content. One of the most widely suggested approaches has been the anonymization of networks based on the onion router system that aims to achieve confidentiality and anonymity of networks. Tor, I2P, Tails, Freenet, and VPN are some of the popular choices of security professionals for such anonymization of systems geared towards preserving user's privacy and securing data. Jahani and Jalili (2018) argued that the anonymization of a network aimed to protect data by hiding traffic data flow to avoid exploitation of data that gets saved at routers and Internet Service Provider zones. However, the researchers concluded that website fingerprinting attack was possible even for such networks and thus making Tor or VPN vulnerable to sophisticated intruders. Lee, Kim, and Kim (2019) suggested a moving target defence method that puts in place a system of random change of file extensions that ransomware attempts to encrypt. Harrell (2019) believed that some identity thieves await a long period before using the information to commit fraud and suggested that all affected persons should remain vigilant in the short-run as well as in the long-run.

Intelligence and National Security Alliance (2013) found precautionary measures for insider threat to include insider threat mitigation programs with a formal insider threat structure either as an incidental response team or a multi-departmental focused team and insider threat awareness programs including presentations, mandatory annual training, training focused on social engineering, informal helpdesk team training, targeted training modules, training for all users with specific privileges, and training on how to handle potential foreign intelligence.

Hayslip (2018) suggested 9 policies and procedures for a cybersecurity program which are: 1) acceptable use policy, 2) access control policy, 3) changes to IT policy, 4) information security policy, 5) incident response policy, 6) remote access policy, 7) email/communication policy, 8) disaster recovery policy, and 9) business continuity plan.

6. Data Breach Disclosure Laws

There are 48 states (except Alabama and South Dakota) that have responded to the growing data breaches by adopting data breach disclosure laws that require the organizations to notify customers about their personal information lost in a data breach (IT Governance, 2018). California's Security Breach Information Act and California's Consumer Privacy Act that came into effect on January 1, 2020 are probably the most elaborate data breach and privacy related laws. Several federal statutes govern data breach and privacy regulations like Fair Accurate Credit Transactions Act, Gramm-Leach-Bliley, FERPA, HIPAA, No Electronic Theft Act, Economic Espionage Act, Computer Fraud and Abuse Act, Identity Theft Assumption and Deterrence Act, Computer Security Act, National Infrastructure Act, Federal Information Security Management Act, Defence Federal Regulation Supplement. Similarly, public companies like Equifax, Uber, Target, CapitalOne are required by the Securities Act of 1933 and Securities Exchange Act of 1934 to disclose a data breach in the management and discussion analysis section of their periodic reports. Robbins and Sechooler (2018) asserted that recent high-profile data breaches were material events, triggering duties to disclose or to refrain from trading for corporations governed by the Securities and Exchange Commission (SEC). Apart from the national laws, there are some well-known international regulations like Basel II Capital Accord and EU's General Data Protection Regulations. Romanosky, Telang, and Acquisti (2011) found that the adoption of data breach disclosure laws reduced identity theft caused by data breaches.

7. Costing of a Data Breach

IBM Security and Ponemon Institute released their report for 2019 and reported global average cost of a data breach was $3.9 million -with a highest cost average of $ 8.19 in US, average cost per record lost was $150, the health care industry was the most costly industry with $6.45 million average costs, and a breach lifecycle cost $1.2 million less than when a lifecycle was more than 200 days (IBM Security, 2019). The report further elaborated that 67% of the cost was incurred in the first year, 22% of cost in the second year and 11% of cost occurred after two years. The formation of an incident response team would reduce the cost of a data breach by $360,000. Other key findings were:

- Lost business was the biggest contributor to costs.
- Data breach costs impacted organizations for years.
- The lifecycle of a data breach increased by 4.9% in 2019 as compared to 2018.
- Malicious attacks were the most common cause of breaches with 51% of breaches attributable to such attacks.
- Breaches from system glitches and the human error still account for 49% of data breaches.
- Smaller businesses faced disproportionately higher costs as compared to larger organizations.
- Cloud migration, IT complexity and third-party breaches were identified as cost amplifiers'.

- Encryption, business continuity management, and threat sharing were cost mitigators.
- Automation of security reduced costs.
- The odds of experiencing a data breach has increased over the years.

IBM Security (2019) explained the method of calculating the cost of a data breach was based on an activity-based costing approach. The activity-based costing method utilizes multiple activity drivers to allocate the costs to an identifiable cost object as compared to a single volume-based driver (Kaplan & Cooper, 1998). IBM Security and Ponemon Institute report used four cost centers: detection and escalation, notification, post-data breach, and lost business costs. Similarly, the following cost drivers associated with each of the cost centers were identified:

7.1. Detection and Escalation

- Forensic and investigative activities.
- Assessment and audit services.
- Crisis team management.
- Communications to executive management and board of directors.

7.2. Notification

- Emails, letters, outbound telephone calls, or general notice to data subjects that their personal information was lost or stolen.
- Communication with regulators; determination of all regulatory requirements, engagement of outside experts.

7.3. Post-data breach

- Help desk activities / Inbound communications.
- Credit report monitoring and identity protection services.
- Issuing new accounts or credit cards.
- Legal expenditures.
- Product discounts.
- Regulatory interventions (fines).

7.4. Lost business costs

- Cost of lost customers and acquiring new customers (customer turnover).
- Reputation losses and diminished goodwill.

8. Conclusions and Recommendations

In view of several findings on the topic, some conclusions have been made: A data breach has been defined in several ways but the simplest one is the release of personally identifiable information from a secured location to an unsecured location. Howsoever it is defined, data breaches create severe legal implications and public relation crisis to the companies managing the data. Organizations are viewed suspiciously because of the general belief that it has been negligent in safeguarding the entrusted information by customers, employees, vendors, and others interacting with the company. Apart from the public image and legal implications, there is also a significant cost emanating from instances of such data breaches.

There are several causes of data breaches, but, generally, a data breach occurs because of a lack of security, elimination of security, and a breach of security either by actions of external or internal actors. The modus operandi could be as a result of malware, hacking, virus, social engineering, cyber espionage, sabotage or inadvertently leaked by accidental publication, configuration errors, improper encryption, lost computer, and privilege abuse. Based on global data, technology and web-related entities are more prone to data breaches, followed by government entities and the financial sector. Data breaches negatively affect shareholder wealth, but insurance-sector companies could be impacted favorably in anticipation of increased cyber-insurance sales and the higher premiums resulting from a heightened awareness of cyber-insurance. Some affected organizations may lose their financial sustainability and go bankrupt but if it is managed appropriately, the crisis could be used to harden infrastructure and enhance corporate governance mechanisms for better outcomes.

The risk factor, in terms of costs, seems to be higher for the health care sector and generally for companies that store, process, and transmit sensitive information like credit cards, social security numbers, medical records, educational records, financial records, and other personally identifiable information. Apart from effects for organizations, affected individuals whose data is compromised can also be impacted with increased risk of identity theft, the anxiety of possible misuse of the data for fraud. Most data breaches happen because the data stolen is of value as it can be used to defraud the businesses and steal the identities of those

whose personal information was breached. There are two levels of precautions entities can take: basic and dedicated. The basic security mechanisms are security measures like firewall, antivirus software, intrusion detection, authentication, access control, and encryption. The dedicated systems are designed to deal with data breaches, and it is geared towards, identifying, monitoring, and protecting confidential data from unapproved access. All states in the US (except Alabama and South Dakota) have data breach disclosure laws. There are also several federal statutes that govern data breach and privacy regulations. The cost of a data breach can be computed using the activity-based costing system by identifying appropriate cost centers and cost drivers.

It is recommended that organizations and individuals have a plan in place because data breach is eminent as the question is not if but when. All organizations need to have policies and procedures for a cybersecurity program against possible breach externally and internally. The plan in place will minimize undue costs and problems to any organization, big or small, that will face data breach.

References

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security*, *8*(2), 33-56. Available at: https://doi.org/10.1080/15536548.2012.10845654.

Bellemare, J. (2017). What happens to stolen data after a breach. Identity Force (Blog). Retrieved from: https://www.identityforce.com/blog/what-happens-stolen-data

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991-1010. Available at: https://doi.org/10.1108/09596111211258883.

Callahan, M. E. (2017). Once more into the breach. *Criminal Justice*, *32*(2), 20-23.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), 1-14. Available at: https://doi.org/10.1002/widm.1211.

Chertoff, M. (2017). A public policy perspective of the dark web. *Journal of Cyber Policy*, *2*(1), 26-38. Available at: https://doi.org/10.1080/23738871.2017.1298643.

Clearswift. (2013). The enemy within research 2013. Retrieved from: https://www.clearswift.com/about-us/pr/press-releases/enemy-within-research-2013.

Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal*, *37*(4), 492-504. Available at: https://doi.org/10.1016/j.emj.2019.01.007.

Fruhlinger, J. (2019a). Equifax data breach FAQ: What happened, who was affected, what was the impact? CSO (Online), Retrieved from: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Fruhlinger, J. (2019b). Marriott data breach FAQ: How did it happen and what was the impact? CSO (Online). Retrieved from: https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think? *Information Systems Security*, *12*(1), 22-33. Available at: 10.1201/1086/43325.12.1.20030301/41478.5.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61-83. Available at: https://doi.org/10.1111/j.1540-6296.2010.01178.x.

Goldberg, E. (2013). Preventing a data breach from becoming a disaster. *Journal of Business Continuity & Emergency Planning*, *6*(4), 295-303.

Gritzalis, S. (2004). Enhancing web privacy and anonymity in the digital era. *Information Management & Computer Security*, *12*(3), 255-287. Available at: https://doi.org/10.1108/09685220410542615.

Hammouchia, H., Cherqia, O., Mezzoura, G., Ghoghoa, M., & El Koutbib, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, *151*, 1004-1009. Available at: https://doi.org/10.1016/j.procs.2019.04.141.

Harrell, E. (2019). How to help your clients when a data breach hits. InforArmor(blog). Retrieved from: https://blog.infoarmor.com/brokers/author/eric-harrell.

Hayslip, G. (2018). 9 policies and procedures you need to know about if you're starting a new security program. Adaptive Security. Retrieved from: https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html.

IBM Security. (2019). Cost of a data breach report 2019. IBM Security and Ponemon Institute. Retrieved from: https://databreachcalculator.mybluemix.net.

Identity Theft Resource Center (ITRC). (2019). 2018 end-of-year data breach report, Retrieved from: https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

Intelligence and National Security Alliance. (2013). A preliminary examinations of insider threat programs in the US private sector. Retrieved from: https://www.insaonline.org/wp-content/uploads/2017/04/INSA_InsiderThreat_WP.pdf.

IT Governance. (2018). Data breach notification laws by state. Retrieved from: https://www.itgovernanceusa.com/data-breach-notification-laws.

Jahani, H., & Jalili, S. (2018). Online tor privacy breach through website fingerprinting attack. *Journal of Network and Systems Management*, *27*(2), 289-326.

Kaplan, R. S., & Cooper, R. (1998). *Cost & effect: Using integrated cost systems to drive profitability and performance*. Boston, MA: Harvard Business School Press.

Kilovaty, I. (2018). Data breach through social engineering. Retrieved from: https://blog.harvardlawreview.org/data-breach-through-social-engineering.

Lee, S., Kim, H. K., & Kim, K. (2019). Ransomware protection using the moving target defense perspective. *Computers & Electrical Engineering, 78*, 288-299. Available at: https://doi.org/10.1016/j.compeleceng.2019.07.014.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review, 53*(2), 413-455. Available at: https://doi.org/10.1111/fire.12160.

McAfee. (2017). Data exfiltration study: Actors, tactics, and detection. Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf.

McCandless, D. (2019). World's biggest data breaches. Retrieved from: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

Onaolapo, J., Mariconti, E., & Stringhini, G. (2016). *What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild*. Paper presented at the Paper Presented at the 2016 Internet Measurement Conference.

Plachkinova, M., & Maurer, C. (2018). Teaching case: Security breach at target. *Journal of Information Systems Education, 29*(1), 11-19.

Rashid, F. Y. (2016). Ransomware targets flash and silverlight vulnerabilities. Retrieved from InfoWorld: https://www.infoworld.com/article/3046531/ransomware-targets-flash-and-silverlight-vulnerabilities.html.

Richie, J. T. (2015). Data breach class actions. *GP Solo, 32*(5), 66.

Robbins, J. M., & Sechooler, A. M. (2018). Once more unto the breach: What the equifax and uber data breaches reveal about the intersection of information security and the enforecement of securities laws. *Criminal Justice, 33*(1), 4-7. Available at: https://doi.org/10.1016/s1353-4858(12)70090-9.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2), 256-286. Available at: https://doi.org/10.1002/pam.20567.

Smith, C. (2019). Massive desjardins group data breach caused by employee who's since been fired. Straight Talk. Retrieved from https://www.straight.com/news/1257561/massive-desjardins-group-data-breach-caused-employee-whos-been-fired.

Solove, D. J., & Citron, D. K. (2018b). Risk and anxiety: A theory of data-breach harms. *Texas Law Review, 96*(4), 737-786.

State of California. (1988). Civil code section 1798.82. Retrieved from http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

Stolen Camera Creates Privacy Breach for Arkansas Hospital. (2011). Briefings on hospital safety. Retrieved from https://link-gale-com.ecsu1891.idm.oclc.org/apps/doc/A243802405/AONE?u=ncliveecsu&sid=AONE&xid=b05c306e. *19*(1), 8.

Stone, J. (2019). AMCA parent company files for bankruptcy amid data breach fallout. Cyberscoop. Retrieved from: https://www.cyberscoop.com/amca-bankruptcy-data-breach-quest-diagnostics-labcorp/.

Supriya, R. (2018). What happens to an organization after a data breach? Dataquest, Retrieved from: https://www.dqindia.com/happens-organization-data-breach/.

Toe, C. A. (2013). An examination of the explicit costs of sensitive information security breaches (Doctoral Dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3588090).

US Department of Health and Human Services. (2009). Definition of breach. Retrieved from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

US National Initiative for Cybersecurity Careers and Studies (NICCS). (2018). Glossary. Retrieved from: https://niccs.us-cert.gov/about-niccs/glossary#D.

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management, 11*(Fall).