DATA BREACHES

Drew Diedrich*

CITE AS: 4 GEO. L. TECH. REV. 315 (2019)

TABLE OF CONTENTS

I. INTRODUCTION: DATA BREACHES IN MODERN SOCIETY 315
II. WHAT IS A DATA BREACH, AND HOW DOES IT OCCUR? 316
A. Data Breaches from Human Error 317
B. Data Breaches from System Glitches 318
C. Malicious or Criminal Data Breaches... 319
1. *Malware Infections* 319
2. *Hacking* 321
3. *Social Engineering* 322
III. WHY MALICIOUS ACTORS CONDUCT DATA BREACHES 322
A. Financial Gain 323
B. Espionage 323
IV. CONCLUSION 324

I. INTRODUCTION: DATA BREACHES IN MODERN SOCIETY

To say that data breaches are ubiquitous within the modern digital society may be an understatement.[1] Over the past fifteen years, more than ten billion records have been breached from over 9,000 data breaches in the United States, impacting a majority of Americans.[2] In the first three months of 2019 alone, there were twenty data breaches that each exposed over ten million

* Georgetown University Law Center, J.D. Candidate 2020; Cornell University, B.A. Government, 2017. Thank you to all the editors on the Georgetown Law Technology Review for their help and advice.

[1] *See Roughly Half of Americans Do Not Trust the Federal Government or Social Media Sites to Protect Their Data*, PEW RES. CENTER (Jan. 23, 2017), https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/pi_01-26-cyber-00-02 [https://perma.cc/7EUT-HAKW].

[2] Aaron Smith, *Americans and Cybersecurity*, PEW RES. CENTER (Jan. 26, 2017), https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity [https://perma.cc/243G-VCQW]; *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://privacyrights.org/data-breaches (accessed Oct. 20, 2019) [https://perma.cc/AE3L-G3U4].

records.[3] Data breaches have hit all sectors and industries, from businesses and medical organizations to governments and educational entities.[4] Within the past year, Dunkin' Donuts, Facebook, the Atlanta Hawks, Uniqlo, and the Federal Emergency Management Agency (FEMA) were some of the many victims.[5] Even law firms have been targeted.[6] In response to the prevalence of breaches, legal clients increasingly demand work in the realm of data breaches.[7] A working knowledge of how they occur may prove useful to many attorneys.

II. WHAT IS A DATA BREACH, AND HOW DOES IT OCCUR?

Data breaches are not consistently defined across jurisdictions. Federal legislation for specific sectors, regulations from agencies, state statutes, and even international bodies establish rules governing data breaches, resulting in a variety of data breach definitions.[8] Further, the private data security sector

[3] RISK BASED SEC., INC., DATA BREACH QUICKVIEW REPORT-FIRST QUARTER 2019 DATA BREACH TRENDS 3 (Apr. 30, 2019), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Q1%20Data%20Breach%20QuickView%20Report.pdf [https://perma.cc/JUV4-G8M4].

[4] *Id.* at 1, 10.

[5] Steve Turner, *2019 Data Breaches—The Worst so Far*, IDENTITY FORCE (Jan. 3 2019), https://www.identityforce.com/blog/2019-data-breaches [https://perma.cc/9WKK-2WUV].

[6] Debra C. Weiss, *More Than 100 Law Firms Have Reported Data Breaches; 2 BigLaw Firms Affected,* ABA J. (Oct. 18, 2019), http://www.abajournal.com/news/article/more-than-100-law-firms-have-reported-data-breaches-2-biglaw-firms-affected [https://perma.cc/53VA-L7CX].

[7] *Five Legal Trends to Watch in 2019,* LEXISNEXIS (Feb. 28, 2019), https://www.lexisnexis.com/community/lexis-legal-advantage/b/trends/posts/five-legal-trends-to-watch-in-2019 [https://perma.cc/H9CX-HCLY]; *see* Monique C.M. Leahy, *Litigation of Data Breach*, 14 AM. JUR. TRIALS 327 § I(1), para. 7 (2015); Chris Cwalina et al., *Nine States Pass New and Expanded Data Breach Notification Laws,* NORTON ROSE FULBRIGHT (Jun. 27, 2019), https://www.dataprotectionreport.com/2019/06/nine-states-pass-new-and-expanded-data-breach-notification-laws/ [https://perma.cc/T8L7-485G].

[8] Regulation 2016/679, art. 4, 2016 O.J. (L 119) 33 (EU), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL [https://perma.cc/8DD4-WUYK]; FEDERAL DEPOSIT INSURANCE CORP., FIL-27-2005, FINAL GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE (2005), https://www.fdic.gov/news/news/financial/2005/fil2705.pdf [https://perma.cc/A3FL-ZX88]; *State Data Breach Notification Laws,* FOLEY & LARDNER LLP, (Nov. 11, 2019), https://www.foley.com/-/media/files/insights/publications/2019/11/19mc23532-data-breach-chart-update-101419.pdf [https://perma.cc/RN6E-4QAN]; Dave Maxfield & Bill Latham, *Data Breaches*: *Perspectives from Both Sides of the Wall,* 25 S.C. LAW. 28, 30 (2014),

creates its own definitions while combatting data breaches.[9] Generally, these sources define a data breach as an unintentional release of secure or personally identifiable information to an unsecure environment.[10]

This personally identifiable information is data that is attributable and identifiable to one person.[11] Email addresses and passwords are most frequently stolen, but other frequent targets include credit card numbers and financial information.[12] Separate from personally identifiable information, data breaches may result in the exposure of sensitive corporate information, such as business-sensitive trade secrets.[13] The annual "Cost of A Data Breach" study conducted by the Ponemon Institute estimated that roughly one quarter of data breaches in 2019 resulted from human error ("breaches caused by neglect or error by a person"), one quarter followed system glitches ("breaches caused by technology failures"), and the remaining half were caused by malicious or criminal attacks.[14]

A. Data Breaches from Human Error

Human error, or "an error caused by neglect or error by a person," that results in a data breach may be frustrating as it appears to be the most

[9] *Data Breach*, TREND MICRO (2019), https://www.trendmicro.com/vinfo/us/security/definition/data-breach, (accessed Oct. 19, 2019) [https://perma.cc/J45F-J48P]; Steve Symanovich, *What is a Data Breach?*, NORTON LIFELOCK, https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html (accessed Nov. 20, 2019) [https://perma.cc/C46V-M3RV]; *What is a Data Breach*, KASPERSKY (2019), https://usa.kaspersky.com/resource-center/definitions/data-breach [https://perma.cc/J55Y-H785].

[10] *State Data Breach Notification Laws*, *supra* note 8; Maxfield & Latham *supra* note 8, at 30.

[11] *What is Personally Identifiable Information (PII)?*, NORTON LIFELOCK, https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html [https://perma.cc/2QGG-YPQ6]; *see State Data Breach Notification Laws*, *supra* note 8.

[12] RISK BASED SEC., INC., *supra* note 3, at 9; *What Is a Data Breach*, KASPERSKY (2019), https://usa.kaspersky.com/resource-center/definitions/data-breach [https://perma.cc/J55Y-H785].

[13] RISK BASED SEC., INC., *supra* note 3, at 9.

[14] IBM SECURITY, COST OF A DATA BREACH REPORT 2019 at 30 https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.249958785.687410232.1571437539- 250560343.1569949773&_gac=1.16575106.1571437539.EAIaIQobChMI_rqhgO2m5QIVQpyzCh2yBw32EAAYASAAEgLZ9fD_BwE (accessed Oct. 19, 2019) [https://perma.cc/R2N6-SUBA]; Larry Ponemon, *What's New in the 2019 Cost of a Data Breach Report,* SECURITYINTELLIGENCE (Jul. 23, 2019), https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report [https://perma.cc/GV7T-2MJA].

preventable.[15] Illustrative examples include failing to fix known vulnerabilities, mistakenly emailing the wrong person sensitive information, and unintentionally storing information on a public database.[16] Often, data breaches like these result from something as simple as a school administrator accidentally publishing student medical records on the school's intranet.[17]

B. Data Breaches from System Glitches

System glitches resulting in data breaches, or "breaches caused by technology failure," are the result of purely system issues and are not directly connected to the actions of individuals.[18] Examples of system glitches resulting in data breaches include "application failures, inadvertent data dumps, [and] logic errors in data transfer."[19] The data breach of First American Financial Corporation's insurance records, one of the largest so far in 2019, is a recent example of a system glitch that caused a data breach.[20] Early this year, a real estate developer was given links to documents that he had legitimate access to on the company website, but by switching one digit in the link, he was suddenly able to access millions of sensitive private records containing social security numbers and bank account information.[21] Once notified of the incident, First American concluded that a "technological defect" had caused the data breach.[22] It is estimated this data breach exposed 885 million records.[23]

[15] Ponemon, *supra* note 14; *Top 3 Causes of Data Breach Are Expensive*, CALYPTIX SEC. (Jun. 29, 2017), https://www.calyptix.com/top-threats/top-3-causes-data-breach-expensive [https://perma.cc/WF4U-XXH8].

[16] *Top 3 Causes of Data Breach Are Expensive*, *supra* note 15.

[17] Australian Associated Press, *Melbourne Student Health Records Posted Online in "Appalling" Privacy Breach*, GUARDIAN (Aug. 21, 2018, 8:47 PM), https://www.theguardian.com/australia-news/2018/aug/22/melbourne-student-health-records-posted-online-in-appalling-privacy-breach [https://perma.cc/WQ5U-57VM].

[18] Ponemon, *supra* note 15.

[19] Thor Olavsrud, *Most Data Breaches Caused by Human Error, System Glitches,* CSO (Jun. 17, 2013, 7:00 AM), https://www.csoonline.com/article/2133631/most-data-breaches-caused-by-human-error--system-glitches.html [https://perma.cc/7GBA-DVW9].

[20] *Frequently Asked Questions,* FIRST AM. FIN. CORP. (May 31, 2019), https://www.firstam.com/incidentupdate/update20190531.html [https://perma.cc/D8NZ-RNLD]; Brian Krebs, *First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records,* KREBS ON SECURITY (May 24, 2019), https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/ [https://perma.cc/8T4N-GDAR].

[21] Krebs, *supra* note 20.

[22] *Frequently Asked Questions*, *supra* note 20.

[23] Krebs, *supra* note 20.

C. Malicious or Criminal Data Breaches

Malicious and criminal attacks were the most common form of data breaches in fiscal year 2019 and are on the rise.[24] While cybercriminals are constantly trying to develop new methods to stay ahead of data security, it may be useful to understand some of the most prevalent techniques currently in use.[25] Some strategies used in malicious and criminal attacks are malware infections, hacking, and social engineering.[26]

1. *Malware Infections*

Malware is a compound word referring to "malicious software" and is an umbrella term for any type of software designed to infiltrate a computer without the owner's permission.[27] Twenty-eight percent of data breaches in 2018 involved malware installation.[28] Some of the most used techniques to install malware are email attachments, direct installations (where further malware is installed after the device is already compromised), and web drive-bys (where the user visits a compromised website that downloads malicious files onto the user's computer).[29] Different types of malware are often used simultaneously and in conjunction with one another.[30]

[24] IBM SECURITY*, supra* note 14, at 6, 21.

[25] IDENTITY THEFT RESOURCE CTR., 2018 END-OF-YEAR DATA BREACH REPORT 5 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf [https://perma.cc/9GFV-ALNH]; EXPERIAN, DATA BREACH INDUSTRY FORECAST 2 (2019) https://www.experian.com/assets/data-breach/white-papers/2019-experian-data-breach-industry-forecast.pdf [https://perma.cc/SHZ7-2WGJ].

[26] VERIZON, 2018 DATA BREACH INVESTIGATIONS REPORT 7 (2018), https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf [https://perma.cc/D2PT-7KPD].

[27] *The Playpen Cases: Frequently Asked Questions,* ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whatismalware (accessed Oct. 20, 2019) [https://perma.cc/YGX7-HHS3]; *Threat Actions,* VERIS, http://veriscommunity.net/actions.html (accessed Oct. 20, 2019) [https://perma.cc/9C2E-5X93].

[28] VERIZON, 2019 DATA BREACH INVESTIGATIONS REPORT 5 (2019) https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf [https://perma.cc/R5F9-NFBD].

[29] *Id.*at 12; *Drive- by Download*, TREND MICRO (2019), https://www.trendmicro.com/vinfo/us/security/definition/drive-by-download [https://perma.cc/9EP8-GCZT]; *What Is a Drive-By Download?*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/drive-by-download [https://perma.cc/3FUB-PW3S].

[30] *Threat Actions*, *supra* note 27.

Some of the most prevalent malware activities used in recent data breaches are the use of backdoors, spyware, and RAM scrapers.[31] A computer "backdoor" is designed to create an alternative access point, or "backdoor," around computer security measures, allowing actors unauthorized access to data and can be exploited via either malware or hacking.[32] These backdoors are designed to circumvent security in a number of ways and allow actors to access and move files undetected and acquire user passwords.[33] A RAM scraper is malware that is designed to steal credit or debit card data while it is stored in the random access memory (RAM) of a point-of-sale terminal.[34] Once installed, the RAM scraper malware collects the card numbers in a readable text file which the malicious actor has access to.[35] Spyware is software that is installed in the computer and monitors user activity, sending the information back to the malicious actor.[36] The software records information such as the user's surfing behavior and goes unnoticed by the computer's owner.[37] Using information found by monitoring the user, the malicious actor is able to gain access to data on the computer.[38]

[31] VERIZON, *supra* note 28, at 12.

[32] VERIZON, *supra* note 28, at 67; *Backdoor*, MALWAREBYTES, https://www.malwarebytes.com/backdoor/ (accessed Oct. 20, 2019) [https://perma.cc/UKB9-YR3P]; Devin Coldewey, *WTF is a Backdoor?*, TECHCRUNCH (Jan. 29, 2017), https://techcrunch.com/2017/01/29/wtf-is-a-backdoor/ [https://perma.cc/MQ5B-EGH6].

[33] DOVE CHIU, SHIH-HAO WENG, & JOSEPH CHIU, TREND MICRO, BACKDOOR USE IN TARGETED ATTACKS (2014), https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-backdoor-use-in-targeted-attacks.pdf [https://perma.cc/YU9A-TTWZ]; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-361, IT SUPPLY CHAIN: NATIONAL SECURITY-RELATED AGENCIES NEED TO BETTER ADDRESS RISKS (2012), http://www.gao.gov/assets/590/589568.pdf [https://perma.cc/AL24-945Z]; *Backdoor, supra* note 32.

[34] David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 959 (2016); Brian Riley, *Ram Scraper Malware: Why PCI DSS Can't Fix Retail*, DARK READING (Jul. 23, 2014), https://www.darkreading.com/attacks-breaches/ram-scraper-malware-why-pci-dss-cant-fix-retail/a/d-id/1297501 [https://perma.cc/67D3-LJKS].

[35] Numaan Huq, *A Look at Point of Sale RAM Scraper Malware and How it Works*, SOPHOS (July 16, 2013), https://nakedsecurity.sophos.com/2013/07/16/a-look-at-point-of-sale-ram-scraper-malware-and-how-it-works/ [https://perma.cc/ED7M-76FY].

[36] *What is Spyware?—Definition*, KASPERSKY, https://usa.kaspersky.com/resource-center/threats/spyware (accessed Oct. 19, 2019) [https://perma.cc/VV7Q-8JV6].

[37] Stephen Y. Chow, *Conceptions of Privacy and Security in a Digital World*, *in* DATA SECURITY AND PRIVACY IN MASSACHUSETTS § 1.2.2(a) (2018).

[38] *What is Spyware*, supra note 36.

2. *Hacking*

Hacking refers to deliberate actions taken to access information by avoiding logical security mechanisms (including passwords and two-factor authentication).[39] This is distinct from malware, where the attack focuses on the downloading or use of malicious software.[40] Hacking techniques were used in fifty-two percent of data breaches in 2018.[41] There are a plethora of activities that fall under the hacking umbrella but three of the more often used strategies are brute force attacks, RFI hacks, and SQL injections.[42] A brute force attack is conceptually straight-forward. A malicious actor wants to gain access into a database or an encrypted file that is protected behind a username and password.[43] The actor utilizes computer programs to run an attack that tries out every combination of, for example, username and password and runs through them as long as it takes until the key is found.[44] An RFI, or "remote file inclusion," attack is when a malicious actor inserts language in a website's URL to redirect a website's request for a remote file to be used on the website to a malicious file.[45] Instead of connecting with the intended file, the website connects and runs the malicious file, and depending on what the file is meant to do, can allow the attacker to gain access to the website's server and the data contained therein.[46] A Structured Query Language (SQL) Injection is an injection of SQL statements within user inputs to gain access to a database.[47] SQL is a coding language that is used in managing databases of information.[48] Often to access this database, a user is asked for a username and password

[39] *Threat Actions*, *supra* note 27; Ernest Sampera, *What You Need to Know About Logical Security vs Physical Security*, VXCHNGE, (Jan. 30, 2019), https://www.vxchnge.com/blog/logical-security-vs-physical-security [https://perma.cc/2K2Y-SUNE].

[40] *See The Playpen Cases: Frequently Asked Questions*, *supra* note 27; *Threat Actions*, supra note 27.

[41] VERIZON, *supra* note 28, at 5.

[42] VERIZON, *supra* note 28, 10.

[43] Chris Hoffman, *Brute Force Attacks Explained: How All Encryption is Vulnerable*, HOW-TO-GEEK (Jul. 6, 2013), https://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/ [https://perma.cc/9V3W-9EVQ].

[44] *Id.*; Jeff Peters, *What is a Brute Force Attack*, VARONIS (Oct. 16, 2018), https://www.varonis.com/blog/brute-force-attack/ [https://perma.cc/P3BA-TE58].

[45] *Remote File Inclusion (RFI)*, CWATCH (Feb. 4, 2019) https://cwatch.comodo.com/blog/cyber-attack/remote-file-inclusion-rfi/ [https://perma.cc/RXQ9-YW9D].

[46] *Id.*

[47] *What is SQL Injection (SQLi) and How to Prevent It,* ACUNETIX https://ww.acunetix.com/websitesecurity/sql-injection (accessed Nov. 20, 2019) [https://perma.cc/32TQ-V4BU].

[48] *Understanding SQL Injection,* CISCO SECURITY, https://tools.cisco.com/security/center/resources/sql_injection (accessed Nov. 20, 2019) [https://perma.cc/7N8A-9GE4].

(user inputs).[49] The malicious actor inserts user inputs that are coded in the SQL that the database server reads as a correct input and allows the malicious user access without guessing the username or password.[50]

3. *Social Engineering*

Social engineering utilizes "deception, manipulation, or intimidation" to manipulate humans into providing access to sensitive data. The most prevalent types are phishing and pretexting.[51] Social engineering was a component in thirty-three percent of data breaches in 2018.[52]

Phishing is a technique where nefarious actors send a designated recipient an email or text message that looks like it is sent from a trusted source.[53] They will then direct you to click on a link or open an attachment.[54] Once the recipient clicks on the link, often either malware is downloaded or a website pops up asking the user to submit sensitive information, which will unknowingly be given to nefarious actors.[55] Pretexting is a more targeted form of phishing where a cybercriminal attempts to create a dialogue with a designated target.[56] An example of pretexting would be if a cybercriminal sent an email to a company employee pretending to be the CEO of the company.[57] The cybercriminal would ask for sensitive information pretending to be the CEO with the aim of getting the employee to provide information that the cybercriminal would otherwise not have access to.[58]

III. WHY MALICIOUS ACTORS CONDUCT DATA BREACHES

There are a number of reasons why an individual or group or organization would conduct a data breach. However, the two most common

[49] *What is SQL Injection (SQLi) and How to Prevent It*, *supra* note 47.

[50] *SQL Injection*, HACKSPLAINING, https://www.hacksplaining.com/exercises/sql-injection#/hack-complete (accessed Nov. 20, 2019) [https://perma.cc/K6X7-NTTJ].

[51] *Threat Actions*, *supra* note 27.

[52] VERIZON, *supra* note 28, at 5.

[53] Fed. Trade Comm'n, *How to Recognize and Avoid Phishing Scams,* FTC: CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Oct. 19, 2019) [https://perma.cc/C98U-RGGJ].

[54] *Id.*

[55] Mark Bassingthwaighte, *Cybercrime and Social Engineering*, 61 ADVOCATE 42, 42 (2018); *Phishing vs Spear Phishing,* BARRACUDA NETWORKS, INC., https://www.barracuda.com/glossary/phishing-spear-phishing (accessed Oct. 19, 2019) [https://perma.cc/Z69R-KLLE].

[56] VERIZON, *supra* note 26, at 11.

[57] *Id.*

[58] *Id.*

motivations of data breaches are financial gain and espionage.[59] These two motivations are believed to make up the vast majority of data breaches.[60]

A. Financial Gain

Often, hackers and cybercriminals will conduct data breaches for the sole purpose of financial gain. In fact, well over fifty percent of data breaches from 2010 to 2016 were for financial gain.[61] Cybercriminals can profit off of data breaches through both goods (the stolen data itself) and services (conducting attacks that result in data breaches), both of which can be bought and sold on the online black market.[62] On the black market earlier this year, the value of an individual Facebook account was $9.12 and the value of individual debit card information was $250.05.[63] Further, the market for a specific piece of data can vary depending on its potential access to new sources of data, especially if the data may be used to unlock other accounts.[64] These purchases of goods and services may be completed with traditional currency but are increasingly conducted using cryptocurrencies as both a source of security and anonymity for the parties involved.[65]

B. Espionage

The second most common motivation behind data breaches is espionage.[66] These are conducted to gain insight into either company trade secrets or to spy into a country's classified information.[67] State-affiliated groups and countries are behind ninety-six percent of espionage motivated

[59] COUNCIL OF ECON. ADVISERS, EXEC. OFFICE OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 6 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/5DFW-MK68].

[60] VERIZON, *supra* note 26, at 6, 7.

[61] *Top 3 Causes of Data Breach Are Expensive*, *supra* note 15.

[62] Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Monetization of Stolen Data*, RAND CORP. (Mar. 15, 2018) https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf [https://perma.cc/26A6-FY8F].

[63] *Id.*, Simon Migliano, *Dark Web Market Price Index-2019 (US Edition)*, TOP10VPN.COM (Feb. 20, 2019), https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-us-edition/ [https://perma.cc/ZSM4-G5T6].

[64] Ablon, *supra* note 62.

[65] *Id.*

[66] VERIZON, *supra* note 26, at 6.

[67] NAT'L COUNTERINTELLIGENCE AND SEC. CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE (2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf [https://perma.cc/ZH92-NY6Y]; Ablon, *supra* note 62.

breaches.[68] Phishing and backdoors were used in a high number of cyber-espionage incidents.[69] Attacks conducted by state-sponsored actors are unique in that they are conducted on behalf of a nation's interest and are widely considered "legitimate state activity."[70] A number of data breaches over the past few years have come to the front of public conversation due to state-sponsored subversion and espionage, with prominent examples being the North Korean attack on Sony Entertainment in response to the release of the movie *The Interview* and the United States Democratic National Committee breach in 2016.[71]

IV. CONCLUSION

Data breaches are a constant threat to information kept on computer systems and all sectors and industries within our society are targeted. The breaches occur in a number of ways ranging from innocent human mistakes to malicious and complex malware infections or hacking. When these breaches are deliberate, they are often conducted for financial gain or espionage purposes. The legal community is increasingly asked to respond to the persistent threat of data breaches. Understanding the problem of how data breaches happen and what the motivations are behind them is a baseline for informed decision-making to combat this threat in all aspects of our society.

[68] VERIZON, *supra* note 28, at 25.

[69] *Id.*

[70] Ablon, *supra* note 62.

[71] Ablon, *supra* note 62; SYMANTEC, INTERNET SECURITY THREAT REPORT: VOLUME 22 at 7, 44(2017), https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [https://perma.cc/4HAD-3QLL].