The Heritage Foundation

ISSUE BRIEF

No. 4803 | JANUARY 3, 2018

Private Sector Cyber Incidents in 2017

Riley Walters

This *Issue Brief* is a continuation of a series of papers on cyber incidents involving U.S. companies since 2014.[1] The private sector continues to be plagued by cyber incidents ranging from systems hacking to poor practices that leave companies' information exposed. In the U.S. alone, the financial loss from cybercrimes exceeded $1.3 billion in 2016. Per the Federal Bureau of Investigation, the most prevalent and types of attacks are data breaches, malicious e-mails, and forms of extortion.[2]

This list does not represent even a majority of known breaches to the private sector. Incidents are listed below are in chronological order by the date the incident is released to the public.

December 2016[3]

Dailymotion (online media). Breach notification service LeakedSource found 85 million usernames, e-mail addresses, and passwords from the online media player.[4] The data was compromised as early as October 2016.

Community Health Plan of Washington (health care). A data breach exposed the social security numbers and personal information of 380,000 current and former members of the health insurance nonprofit.[5]

This paper, in its entirety, can be found at
http://report.heritage.org/ib4803

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

January 2017

E-Sport Entertainment Association (entertainment). A hacker exposed 1.5 million usernames, birthdates, and contact information from the online gaming association after E-Sports refused to pay ransom.[6]

Popeyes Louisiana Kitchen (restaurant chain). The point of sale system of 10 CCC restaurants, doing business as Popeyes, were infected with malware between May and August 2016.[7] The malware collected information on credit and debit cards used at those locations.

February 2017

ISO Forum (entertainment). This forum for Xbox and PlayStation gamers was breached in 2015, exposing 2.5 million users.[8] Hackers reportedly compromised e-mails, passwords, and IP addresses.

Arby's (restaurant chain). The point of sale system at hundreds of Arby's restaurants was breached as early as January 2017.[9] Credit and debit card information was compromised.

March 2017

Commonwealth Health Corporation (health care). A former employee compromised the personal information of as many as 697,000 customers of Commonwealth Health's Med Center Health between 2014 and 2015.[10]

River City Media (e-mail marketing). 1.34 billion e-mails, names, and IP addresses stored on River City Media's database was exposed as early as January 2017.[11] The unsecure data was found by Chris Vickery, a "data breach hunter."[12]

Dun and Bradstreet (business services). 34 million e-mail addresses and other corporate contact information was exposed.[13]

April 2017

InterContinental Hotels Group (hotel chain). The point of sale system at over 1,000 InterContinental locations was compromised as early as December 2016.[14] InterContinental, which is parent company to hotels like Holiday Inn, first acknowledged a breach in February 2017, but only to 12 of its properties. Credit card information was compromised.

Schooolzilla (data analytics). Information on 1.3 million K–12 students was compromised, including names, addresses, birthdates, test scores, and some social security numbers.[15]

May 2017

Google Docs (online word processor). Nearly 1 million Gmail users may have been the target of a phishing e-mail attack in the form of a Google Document.[16]

Sabre Corporation (technology company). Hackers were able to gain credentials to Sabre's SynXis reservation system and gain access to customer data.[17] SynXis handles bookings for 35,000 hotels.

[1] Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation *Issue Brief* No. 4289, October 27, 2014, http://www.heritage.org/defense/report/cyber-attacks-us-companies-2014; Riley Walters, "Cyber Attacks on U.S. Companies Since November 2014," Heritage Foundation *Issue Brief* No. 4487, November 18, 2015, http://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014; and Riley Walters, "Cyber Attacks on U.S. Companies in 2016," Heritage Foundation *Issue Brief* No. 4636, December 2, 2016, http://www.heritage.org/defense/report/cyber-attacks-us-companies-2016.

[2] Federal Bureau of Investigation, *2016 Internet Crime Report*, https://pdf.ic3.gov/2016_IC3Report.pdf (accessed January 2, 2018).

[3] The previous paper in this series examined events up to November 2016. Thus, while this *Issue Brief* focuses on cyber incidents that occurred in 2017, these events from December 2016 are included to ensure no gaps exist in the research on the issue of cyber incidents in the private sector.

[4] Steve Ragan, "85 Million Accounts Exposed in Dailymotion Hack," CSO, December 5, 2016, https://www.csoonline.com/article/3147424/security/85-million-accounts-exposed-in-dailymotion-hack.html (accessed January 2, 2018).

[5] Bob Young, "Data Breach Exposes Info for 400,000 Community Health Plan Members," *Seattle Times*, December 21, 2016, https://www.seattletimes.com/seattle-news/health/data-breach-exposes-info-for-400000-community-health-plan-members/ (accessed January 2, 2018).

[6] Steve Ragan, "ESEA Hacked, 1.5 Million Records Leaked After Alleged Failed Extortion Attempt," CSO, January 8, 2017, https://www.csoonline.com/article/3155397/security/esea-hacked-1-5-million-records-leaked-after-alleged-failed-extortion-attempt.html (accessed January 2, 2018).

[7] News release, "CCC Restaurant Enterprises, LLC—Notice of Data Security Incident," *PRNewswire*, January 18, 2017, https://www.prnewswire.com/news-releases/ccc-restaurant-enterprises-llc---notice-of-data-security-incident-300392999.html (accessed January 2, 2018).

[8] Robert Abel, "2.5 Million XBOX 360 and PSP ISO Forum Accounts Breached," SC Media, January 31, 2017, https://www.scmagazine.com/xbox-and-psp-forum-accounts-breached/article/635024/ (accessed January 2, 2018).

[9] Brian Krebs, "Fast Food Chain Arby's Acknowledges Breach," Krebs on Security, February 17, 2017, https://krebsonsecurity.com/2017/02/fast-food-chain-arbys-acknowledges-breach/ (accessed January 2, 2018).

[10] Marianne Kolbasuk McGee, "Breach Involving Encrypted Devices Raises Questions," Information Security Media Group, March 23, 2017, https://www.careersinfosecurity.com/breach-involving-encrypted-devices-raises-questions-a-9789 (accessed January 2, 2018).

[11] Jonathan Vanian, "Major Spammer Accidentally Leaks Data on a Billion People," *Fortune*, March 6, 2017, http://fortune.com/2017/03/06/spammer-leaks-data/ (accessed January 2, 2018).

[12] Zack Whittaker, "Meet Chris Vickery, the Internet's Data Breacher Hunter," ZDNet, April 26, 2017, http://www.zdnet.com/article/chris-vickery-data-breach-hunter/ (accessed January 2, 2018).

[13] Zack Whittaker, "Millions of Records Leaked from Huge US Corporate Database," ZDNet, March 15, 2017, http://www.zdnet.com/article/millions-of-records-leaked-from-huge-corporate-database/ (accessed January 2, 2018).

[14] Brian Krebs, "Intercontinental Hotel Chain Breach Expands," Krebs on Security, April 17, 2017, https://krebsonsecurity.com/2017/04/intercontinental-hotel-chain-breach-expands/ (accessed January 2, 2018).

[15] Robert Abel, "Data of 1.3 Million Schoolzilla Students Exposed," SCMedia, April 21, 2017, https://www.scmagazine.com/schoolzilla-breach-exposed-13m-students/article/652067/ (accessed January 2, 2018).

[16] Selena Larson, "Major Phishing Attack Targeted Google Docs Users," CNN, May 4, 2017, http://money.cnn.com/2017/05/03/technology/google-docs-phishing-attack/index.html (accessed January 2, 2018).

[17] Lee Matthews, "Travel Giant Sabre Confirms Its Reservation System Was Hacked," *Forbes*, July 6, 2017, https://www.forbes.com/sites/leemathews/2017/07/06/travel-giant-sabre-confirms-its-reservation-system-was-hacked/#188d13e84b20 (accessed January 2, 2018).

June 2017

The Buckle Inc. (retain chain). The point of sale system at Buckle, with more than 450 stores in the U.S., was compromised between October 2016 and April 2017.[18] Credit and debit card information was compromised.

Republican National Committee (political organization). 198 million voters' information managed by the contractor Deep Root Analytics was compromised.[19] Chris Vickery again discovered the unsecured data.

8tracks Radio (online radio). 18 million users' e-mail addresses and passwords were compromised.[20]

July 2017

Verizon (online storage). Third-party contractor NICE Systems exposed 6 million users' names, addresses, account details, and PIN numbers.[21]

Dow Jones (financial services). 2.2 million users' names, e-mail address, and some financial data was potentially exposed.[22]

Home Box Office (entertainment). The entertainment company has experienced a series of breaches in 2017 that include the theft of proprietary information and the leaking of popular shows like Game of Thrones before their intended airdate.[23]

Women's Health Care Group (health care). Hackers may have begun accessing the systems of the health care service as early as January 2017.[24] The personal information of 300,000 patients may have been compromised.

August 2017

Pacific Alliance Medical Center (health care). A ransomware attack in June potentially compromised the health information of 266,000 patients.[25]

September 2017

Equifax (credit agency). A breach between May and July compromised the personal information of 143 million Americans.[26] Compromised information included names, addresses, some driver's license numbers, birthdates, and social security numbers. The breach also compromised the credit card information of about 200,000 people and personal information of residents in both the United Kingdom and Canada.

Sonic (restaurant chain). The point of sale systems at Sonic, which has over 3,600 locations, were compromised.[27] Malware targeted the systems to gather customers' credit card information.

October 2017

Yahoo Inc. (online). All of Yahoo's 3 billion accounts were compromised in an August 2013

[18] Brian Krebs, "Credit Card Breach at Buckle Stores," Krebs on Security, June 17, 2017, https://krebsonsecurity.com/2017/06/credit-card-breach-at-buckle-stores/ (accessed January 2, 2018).

[19] Joe Uchill, "Data on 198M Voters Exposed by GOP Contractor," *The Hill*, June 19, 2017, http://thehill.com/policy/cybersecurity/338383-data-on-198-million-us-voters-left-exposed-to-the-internet-by-rnc-data (accessed January 2, 2018).

[20] Teri Robinson, "8tracks Breach Yields Data on 18M accounts," SCMedia, June 29, 2017, https://www.scmagazine.com/8tracks-breach-yields-data-on-18m-accounts/article/672233/ (accessed January 2, 2018).

[21] Dan O'Sullivan, "Verizon Partner Exposed Millions of Customer Accounts," UpGuard, November 28, 2017, https://www.upguard.com/breaches/verizon-cloud-leak (accessed January 2, 2018).

[22] Morgan Chalfant, "Dow Jones Customer Data Exposed in Cloud Error," *The Hill*, July 17, 2017, http://thehill.com/policy/cybersecurity/342333-dow-jones-customer-data-exposed-in-cloud-error (accessed January 2, 2018).

[23] Brian Barrett, "Breaking Down HBO's Brutal Month of Hacks," *Wired*, August 18, 2017, https://www.wired.com/story/hbo-hacks-game-of-thrones/ (accessed January 2, 2018).

[24] Harold Brubaker, "Data Breach at Philly-area Ob/Gyn Practice Among This Year's Largest Nationally," *The Inquirer*, August 12, 2017, http://www.philly.com/philly/business/pharma/data-breach-at-philly-area-obgyn-practice-among-this-years-largest-nationally-20170812.html (accessed January 2, 2018).

[25] Jessica Davis, "Los Angeles Provider Breached by Ransomware Attack, over 260,000 Patients Affected," *Healthcare IT News*, August 14, 2017, http://www.healthcareitnews.com/news/los-angeles-provider-breached-ransomware-attack-over-260000-patients-affected-updated (accessed January 2, 2018).

[26] Seena Gressin, "The Equifax Data Breach: What to Do," Federal Trade Commission, September 8, 2017, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do (accessed January 2, 2018).

[27] Brian Krebs, "Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards," Kreb On Security, September 17, 2017, https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/ (accessed January 2, 2018).

breach.[28] This is a significant increase from the December 2016 announcement that only 1 billion accounts had been compromised. Compromised information included usernames, passwords, phone numbers, birthdates, and security questions and answers.

Hyatt (hotel chain). The point of sale system at 41 Hyatt-managed properties across 11 countries was breached between March and July 2017.[29] Credit card information was compromised.

November 2017

Fasten (transportation). 1 million users' names, e-mail addresses, phone numbers, and drivers' information were compromised as early as October 2017.[30]

Uber (transportation). Information from 57 million driver and rider accounts was compromised in late 2016.[31] Hackers were able to access around 600,000 names and driver's license numbers.

December 2017

PayPal Holdings Inc. (online financing). 1.6 million users' personal information may have been compromised in early 2017 after potential security vulnerabilities were found in PayPal's TIO network systems.[32] Information may include names, addresses, back-account details, and social security numbers.

Incentives Matter

Monetary gain from collecting information on credit cards or from selling person information remain constant targets for hackers. The large amount of personal information accessible online, including from unsecure databases, is used by hackers for any number of malicious activities—especially phishing e-mail attacks. Employees clicking on a bad e-mail remain a constant weak point for businesses trying to secure their networks.

Policymakers and law enforcement agencies should keep three points in mind for strengthening cybersecurity.

- **Everyone gets hacked.** All companies should consistently invest in their cybersecurity. This includes teaching employees good cyber hygiene. No one is 100 percent safe from hackers, but that does not excuse poor cybersecurity.

- **Learning from others' experiences.** When one restaurant chain reports an attack on its point of sale system, other restaurants should consider checking the security of their point of sale systems. If a company's services mostly rely on the Internet, it should have a greater investment in cybersecurity than its brick-and-mortar competitor.

- **Importance of third-party security analysts.** A number of these failures were found by security analysts doing their civic duty of protecting consumers' information. Companies should seek outside analysis when developing their cybersecurity policies.

Conclusion

While the Department of Justice and FBI do a good job at hunting down malicious cyber aggressors, Congress needs to have a serious debate over how it can enable private companies to better secure their networks with active cyber defense.

*—**Riley Walters** is a Research Associate in the Asian Studies Center, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

[28] Lily Hay Newman, "Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts," *Wired*, October 3, 2017, https://www.wired.com/story/yahoo-breach-three-billion-accounts/ (accessed January 2, 2018).

[29] "Hyatt Hotels Discovers Card Data Breach at 41 Properties," Reuters, October 12, 2017, https://www.reuters.com/article/us-hyatt-hotels-cyber/hyatt-hotels-discovers-card-data-breach-at-41-properties-idUSKBN1CH2WP (accessed January 2, 2018).

[30] Dell Cameron, "Ride-Hailing Service Prominent at SXSW Briefly Exposed Data on as Many as 1 Million Customers," Gizmodo, November 10, 2017, https://gizmodo.com/ride-hailing-service-prominent-at-sxsw-briefly-exposed-1820335380 (accessed January 2, 2018).

[31] Mike Isaac, Katie Benner, and Sheera Frenkel, "Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data," *The New York Times*, November 21, 2017, https://www.nytimes.com/2017/11/21/technology/uber-hack.html?_r=0 (accessed January 2, 2018).

[32] Peter Rudegair, "PayPal Says Personal Data May Be Compromised for 1.6 Million TIO Users," *The Wall Street Journal*, December 1, 2017, https://www.wsj.com/articles/paypal-says-personal-data-may-be-compromised-for-1-6-million-tio-users-1512170657 (accessed January 2, 2018).