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.\(^5\)

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.

Schoolzilla (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.


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.


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. 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. Chris Vickery again discovered the unsecured data.

**8tracks Radio (online radio).** 18 million users’ e-mail addresses and passwords were compromised.

July 2017

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

**Dow Jones (financial services).** 2.2 million users’ names, e-mail address, and some financial data was potentially exposed.

**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.

**Women's Health Care Group (health care).** Hackers may have begun accessing the systems of the health care service as early as January 2017. 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.

September 2017

**Equifax (credit agency).** A breach between May and July compromised the personal information of 143 million Americans. 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. 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 breach.
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. 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.

**Uber (transportation).** Information from 57 million driver and rider accounts was compromised in late 2016. 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. 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.