The Heritage Foundation

ISSUE BRIEF

No. 4289 | OCTOBER 27, 2014

Cyber Attacks on U.S. Companies in 2014

Riley Walters

The spate of recent data breaches at big-name companies such as JPMorgan Chase, Home Depot, and Target raises questions about the effectiveness of the private sector's information security. According to FBI Director James Comey, "There are two kinds of big companies in the United States. There are those who've been hacked...and those who don't know they've been hacked."[1]

A recent survey by the Ponemon Institute showed the average cost of cyber crime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 million per company in 2014.[2] The annual average cost per company of successful cyber attacks increased to $20.8 million in financial services, $14.5 million in the technology sector, and $12.7 million in communications industries.

This paper lists known cyber attacks on private U.S. companies since the beginning of 2014. (A companion paper discussed cyber breaches in the federal government.)[3] By its very nature, a list of this sort is incomplete. The scope of many attacks is not fully known. For example, in July, the U.S. Computer Emergency Readiness Team issued an advisory that more than 1,000 U.S. businesses have been affected by the Backoff malware, which targets point-of-sale (POS) systems used by most retail industries.[4] These attacks targeted administrative and customer data and, in some cases, financial data.

This list includes only cyber attacks that have been made known to the public. Most companies encounter multiple cyber attacks every day, many unknown to the public and many unknown to the companies themselves.

The data breaches below are listed chronologically by month of public notice.

January

- **Target (retail).** In January, Target announced an additional 70 million individuals' contact information was taken during the December 2013 breach, in which 40 million customer's credit and debit card information was stolen.[5]

- **Neiman Marcus (retail).** Between July and October 2013, the credit card information of 350,000 individuals was stolen, and more than 9,000 of the credit cards have been used fraudulently since the attack.[6] Sophisticated code written by the hackers allowed them to move through company computers, undetected by company employees for months.

- **Michaels (retail).** Between May 2013 and January 2014, the payment cards of 2.6 million Michaels customers were affected.[7] Attackers targeted the Michaels POS system to gain access to their systems.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4289

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.

- **Yahoo! Mail (communications).** The e-mail service for 273 million users was reportedly hacked in January, although the specific number of accounts affected was not released.[8]

April

- **Aaron Brothers (retail).** The credit and debit card information for roughly 400,000 customers of Aaron Brothers, a subsidiary of Michaels, was compromised by the same POS system malware.[9]

- **AT&T (communications).** For two weeks AT&T was hacked from the inside by personnel who accessed user information, including social security information.[10]

May

- **eBay (retail).** Cyber attacks in late February and early March led to the compromise of eBay employee log-ins, allowing access to the contact and log-in information for 233 million eBay customers.[11] eBay issued a statement asking all users to change their passwords.

- **Five Chinese hackers indicted.** Five Chinese nationals were indicted for computer hacking and economic espionage of U.S. companies between 2006 and 2014. The targeted companies included Westinghouse Electric (energy and utilities), U.S. subsidiaries of SolarWorld AG (industrial), United States Steel (industrial), Allegheny Technologies (technology), United Steel Workers Union (services), and Alcoa (industrial).[12]

1. James Cook, "FBI Director: China Has Hacked Every Big US Company," *Business Insider*, October 6, 2014, http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 (accessed October 10, 2014).
2. Ponemon Institute, "2014 Cost of Cyber Crime Study: United States," Hewlett-Packard, October 9, 2014, https://ssl.www8.hp.com/us/en/ssl/leadgen/document_download.html?objid=4AA5-5208ENW (accessed October 24, 2014).
3. For a list of federal cyber breaches, see David Inserra and Paul Rosenzweig, "Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation," Heritage Foundation *Issue Brief* No. 4288, October 27, 2014, http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.
4. U.S. Department of Homeland Security, Computer Emergency Readiness Team, "Backoff Point-of-Sale Malware," July 31, 2014, https://www.us-cert.gov/ncas/alerts/TA14-212A (accessed October 10, 2014).
5. News release, "Target Provides Update on Data Breach and Financial Performance," Target, January 10, 2014, http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance (accessed October 10, 2014).
6. Benjamin Elgin, Dune Lawrence, and Michael Riley, "Neiman Marcus Hackers Set Off 60,000 Alerts with Card Thefts," Bloomberg, February 21, 2014, http://www.bloomberg.com/news/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-in-bagging-card-data.html (accessed October 9, 2014).
7. Chuck Rubin, "A Letter from Our CEO," Michaels Stores, Inc., April 17, 2014, http://www.michaels.com/payment-card-notice-ceo-letter/payment-card-notice-CEO.html (accessed October 9, 2014).
8. Hayley Tsukayama, "Yahoo Mail Hacked: What to Do If You've Been Affected," *The Washington Post*, January 31, 2014, http://www.washingtonpost.com/business/technology/yahoo-mail-hacked-what-to-do-if-youve-been-affected/2014/01/31/2857ef8a-8a7d-11e3-833c-33098f9e5267_story.html (accessed October 14, 2014).
9. News release, "Michaels Identifies and Contains Previously Announced Data Security Issue," Michaels Stores, April 17, 2014, http://demandware.edgesuite.net/aaeo_prd/on/demandware.static/Sites-MichaelsUS-Site/Sites-MichaelsUS-Library/default/v1412927934297/docs/press-releases/Michaels-FINAL-Press-Release-041714.pdf (accessed October 10, 2014).
10. Dave Smith, "AT&T Was Hacked in April and Some Customers Had Their Social Security Numbers Stolen," *Business Insider*, June 16, 2014, http://www.businessinsider.com/att-hacked-2014-6 (accessed October 14, 2014).
11. News release, "eBay Inc. to Ask eBay Users to Change Passwords," eBay, May 21, 2014, http://www.ebayinc.com/in_the_news/story/ebay-inc-ask-ebay-users-change-passwords (accessed October 10, 2014).
12. News release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (accessed October 9, 2014).

- **Unnamed public works (energy and utilities).** According to the Department of Homeland Security, an unnamed public utility's control systems were accessed by hackers through a brute-force attack[13] on employee's log-in passwords.[14]

June

- **Feedly (communications).** Feedly's 15 million users were temporarily affected by three distributed denial-of-service attacks.[15]

- **Evernote (technology).** In the same week as the Feedly cyber attack, Evernote and its 100 million users faced a similar denial-of-service attack.[16]

- **P.F. Chang's China Bistro (restaurant).** Between September 2013 and June 2014, credit and debit card information from 33 P.F. Chang's restaurants was compromised and reportedly sold online.[17]

August

- **U.S. Investigations Services (services).** U.S. Investigations Services, a subcontractor for federal employee background checks, suffered a data breach in August, which led to the theft of employee personnel information.[18] Although no specific origin of attack was reported, the company believes the attack was state-sponsored.

- **Community Health Services (health care).** At Community Health Service (CHS), the personal data for 4.5 million patients were compromised between April and June.[19] CHS warns that any patient who visited any of its 206 hospital locations over the past five years may have had his or her data compromised. The sophisticated malware used in the attack reportedly originated in China. The FBI warns that other health care firms may also have been attacked.

- **UPS (services).** Between January and August, customer information from more than 60 UPS stores was compromised, including financial data,[20] reportedly as a result of the Backoff malware attacks.

- **Defense Industries (defense).** Su Bin, a 49-year-old Chinese national, was indicted for hacking defense companies such as Boeing.[21] Between 2009 and 2013, Bin reportedly worked with two other hackers in an attempt to steal manufacturing plans for defense programs, such as the F-35 and F-22 fighter jets.

13. A brute-force attack involves repeatedly guessing a password.
14. Jim Finkle, "U.S. Utility's Control System Was Hacked, Says Homeland Security," Reuters, May 20, 2014, http://www.reuters.com/article/2014/05/21/us-usa-cybercrime-infrastructure-idUSBREA4J10D20140521 (accessed October 14, 2014).
15. Oliv, Seb, and Edwin, "Denial of Service Attack [Neutralized]," Feedly, June 11, 2014, http://blog.feedly.com/2014/06/11/denial-of-service-attack/ (accessed October 10, 2014).
16. Leo Kelion, "Feedly and Evernote Struck by Denial of Service Cyber-Attacks," BBC News, June 11, 2014, http://www.bbc.com/news/technology-27790068 (accessed October 14, 2014).
17. News release, P.F. Chang's, August 4, 2014, http://pfchangs.com/security/ (accessed October 10, 2014).
18. News release, "USIS Comments on Recent Self-Reported Cyber-Attack on Corporate Network," US Investigations Services, August 6, 2014, http://www.usis.com/Media-Release-Detail.aspx?dpid=151 (accessed October 10, 2014).
19. Jose Pagliery, "Hospital Network Hacked, 4.5 Million Records Stolen," CNN Money, August 18, 2014, http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/ (accessed October 10, 2014).
20. Hannah Kuchler, "UPS Hit by Cyber Attack," *Financial Times*, August 21, 2014, http://www.ft.com/intl/cms/s/0/fb206340-28be-11e4-8bda-00144feabdc0.html (accessed October 14, 2014).
21. News release, "Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Allegedly Involving Theft of Trade Secrets," Federal Bureau of Investigation, Los Angeles Division, August 15, 2014, http://www.fbi.gov/losangeles/press-releases/2014/los-angeles-grand-jury-indicts-chinese-national-in-computer-hacking-scheme-allegedly-involving-theft-of-trade-secrets (accessed October 10, 2014).

September

- **Home Depot (retail).** Cyber criminals reportedly used malware to compromise the credit card information for roughly 56 million shoppers in Home Depot's 2,000 U.S. and Canadian outlets.[22]

- **Google (communications).** Reportedly, 5 million Gmail usernames and passwords were compromised.[23] About 100,000 were released on a Russian forum site.

- **Apple iCloud (technology).** Hackers reportedly used passwords hacked with brute-force tactics and third-party applications to access Apple user's online data storage, leading to the subsequent posting of celebrities' private photos online.[24] It is uncertain whether users or Apple were at fault for the attack.

- **Goodwill Industries International (retail).** Between February 2013 and August 2014, information for roughly 868,000 credit and debit cards was reportedly stolen from 330 Goodwill stores.[25] Malware infected the chain store through infected third-party vendors.

- **SuperValu (retail).** SuperValu was attacked between June and July, and suffered another malware attack between late August and September.[26] The first theft included customer and payment card information from some of its Cub Foods, Farm Fresh, Shop 'n Save, and Shoppers stores. The second attack reportedly involved only payment card data.

- **Bartell Hotels (hotel).** The information for up to 55,000 customers was reportedly stolen between February and May.[27]

- **U.S. Transportation Command contractors (transportation).** A Senate report revealed that networks of the U.S. Transportation Command's contractors were successfully breached 50 times between June 2012 and May 2013.[28] At least 20 of the breaches were attributed to attacks originating from China.

October

- **J.P. Morgan Chase (financial).** An attack in June was not noticed until August.[29] The contact information for 76 million households and 7 million small businesses was compromised. The hackers may have originated in Russia and may have ties to the Russian government.

- **Dairy Queen International (restaurant).** Credit and debit card information from 395 Dairy Queen and Orange Julius stores was compromised by the Backoff malware.[30]

22. Press release, "The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores," Home Depot, September 18, 2014, https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf (accessed October 10, 2014).
23. Alexis Kleinman, "5 Million Gmail Usernames and Associated Passwords Leaked," *The Huffington Post*, September 11, 2014, http://www.huffingtonpost.com/2014/09/11/gmail-passwords-hacked_n_5805104.html (accessed October 14, 2014).
24. Steve Kovach, "We Still Don't Have Assurance from Apple That iCloud Is Safe," *Business Insider*, September 2, 2014, http://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9 (accessed October 14, 2014).
25. Charlene Sarmiento, "Goodwill Provides Update on Data Security Issue," Goodwill Industries International, http://www.goodwill.org/press-releases/goodwill-provides-update-on-data-security-issue/ (accessed October 14, 2014).
26. Martyn Williams, "Second Cyberattack Hits SuperValu Grocery Stores' Payment Systems," *PCWorld*, September 29, 2014, http://www.pcworld.com/article/2689372/second-cyberattack-hits-supervalu-grocery-stores-payment-systems.html (accessed October 10, 2014).
27. Mike Freeman, "Cyber Attack Hits San Diego Hotel Chain," *San Diego Union-Tribune*, September 9, 2014, http://www.utsandiego.com/news/2014/sep/09/target-home-depot-bartell-hotels-cyber-hacking/ (accessed October 10, 2014).
28. U.S. Senate, Committee on Armed Services, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors*, 2014, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf (accessed October 9, 2014).
29. Emily Glazer, "J.P. Morgan's Cyber Attack: How the Bank Responded," *The Wall Street Journal*, October 3, 2014, http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/ (accessed October 9, 2014).
30. News release, "International Dairy Queen Confirms Malware Intrusion at Some U.S. Locations," American Dairy Queen Corporation, October 9, 2014, http://www.dq.com/datasecurityincident/press-release/ (accessed October 10, 2014).

- **Snapsave (communications).** Reportedly, the photos of 200,000 users were hacked from Snapsave, a third-party app for saving photos from Snapchat, an instant photo-sharing app.[31]

Securing Information

As cyber attacks on retail, technology, and industrial companies increase so does the importance of cybersecurity. From brute-force attacks on networks to malware compromising credit card information to disgruntled employees sabotaging their companies' networks from the inside, companies and their customers need to secure their data. To improve the private sector's ability to defend itself, Congress should:

- **Create a safe legal environment for sharing information**. As the leaders of technological growth, private companies are in most ways at the forefront of cyber security. Much like government agencies, companies must share information that concerns cyber threats and attack among themselves and with appropriate private-public organizations.[32] Congress needs to create a safe environment in which companies can voluntarily share information without fear of legal or regulatory backlash.

- **Work with international partners**. As with the Backoff malware attacks, attacks can affect hundreds if not thousands of individual networks. These infected networks can then infect companies outside the U.S. and vice versa. U.S. and foreign companies and governments need to work together to increase overall cybersecurity and to enable action against individual cyber criminals and known state-sponsored cyber aggressors.[33]

- **Encourage cyber insurance.** Successful cyber attacks are inevitable because no security is perfect. With the number of breaches growing daily, a cybersecurity insurance market is developing to mitigate the cost of breaches. Congress and the Administration should encourage the proper allocation of liability and the establishment of a cyber insurance system to mitigate faulty cyber practices and human error.[34]

Conclusion

The recent increases in the rate and the severity of cyber attacks on U.S. companies indicate a clear threat to businesses and customers. As businesses come to terms with the increasing threat of hackers, instituting the right policies is critical to harnessing the power of the private sector. In a cyber environment with ever-changing risks and threats, the government needs to do more to support the private sector in establishing sound cybersecurity while not creating regulations that hinder businesses more than help them.

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

31. Alexis Kleinman, "200,000 Snapchat Photos Leaked on 4Chan," *The Huffington Post*, October 10, 2014, http://www.huffingtonpost.com/2014/10/10/snapchat-leak_n_5965590.html (accessed October 10, 2014).
32. Paul Rosenzweig and David Inserra, "Government Cyber Failures Reveal Weaknesses of Regulatory Approach to Cybersecurity," Heritage Foundation *Issue Brief* No. 3968, June 12, 2013, http://www.heritage.org/research/reports/2013/06/weaknesses-of-a-regulatory-approach-to-cybersecurity (accessed October 14, 2014).
33. Steven P. Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1, 2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.
34. Ibid.