Data Breach Events

and the US Population

Second Edition, July 20, 2015
First Edition, February 19, 2015

About The Copper River Group

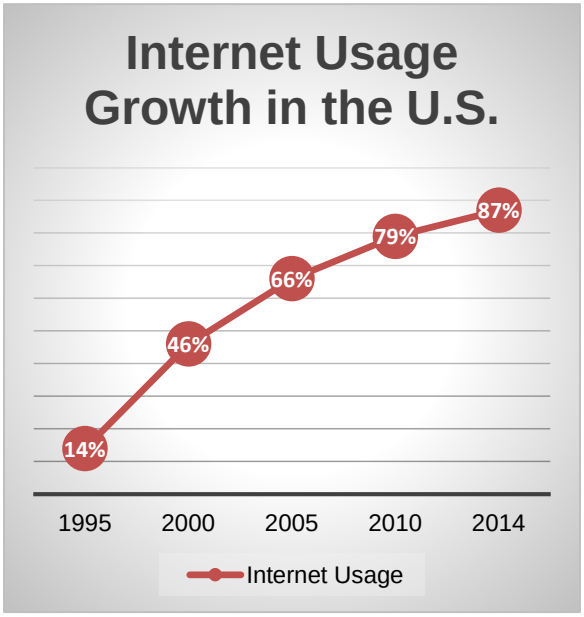
10 years and still going strong—The Copper River Group offers experience when you need it now.

The Copper River Group offers the experience and knowledge you're seeking to take your organization to the next level. The Copper River Group provides consulting and research services for independent community financial institutions. Our expertise is in vendor contract negotiations, regulatory compliance, and technology strategies.

The Copper River Group was established in 2005 in Fargo, ND. The company started with the mission to offer consulting services to community financial institutions. Since its inception, the Copper River Group has experienced a tremendous amount of growth. We provide services to financial institutions across the United States, and have worked internationally with banks in Canada and Ecuador.

Introduction

During the 21 month period between November 2013 and July 2015, 81% of the U.S. population became victims of data breaches. More importantly, few tasks in the lives of Americans remain free of technology, computers, and the Internet.



Movies and TV shows are streamed through Netflix, books can be downloaded from the internet and arrive instantly on devices such as Nook and Kindle, children use the internet to conduct research for school, and consumers conduct bank transactions on smartphones. It is an anytime, anywhere, technology driven environment. Today, 84% of US households own a computer, whether that includes a desktop, laptop, tablet, or smartphone, and 73% have a connection to the internet.[1] Since 1995 when the European Organization for Nuclear Research (CERN) released it to the public, internet usage has increased from 14% of American adults to 87% in 2014. In 2000, 53% of American adults owned a cell phone, up to 90% in 2014, and smartphone ownership is up from 35% in 2011 to 53% in 2014.[2]

Businesses rely heavily on the internet to accomplish everything from processing their customers' payments to communicating with co-workers and sending information. Among people who said it would be difficult to give up the internet, 61% said it was important because their job relied on it.[3] The internet is

[1] Lee Rainie. "Census: Computer Ownership, internet connection varies widely across US," *Pew Research Center,* last modified September 19, 2014, accessed February 19, 2015, http://www.pewresearch.org/fact-tank/2014/09/19/census-computer-ownership-internet-connection-varies-widely-across-u-s/.
[2] Susannah Fox "The Web at 25 in the US," .*Pew Research Center*, last modified February 27, 2014, accessed February 19, 2015, http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/.
[3] Susannah Fox. "The Web at 25 in the US," *Pew Research Center,* last modified February 27, 2014, accessed February 19, 2015, http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/.

important to successfully operate point-of-sale (POS) and cash register systems, store digital information, and for websites and online stores. Software capable of tracking the efficiency of each department give managers a far more substantial and detailed view of their business.[4] The internet allows businesses to extend their reach from local to global. The internet is used to share, transport and access large amounts of data, and that data grows in volume every day.

Data is not stored in a single place, but in a multitude of different facilities around the world. Massive organizations such as Facebook or Google have their own enormous data storage sites, whereas smaller organizations hire hosting services from a third party.[5] Data storage centers such as Facebook's are composed of thousands of servers which look like giant computer towers composed of racks containing hard disks, and each one is connected and awaits internet users to request the information they hold.[6] These data storage facilities claim to be completely secure surrounded by security doors, surveillance cameras, and fire-retardant materials, as well as top of the line cyber security software to keep hackers out. Unfortunately, over the past few years an increasing amount of cyber criminals have been finding their way in.

Hackers most often gain unauthorized access to a network by simply cracking the password. Others dig up security weaknesses such as configuration errors or bugs. Sometimes hackers send out phishing e-mails in an attempt to discover login credentials and easily infiltrate the network. Some hackers, such as former employees who feel slighted, perform inside jobs on the companies they used to work for. After the hacker gains access, he can move across the network and install malicious software, called malware, or steal confidential information, and sometimes the victim does not even know it.[7] Consumers may believe that their sensitive information, such as credit card numbers or social security numbers, remains safe behind the firewalls, but recent data breaches prove retailers and other businesses

[4] Osmond Vitez. "The Effect of the Internet on Modern Businesses and Corporations," *Houston Chronicle*, accessed February 19, 2015, http://smallbusiness.chron.com/effect-internet-modern-businesses-corporations-896.html.
[5] David Frankk. "Where is all the data on the Internet stored?" *Examiner*, last modified March 19, 2013, accessed February 19, 2015, http://www.examiner.com/article/where-is-all-the-data-on-the-internet-stored.
[6] Jordon Novet. "First Look: Facebook's Oregon Cold Storage Facility," *Data Center Knowledge*, last modified October 16, 2013, accessed February 19, 2015, http://www.datacenterknowledge.com/archives/2013/10/16/first-look-facebooks-oregon-cold-storage-facility/.
[7] Margaret Rouse. "Advanced Persistent Threat (APT) Definition," *TechTarget,* accessed January 28, 2015, http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

neglect their cyber security when upgrading their technology may have prevented the exposure of millions of confidential records and the loss of billions of dollars.

As cyber criminals become more advanced, the U.S. falls behind in cyber security, making U.S. businesses an easy target and the consumers whose information they claim to protect readily available to any hacker willing to ferret out an organization's security shortcomings. Going forward, any organization conducting business via the internet can expect to experience a major data breach jeopardizing their reputation and the confidential information of their customers if they do not significantly strengthen defenses, actively monitor their network environment, encrypt and compartmentalize their databases, and always remain prepared for an attack.

Data Breach Events and the US Population

In 2007 cyber breaches became a serious issue in the eyes of U.S. financial institutions, retailers, and consumers with the enormous attack on TJX Companies Inc., which includes stores such as TJMaxx, HomeGoods, and Marshalls. The breach exposed over 100 million records. Further investigation revealed hackers most likely infiltrated their network in July of 2005, and repeatedly returned to the network for 17 months before the company noticed abnormal activity. TJX stores admitted not using upgraded cyber security programs, as well as storing unencrypted credit and debit card information on local servers. A 26 year old college dropout and former IT consultant for the U.S. government named Albert Gonzalez spearheaded the attacks.

Heartland Payment Systems, a company dedicated to processing card payment transactions, discovered an intrusion into their systems in January 2009. Authorities once again found Albert Gonzalez and his conspirators guilty of the crime. The hackers claimed over 130 million confidential records by using techniques that take advantage of weak server configurations, and the cleanup cost Heartland $134.9 million.[8]

These attacks alerted U.S. industries of the danger to the private sector posed by cyber criminals, but nearly six years after those first incidents, businesses still fail to properly protect their customers' confidential data. Despite new security technology, many retailers neglect to upgrade their current cyber security systems and leave their networks vulnerable to new forms of malware. Most do not realize their mistake until hackers find weaknesses exposed by outdated security programs or lax controls and the company's data is breached.

Over the past 21 months, 20 major data breaches affected consumers in the US. These breaches included large retailers such as Target, Nieman Marcus, Home Depot, Michael's craft stores, Goodwill Industries, and Staples. Hackers targeted banks such as JP Morgan Chase, Total Bank, and Bank of the West. Restaurants including Dairy Queen, P.F. Chang's, and, most recently, Chik-Fil-A, fell victim to data thieves.[9] No industry is immune from cyber criminals. These 20 data breaches exposed at least 256,931,326 people's confidential records, or 81% of the U.S.'s

[8] Privacy Rights Clearinghouse. "Chronology of Data Breaches," accessed February 4, 2015, https://www.privacyrights.org/.
[9] Privacy Rights Clearinghouse. "Chronology of Data Breaches," accessed January 27, 2015, https://www.privacyrights.org/.

population.[10] The last 21 months amount to approximately 30% of the total number of records breached since 2005.The number does not reflect companies who claimed an 'unknown' number of personal records leaked into criminals' hands.

One of the largest and most frightening data breaches involved Anthem, a large health insurance company, where hackers infiltrated their database and stole the records of possibly tens of millions of their customers, including personal information such as Social Security numbers, addresses, phone numbers, e-mail addresses, and dates of birth. Anthem announced the breach on February 4, 2015, and they claimed they became aware of the breach on January 29, 2015.[11] Although the exact number of compromised records is unknown, the hackers infected a database that contains over 80 million records of customers and employees. The hackers did not expose any financial records, but Social Security numbers, names, and birth dates sell for more than credit and debit card information on the black market because criminals can use them to create fake identities.[12]

For retailers, the number one weakness cyber criminals prey upon is their POS systems. Hackers dig deep to uncover fatal holes, called zero-day vulnerabilities, in companies' networks. These holes are unknown to companies and vendors, and when discovered they must rush to patch them before hackers can intrude.[13] Cyber thieves also employ a method of entry called 'spear phishing' in which they send out malicious e-mails that look trustworthy in the hopes that an employee of their targeted company will open it and create a door for the hackers. Once entry is gained, hackers will move across the network creating multiple 'back doors' which allow continued access. Hackers can steal high-security user credentials which allow them to develop a 'ghost infrastructure' and bogus 'utilities.' The hacker can then install malicious malware onto a retailer's POS system and steal confidential information every time customers swipe their cards.[14]

---

[10] United States Census Bureau. "US and World Population Clock," last modified January 30, 2015, accessed January 30, 2015, http://www.census.gov/popclock/.
[11] Brian Krebs. "Data Breach at Health Insurer Anthem Could Impact Millions," *KrebsonSecurity*, last modified February 4, 2015, accessed February 5, 2015, https://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/.
[12] Reed Abelson. "Anthem Health Insurer said Cyberattack Stole Data of Millions," *The New York Times*, last modified February 5, 2015, accessed February 5, 2015, http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html.
[13] PCTools by Symantec. "What is a Zero Day Vulnerability?" accessed January 27, 2015, http://www.pctools.com/security-news/zero-day-vulnerability/.
[14] Margaret Rouse. "Advanced Persistent Threat (APT) Definition," *TechTarget*, accessed January 28, 2015, http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.

These hacks can become so complex that cyber criminals must employ a full-time administrator to continually rewrite code and deploy evasion programs. Although hard to detect, these hackers, dubbed Advanced Persistent Threats or APTs, are not invisible. Companies must remain vigilant in identifying abnormal activity within their networks if they wish to keep their customers' data safe from hackers. Updating security systems frequently is a necessity, but some companies learn the importance of cyber security too late.

Many companies assume a reactive rather than a proactive stance in their cyber security departments. After the hack attack that exposed 56 million of Home Depot's customers' confidential records, the home improvement store claimed that their assailants used a new, custom built type of malware to expose their data. Hitesh Sheth, the CEO of the cyber security firm Vectra Networks, said, "This essentially means the technology they are using is only designed to detect malware that has already been used in a previous attack, and that is symptomatic of the retail industry. Retailers need to upgrade to technology that is available and detects behavior of malware that is new because these attacks are not going to stop anytime soon."[15] If companies continue to place their cyber security on the back burner they are potentially placing themselves at a higher risk for a major data breach.

In the recent Anthem attack, the investigation uncovered that the company did not encrypt data stored within its computer network, although they encrypted the data they exported.[16] The FBI even warned members of the health industry on August 20, 2014 that cyber criminals wished to target them for personally identifiable information (PII), and told them earlier in April of 2014 that their cyber security systems were far below the standards of other industries.[17] Anthem claimed they became the victim of a 'very sophisticated' attack, but after two warnings from the FBI their actions can only be perceived as gross negligence of their customers' sensitive information.

In the U.S., companies prove slow to adopt a more secure type of debit and credit card called an EMV. This card uses a chip and pin system to make it more

---

[15] Jim Finkle and Nandita Bose. "Home Depot Breach Bigger than Target at 56 million cards," *Reuters*, last modified September 18, 2014, accessed February 2, 2015, http://www.reuters.com/article/2014/09/18/us-home-depot-dataprotection-idUSKBN0HD2J420140918.

[16] Reed Ableson and Matthew Goldstein. "Anthem Hacking Points to Security Vulnerability in Health Care Industry," *The New York Times,* last modified February 5, 2015, accessed February 17, 2015, http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html.

[17] Jim Finkle. "FBI warns healthcare firms they are targeted by hackers," *Reuters,* last modified August 20, 2014, accessed February 15, 2015, http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

difficult for criminals to steal confidential financial data. Without special POS terminals, however, the enhanced security of the EMV card is useless, and converting costs money that many companies seem to not want to spend. Card distributors such as Visa, MasterCard, American Express, and Discover offer incentives to banks to issue chip and pin cards, and by 2015-2017 retailers and banks who have not switched to EMV cards will be responsible for fraudulent charges.[18] Unfortunately, it seems that many retailers see the benefits of switching to upgraded security technology as lucrative only after experiencing the horror of a major data breach.

No matter how advanced a company's security, hackers become more advanced as well, and data breaches can still occur. A company's data breach response plan can make a significant difference in the amount of moral and fiscal damage. When news of Target's major data breach caught people's ears, customers swamped the company's call centers, flooded their website, and caused their customer service systems to crash. Angry customers blamed Target for purposefully closing their call centers in order to evade the problem. Although Target released information about how customers could protect themselves against fraudulent card activity, the closeness of the holiday season made many reluctant to freeze credit and checking accounts. One customer complained on Target's Facebook page that she would 'shred' her REDCard so hackers couldn't use it, indicating a lack of knowledge on how the breach had taken place.[19] Studies of social media websites showed that 34% of customers criticized Target for slow response times and blamed them for the breach, and consumer opinion made a complete turn-around from 95% positive to 95% negative.[20] Even worse, news of the data breach first appeared on the *Krebs on Security* website a week before Target officially announced anything, which proved a poorly executed effort due to the unobvious placement of the important information.[21] Target lost millions of dollars in sales, a senior executive, and the trust of their customers because of the data breach. With a plan in place to

[18] Becky Krystal. "The basics of chip-and-pin credit cards," *The Washington Post*, last modified May 16, 2013, accessed January 29, 2015, http://www.washingtonpost.com/lifestyle/travel/the-basics-of-chip-and-pin-credit-cards/2013/05/16/9e8bdf9a-a13f-11e2-be47-b44febada3a8_story.html.
[19] Loss of Privacy. "Some Thoughts on the Target Breach," last modified December 29, 2013, accessed January 28, 2015, http://www.lossofprivacy.com/index.php/2013/12/some-thoughts-on-the-target-breach/.
[20] Kirsten Jepson. "What Bank Contact Centers Can Learn from the Target Data Breach," *Sykes*, accessed January 30, 2015, http://www.sykes.com/bank-contact-centers-can-learn-target-data-breach/.
[21] Karen Chu "The Right (and Wrong) Way to Respond to a Data Breach," *Bitium*, last modified August 21, 2014, accessed February 2, 2015, http://blog.bitium.com/the-right-and-wrong-way-to-respond-to-a-data-breach-and-hack.

guide the company in the event of a security breach situation, damages may have been contained and Target would have retained a positive image in the perspectives of their customers.

When a cyberattack exposed the data of millions of Anthem's customers and employees, the health insurance company immediately set up a special website and hotline to field the questions of their concerned customers. They also assured their customers they would set up free credit monitoring and identity repair services for those affected by the breach. Although not required to report the data breach for almost a month after they first learned of it, Anthem chose to call in Mandiant, a cybersecurity firm, less than a week after they became aware of the attack. FBI spokesman Joshua Campbell applauded Anthem for alerting authorities to the matter saying, "Anthem's initial response in promptly notifying the F.B.I. after observing suspicious network activity is a model for other companies and organizations facing similar circumstances."[22] Anthem's actions prove a response plan is feasible in the event of a data breach, and their business and customers will benefit from their decisiveness and rapid reaction.

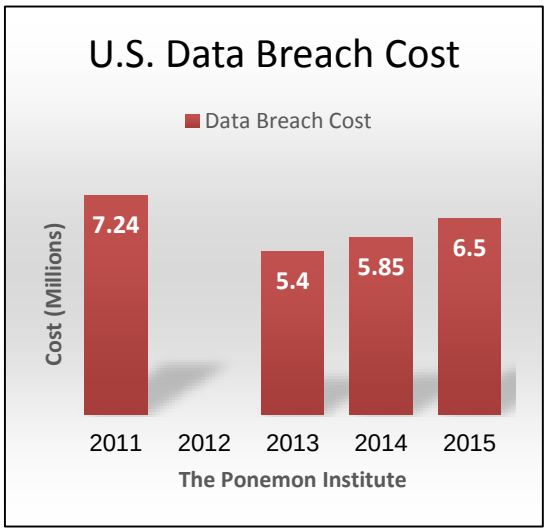
After the string of major data breaches, more companies adopted data breach response plans. In 2013, 61% of companies claimed they had plans in place, and it jumped to 73% in 2014. Still, 41% of these companies admitted they don't periodically review their plan, and 49% said they don't train their personnel on how to answer sensitive questions fielded by customers in the event of a data breach. 68% of companies in the study said they would not know how to deal with negative customer opinion if they were the victim of a data breach, and 67% said they would not know the proper steps to take.[23] Companies need to take a more proactive role in their cyber security by upgrading their technology and practicing their data breach response plans to minimize fiscal and moral damages.

Slow discovery and response to data breaches can also have a significant effect on damages incurred because of stolen information. The longer a company is vulnerable to hackers, the more information can be stolen. URM stores experience data breaches between September and October of 2013, but did not disclose the information until November 26, 2013. Target's data breaches began November 27

[22] Reed Abelson. "Anthem Health Insurer said Cyberattack Stole Data of Millions," *The New York Times*, last modified February 5, 2015, accessed February 5, 2015, http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html.
[23] Ponemon Institute, LLC. "Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness," last modified September 2014, accessed February 2, 2015, http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

and their network was not secure until December 15, 2013, which allowed 110 million confidential records to be exposed. JP Morgan Chase admitted they had a data breach on December 5, 2013, but their network was vulnerable since July of that same year, nearly a five month window! On January 10, 2014 Neiman Marcus disclosed information about their data breach which likely started in July 2013. P.F. Chang's data was possibly compromised for 8 months before the breach was discovered.[24] In most cases, it is credit card companies and banks who alert retailers of a data breach by tracing the purchases of compromised cards back to one common retailer, which is typically the point of infection. Retailers should be able to root out this malware themselves before credit card companies and banks notice a major problem. Each day a hacker is allowed to chip away at a company's cyber defenses, the deeper he can imbed himself in their network, the more 'back doors' he can build, and the more information he can steal.

Data breaches not only affect the victimized company, but they have economic repercussions that ripple down to small banks and their customers. No matter how small, data breaches affect everyone. The United Retail Merchants breach in November of 2013 cost 11 small credit unions $687,598, $491,835 of which was fraudulent charges and $195,763 to replace the compromised cards.[25] In the Target breach financial institutions paid out $200 million just to replace compromised cards, which does not include the price of fraudulent charges, another sum which banks and credit unions would have to pay.[26] The cost is especially high for small banks and credit unions because they pay a much higher price to reissue cards. Small banks spend $11 to reissue a debit card and $12.75 for a credit card, as opposed to $2.70 for a debit card and $2.99 for a credit card for larger banks. Small banks and credit unions



[24] Privacy Rights Clearinghouse. "Chronology of Data Breaches," accessed January 27, 2015, https://www.privacyrights.org/.
[25] Tom Sowa. "URM Stores card fraud tops $687,000 for 11 credit unions," *The Spokesman Review*,last modified March 4, 2014, accessed January 29, 2015, http://www.spokesman.com/stories/2014/mar/04/urm-stores-card-fraud-cost-tops-687000-for-11/.
[26] Saabira Chaudhuri. "Cost of Replacing Cards After Target Breach Estimated at $200 Million," *The Wall Street Journal*, last modified February 18, 2014, accessed February 2, 2015, http://www.wsj.com/articles/SB10001424052702304675504579391080333769014.

spent $90 million in reissuance fees after the Home Depot breach alone. For each data breach, financial institutions can spend between $66,000 and $938,000 depending on their size.[27] Financial institutions must begin to offer chip-and-pin cards to their customers, and also push retailers to adopt EMV compatible POS terminals. Currently, financial institutions assume most of the cost of fraudulently used credit and debit cards and literally pay for a retailer's poor security choices. Retailers and financial institutions must work together to ensure the safety of their customer's confidential records.

Hackers don't attack just retailers, they also target government agencies. Governments often support these highly skilled criminals who infiltrate top security networks in search of classified information. The U.S. recognizes China as one of the top cyber espionage threats. A group called APT1 stole confidential information from 141 industries throughout the U.S. Mandiant, a cybersecurity firm, tracked the perpetrators back to China's Army Headquarters.[28] Russia's sponsored hacker group is called APT28 and has been targeting confidential information from governments, militaries, and security organizations since at least 2007.[29]

The Syrian Electronic Army arose in 2011 when Syria's civil war broke out. They support President Bashar al-Assad in Syria. This group is based out of Syria's universities, and financial statements indicate that the corrupted government supports them. The Syrian Electronic Army typically attacks the U.S. media and people linked to foreign governments and militaries. In 2014, they hijacked the Associated Press's Twitter account and claimed two explosions at the White House injured President Obama. Within a mere 90 seconds the Dow Jones index lost more than 1% of its value.[30] This group is not particularly advanced compared to other cybercrime organizations, but the immediate and remarkable effect of commandeering one Twitter account reveals the profound impact a dedicated,

---

[27] David McMillin. "Small banks pay up for data breaches," *Bankrate*, last modified December 22, 2014, accessed February 2, 2015, http://www.bankrate.com/financing/banking/small-banks-pay-up-for-data-breaches/.
[28] John Ginovsky. "Cybersecurity. See something. Say something. Really," *Banking Exchange*, last modified February 25, 2013, accessed January 28, 2015, http://www.bankingexchange.com/blogs-3/making-sense-of-it-all/item/128-making-sense-of-it-all-cybersecurity-see-something-say-something-really.
[29] FireEye. "APT28: A Window into Russia's Cyber Espionage Operations?" last modified October 27, 2014, accessed January 28, 2015, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.
[30] Emily Chung. "Syrian Electronic Army Hackers: Who are they and why are they targeting the media?" *CBSNews*, last modified December 1, 2014, accessed January 28, 2015, http://www.cbc.ca/news/technology/syrian-electronic-army-hackers-who-are-they-and-why-are-they-targeting-the-media-1.2852694.

malicious group of hackers could unleash on the U.S. should they grasp control of a number of media websites and post false stories.

Although North Korea denies it, hackers sponsored by their government are believed to be behind the attacks on Sony after the release of the controversial film *The Interview*. North Korea warned they would take merciless countermeasures if Sony released the movie. The attack exposed five unreleased films and the data of 7,000 global employees, plus information on celebrities' salaries and other confidential information. Most of the country's civilians don't possess access to the internet, but North Korea's elite have a 3G network. They send the best of their hackers to China for additional training.[31]

Ajax Security Team, based in Iran, is the first hacking group in their country to use custom built malicious software. They have possibly used their creations to launch the "denial-of-service" attacks on major U.S. banks over the past few years. After the Stuxnet virus, which many believe originated in the U.S., infected Tehran's nuclear development program in 2010, the Ajax Security Team ramped up their own cyber espionage efforts. The Iranian hackers targeted U.S. defense company networks, too, but evidence they dabbled in credit fraud indicates they are not under the complete control of the Iranian government.[32] These cyber espionage groups pose an outstanding threat to the U.S. government and its financial institutions. Funded by their governments and advancing their technology every day, any company using the internet must pump up their security and remain vigilant to keep these intruders out of sensitive data.

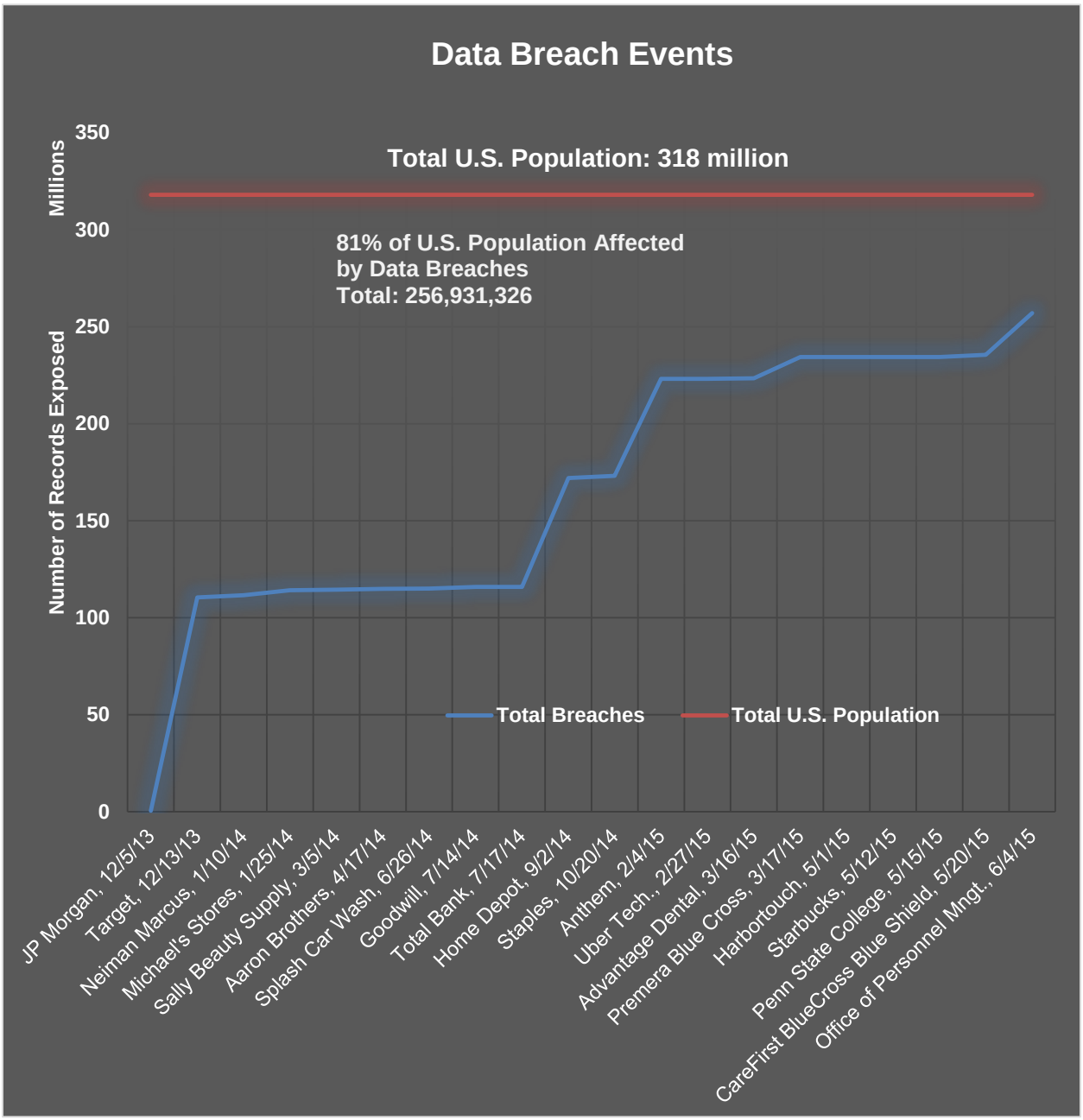
Hack attacks against high profile U.S. industries motivated President Obama to push for tighter cyber security laws in 2015. The proposal stands to improve the method in which the government and the private sector share information about cyber threats. Some people worry that the legislation will reduce their privacy and the government will use it to enhance their surveillance and data collection.[33] As previously stated, credit card companies offered incentives to banks to issue chip and pin cards, and retailers and banks who have not adopted the new technology

[31] Elise Hu. "North Korea's Skills Get Attention Amid Sony Hacking Mystery," *NPR*, last modified December 4, 2014, accessed January 29, 2015, http://www.npr.org/blogs/alltechconsidered/2014/12/04/368449855/north-koreas-cyber-skills-get-attention-amid-sony-hacking-mystery.
[32] Jim Finkle. "Cyber experts warn Iranian hackers becoming more aggressive," *Reuters*, last modified May 13, 2014, accessed January 29, 2015, http://www.reuters.com/article/2014/05/13/us-cyber-summit-iran-hackers-idUSBREA4C03O20140513.
[33] *BBC News*. "Obama makes push for stronger cyber security laws," last modified January 15, 2015, accessed January 28, 2015, http://www.bbc.com/news/world-us-canada-30807463.

between 2015 and 2017 will be responsible for fraudulent charges.

It is clear hackers can infiltrate nearly any network they deem holds lucrative information they can sell on the black market, so consumers must take measures to protect themselves. To ensure their identity is not stolen, consumers can sign up for identity theft protection programs. All financial data should be password protected, and alerts should be placed on any accounts at financial institutions. Corporate, healthcare, or any entity harboring the confidential records of their customers should review their cyber security procedures—and not just once a year—as well as ensure their data is compartmentalized and encrypted.

Cyber criminals take advantage of companies who neglect to beef up their security and upgrade to the newest programs capable of detecting and repelling innovative forms of malware. Each breach delivers a major blow to the U.S. economy and shakes the confidence of millions of consumers. Cybercrime is only increasing, hackers are getting smarter, and to pull ahead of the game the government, retailers, consumers, and financial institutions must band together to protect themselves from this obscure but menacing threat.



[34], [35]

[34] United States Census Bureau. http://www.census.gov/popclock/.
[35] Privacy Rights Clearinghouse. https://www.privacyrights.org/.