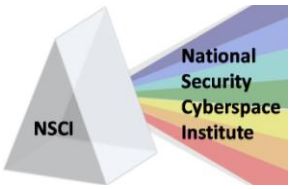

Data Breaches: Ending the Epidemic

Kandice McKee, NSCI
May 4, 2011

Introduction

The vast majority of Americans have sensitive, personal information that could be compromised at any time. While it's in the best interest for institutions that have access to such personal information to keep it private, there are thousands of cases where millions of personal information records haven't been kept secure. From 2005 to April 29, 2011, the Privacy Rights Clearinghouse has documented 2,451 data breaches that have resulted in more than half a billion compromised personal information records.[1]

Because there is no specific federal law concerning data breaches, there is no national standard on what type of data is considered personal information. However, 46 states have some type of legislation concerning data breaches, with variances of what is included as personal information. Most laws have personal information definitions similar to that of California or Arizona legislation. California laws include: "When not encrypted, a person's first name or initial and last name combined with: SSN; driver's license or state ID number; account number, credit or debit card number, combined with any information that allows access to account; or medical information and health insurance information" as personal information. Arizona includes "first name or initial and last name in combination with any one of the following: SSN, driver's license or state ID card number, financial account number, credit or debit card number in combination with any required security or access code that would permit access to an individual's financial account."[2]

As defined by the Government Accountability Office, "the term 'data breach' generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers."[3] To put this definition in perspective, as of July 2010, nearly 460 million SSNs had been issued[4]; the number of credit cardholders projected for 2011 is 183 million owning nearly 1.3 billion cards; and the number of debit cardholders is thought to be even higher at 188 million in 2011, but with a fewer number of cards at just 585 million.[5] Using the GAO's definition, that means there are about 2 billion personally identifiable numbers available – all of which can fall victim to a data breach. The National Security Cyberspace Institute is among many other public and private institutions that believe the likelihood of these personally identifiable numbers becoming compromised is too high.

Data Breach Types and Costs

Data breaches in 2010 cost, on average, $214 per compromised record and $7.2 million per breach – up from $204 per record and $6.8 million per breach in 2009, according to a study conducted by the Ponemon Institute. Twenty percent of institutions in the study experienced their first data breach of more than 1,000 records in 2010. While that figure remained essentially unchanged from 2009's figure, the costs associated with a first-time data breach grew 43 percent to $326 per record. The report gives a

[1] "Chronology of Data Breaches," Privacy Rights Clearinghouse, April 2011, available at http://www.privacyrights.org/data-breach/new

[2] "State Data Security/Breach Notification Laws," Commercial Law League of America, March 2011

[3] "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown," Government Accountability Office, June 2007, available at http://www.gao.gov/new.items/d07737.pdf

[4] "Frequently Asked Questions," Social Security Administration, July 2010, available at http://ssa-custhelp.ssa.gov/app/answers/detail/a_id/387/~/the-number-of-social-security-numbers-issued.

[5] "Banking, Finance, and Insurance," Statistical Abstract of the United States, Tables 1186 and 1187, U.S. Census Bureau, 2011, available at http://www.census.gov/compendia/statab/2011/tables/11s1187.pdf

couple reasons for the higher costs for first time breaches: the lack of data breach experience that would help lower costs and the number of malicious attacks. [6]

Unfortunately for organizations that have access to personal information and those whose data has the potential to be compromised, the number of data breaches that occur due to maliciousness has more than doubled since 2008. According to the Ponemon Institute, malicious attacks accounted for 31 percent of data breaches in 2010 compared to just 12 percent in 2008. "The significant jump in malicious attacks over the past two years is certainly indicative of the worsening threat environment," according to Dr. Larry Ponemon.[7]

A study done by the Identity Theft Resource Center mimics the Ponemon Institute's malicious attack findings. In the ITRC study, nearly one-third of data breaches in 2010 resulted from maliciousness – 17.1 percent from hackers and 15.4 percent from insider theft. However, in the ITRC study, 38.5 percent of the data breaches didn't identify what type of data breach occurred, so the figure of malicious attacks could actually be higher. [8]

According to the ITRC's 2010 data breach study, 16.1 million records were reported breached and about 76 percent included SSNs and 29 percent included credit or debit card numbers (only about half of the reported breaches included what type of data had been compromised). In its 2011 year-to-date study, which concluded April 5, ITRC noted that 130 data breaches had already occurred. Hackers are to blame for almost 37 percent of these breaches and another 16 percent were due to insider theft.[9] With malicious attacks being the most commonly reported type of breach in the ITRC studies, it's likely that the majority of the breached SSNs and financial account numbers were criminally obtained. [10]

"Carders" are often to blame for the malicious attacks that involve stealing financial information. Carders use methods such as hacking and phishing to fraudulently obtain credit card, debit card, bank account numbers, and other types of personal information. This activity is known as carding and "merchants and processors who hold individuals' sensitive financial information are prime targets for hackers and carders."[11] Such sensitive, personal information is then redistributed for a profit on carding forums. According to a report published by the Santa Clara Computer and High Technology Journal, "The types of information for sale on carding forums has evolved from the sale of a few pieces of sensitive information, such as credit card numbers and expiration dates, to full blown identity packages containing multiple types of sensitive personal information." The more invasive the information, the more profit for the carder, and the more harm to the data's true owner.[12] Because of carding organizations and their internationality, several U.S. government agencies have joined in the fight against data breaches, which will be discussed later in this paper.

---

[6] "2010 Annual Study: U.S. Cost of a Data Breach," Symantec, March 2011, available at http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach (hereinafter "U.S. Cost of a Data Breach")

[7] "Cost of a data breach climbs higher," Dr. Larry Ponemon, March 2011, available at http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher (hereinafter "Cost of a data breach climbs higher")

[8] "Data Breaches in 2010," Identity Theft Resource Center, Jan. 3, 2011, available at http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2010.shtml (hereinafter "Data Breaches in 2010")

[9] "Hackers: Duhhh, Winning," Identity Theft Resource Center, April 21, 2011, available at http://www.idtheftcenter.org/artman2/publish/m_press/Hackers_Duhhh_Winning.shtml

[10] "Data Breaches in 2010"

[11] "Statement of Rita M. Glavin," U.S. Department of Justice, March 2009, p. 6, available at http://www.justice.gov/ola/testimony/111-1/2009-03-31-crm-glavin-payment-card.pdf (hereinafter 'Glavin')

[12] "Data Breaches: What the Underground World of 'Carding" Reveals," Kimberly Kiefer Peretti, Santa Clara Computer and High Technology Journal, Volume 25, 2009, p. 388, available at http://www.chtlj.org/sites/default/files/media/articles/v025/v025.i2.Peretti.pdf (hereinafter 'Peretti')

Even worse for institutions that fall victim to a malicious data breach is the fact that this type of breach is the most expensive. The breach costs associated with malicious attacks have "skyrocketed" 48 percent to an average of $318 per record from Ponemon's study in 2009 to its 2010 version. "The huge increases reinforce the extreme danger hostile breaches pose," according to the Ponemon report.

The largest data breach included in the Ponemon study was 105,000 records, [13] which is about ten times less than the number of records compromised by Heartland Payment Systems, Inc. The breach of an estimated 130 million credit and debit card information records was announced in January 2009 and has stood to be one of the largest in breach history. The company, which said the breach resulted from a malicious malware infestation, had set aside more than $140 million in May 2010 to cover the breach expenses. However, it's estimated that Heartland's breach costs will eventually surpass the $250 million TJX Companies, Inc., has estimated it will spend[14] on the data breach that exposed about 94 million card numbers during an 18-month malicious attack that began in 2005.[15]

Epsilon, a subsidiary marketing and communications firm of Alliance Data Systems, also fell victim to a malicious attack March 30, 2011. During the attack, "thieves gained access to the e-mail addresses and names of partners' customers," but no account or credit card numbers were compromised. Given that, Alliance Data Systems has said it doesn't expect any "meaningful" costs to result from the breach.[16]

Sony likely won't be so lucky, though. The company "suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins" April 17 through April 19. The company made the breach public April 26,[17] and by April 28, the first lawsuit regarding the breach was filed.[18] The short timeframe that these two "massive," malicious data breaches occurred has put a sense of urgency in some U.S. Congressional members, which will be discussed later.

While malicious attacks are on the rise, the Ponemon Institute reported that "companies [are] becoming more conscientious about preventing data breaches in the worsening threat environment." This is indicated by the fall in the number of breaches associated with system failures, lost or stolen devices, and third-party mistakes to 27 percent, 35 percent, and 29 percent, respectively. [19]

Though the number of these types of breaches has fallen, they, too, experienced an increase in costs, according to the Ponemon Institute. Breaches resulting from system failures raised an average of $44 to

[13] "U.S. Cost of a Data Breach"

[14] "Heartland breach expenses pegged at $140M – so far," Jaikumar Vijayan, Computer World, May 10, 2010, available at http://www.computerworld.com/s/article/9176507/Heartland_breach_expenses_pegged_at_140M_so_far (hereinafter "Heartland breach")

[15] "One year later: Five takeaways from the TJX breach," Jaikumar Vijayan, Computer World, Jan. 17, 2008, available at http://www.computerworld.com/s/article/9057758/One_year_later_Five_takeaways_from_the_TJX_breach

[16] "Epsilon pledges to build 'Fort Knox' around breached system," Grant Gross, Computer World, April 21, 2011, available at http://www.computerworld.com/s/article/9216029/Epsilon_pledges_to_build_Fort_Knox_around_breached_system (hereinafter "Epsilon")

[17] "Sony PlayStation suffers massive data breach," Liana B. Baker and Jim Finkle, Reuters, April 26, 2011, available at http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

[18] "Suit charges Sony breach caused by poor security," Jaikumar Vijayan, Computer World, April 28, 2011, available at http://www.computerworld.com/s/article/9216258/Suit_charges_Sony_breach_caused_by_poor_security (hereinafter "Suit charges Sony breach caused by poor security")

[19] "U.S. Cost of a Data Breach"

$210 in 2010; those from lost or stolen devices raised an average of $33 to $258; and data lost due to third-party mistakes raised an average $85 to $302. [20]

The most common data breach threat remains negligence, at 41 percent – a one percent growth from 2009, according to the Ponemon study.[21] Such findings are represented by a different 2009 study in which only 52 percent of business managers were given encryption software by their employers. Of that figure, only about half bothered to use it. Business managers were also more likely to share encryption passwords. Because of this "human factor," organizations must not rely solely on encryption as a means of protection.[22]

The Texas Comptroller's office demonstrated the "human factor" in a data breach that went unrecognized for more than a year. While Texas administrative security policy requires encryption of personal information, unencrypted data of nearly 3.5 million Texas teachers and employees were put on an agency public-access server from January 2010 to May 2010. The breach, which included names, mailing addresses, SSNs, and some birth dates and driver license numbers, went unacknowledged until March 31, 2011. The total costs associated with breach remain unknown while the Attorney General's office conducts an investigation.[23]

Although negligence was the leading cause of data breaches among the Ponemon study, it remained the cheapest to remedy, though its costs did also rise. The costs associated with negligence breaches have raised $42 per record since 2009 to be $196 in 2010.[24]

Effects on the Public-at-Large

What may be most provocative about the costs associated with data breaches is when taxpayer dollars are used to remedy and fix the security lapses. Texans, so far, have paid about $1.8 million after the Texas Comptroller's Office compromised 3.5 million people's personal information.[25] After Veterans' Affairs had its first data breach from a stolen laptop in 2006, taxpayers footed the $48 million notifications-and-lawsuit bill.[26] While there is no statistic on how much taxpayers have paid on data breaches as a whole, take the Texas Comptroller's Office and VA costs and consider that the Privacy Rights Clearinghouse has document 436 data breaches by government institutions since 2005.[27] The figure is likely near a billion.

Because data breaches involve personally identifiable information, for the public-at-large, the most common and harmful crime resulting from the breach is identity theft. For the first time since 2007, identity theft fell in 2010 by 28 percent to 8.1 million adults, according to an independent study by the Javelin Strategy & Research. "One likely contributing factor was the significant drop in reported data breaches according to industry reports," the study's press release said. Another contributing factor was the

---

[20] Ibid.

[21] "Cost of a data breach climbs higher"

[22] "Study: Many Employees Undermine Date Breach Prevention Strategies," Insurance Journal, April 27, 2009, available at http://www.insurancejournal.com/news/national/2009/04/27/99982.htm

[23] "Breach Exposes Data Of 3.5 Million Teachers And Employees In Texas," Tim Wilson, Darkreading, April 11, 2011, available at http://www.darkreading.com/database-security/167901020/security/attacks-breaches/229401384/breach-exposes-data-of-3-5-million-teachers-and-employees-in-texas.html

[24] "U.S. Cost of a Data Breach"

[25] "Poor Data Protection in Texas Costs More than $1.8 Million,"Bob Styran, InAudit, April 27, 2011, available at http://inaudit.com/audit/it-audit/poor-data-protection-in-texas-costs-more-than-1-8-million-5840/

[26] "Another VA Data Breach," Press Release from the House Committee on Veterans' Affairs, May 13, 2010, available at http://veterans.house.gov/news/PRArticle.aspx?NewsID=1933

[27] "Chronology of Data Breaches"

economy. Comparing the 2010 study's results with the results from previous years, the study found that "fraud inversely mirrors retails sales … When retail sales have increased, fraud has decreased, which points to economic hardships as an overall contributor to fraudsters committing identity crimes."[28] The Consumer Sentinel Network Report, put together by the Federal Trade Commission, approximates the Javelin Strategy & Research findings. According to the CSN, while identity theft was the number one complaint of 2010, the number of identity thefts fell for the second straight year.[29]

Despite the fall in the number of identity thefts, the costs to consumers associated with such fraud significantly rose. From 2009 to 2010, the average consumer out-of-pocket costs grew 63 percent to $631 per incident. Consumers should heed the warning of this substantial change in costs, the Javelin Strategy & Research release stated. "Consumers cannot put their finances on autopilot or ignore important safeguards," it said. [30]

Then there is "notification fatigue." Considering the decrease in response time that the Ponemon Institute study found, notifications to consumers have rapidly increased. Within days of Epsilon announcing its breach of 130 million email addresses, email notifications to consumers were sent, with some consumers receiving multiple emails due to the number off affected Epsilon customers. Taking these facts into account, some are worried consumers may get "notification fatigue" and tune out breach notifications as well as the potential, serious effects of such breaches. However, some are also optimistic that an increase in notifications will lead to an increase in consumer awareness.[31]

What is Being Done?

Legally

As stated previously, most states have reacted to the increased threats of identity theft and fraud brought by the Information Age through adopting legislation. And while the U.S. Congress has yet to do the same, federal agencies have recognized the seriousness of malicious attacks and have joined the fray..

As stated in 2009 by the Department of Justice's Acting Attorney General of the Criminal Division, Rita Glavin: "The Department of Justice plays a critical role in combating payment card breaches and the fraud and other criminal activity that results." DOJ's various roles are played by the U.S. Attorney's offices throughout the country that prosecute data breach cases; the Computer Crime and Intellectual Property Section within the Criminal Division, which investigates, prosecutes and coordinates prosecutions of large-scale breaches; the Payments Fraud Working Group established by the DOJ's Criminal Division, which is an organization of law enforcement and bank regulatory agencies that examines security issues with payment cards; the Identity Theft Task Force, which has overlapping duties with the fore mentioned groups; and the Office of International Affairs within the Criminal Division, which provides aid when a single breach involves numerous countries. Other U.S. agencies that work with the DOJ include the United States Secret Service, FBI, and United States Postal Inspection Service to "aggressively" investigate and prosecute "data breaches and other criminal activity associated with them." [32]

---

[28] "Identity Fraud Fell 28 Percent in 2010 According to New Javelin Strategy & Research Report," Javelin Strategy & Research, Feb. 8, 2011, available at https://www.javelinstrategy.com/news/1170/92/1 (hereinafter "Identity Fraud Fell 28 Percent")

[29] "Consumer Sentinel Network Data Book for January through December 2010," Federal Trade Commission, March 2011, available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

[30] "Identity Fraud Fell 28 Percent"

[31] "Data breach notification fatigue: Do consumers (eventually) tune out?" George V. Hulme, CSO, April 12, 2011, available at http://www.csoonline.com/article/679415/data-breach-notification-fatigue-do-consumers-eventually-tune-out-

[32] Glavin.

Such investigations have led to numerous arrests and prosecutions – most internationally. In 2004, several offices within the DOJ and the U.S. Secret Service worked together, along with numerous other nations, during Operation Firewall. The undercover investigation resulted in the arrest of 28 members from the "Shadowcrew" criminal organization. The arrested were indicted on 62 counts, including the trafficking of at least 1.5 million stolen credit card and bankcard numbers that led to at least $4 million in losses. "This prosecution was the first of its kind – by prosecuting top-tier members of the organization for conspiracy, it held individuals responsible for the criminal offenses facilitated through the carding forum by virtue of their leadership role in a criminal organization that operated solely online," Glavin said. "Operation Firewall enabled many of our more recent successes." [33]

Such successes include the 2007 arrest of Makysm Yastremskiy, a Ukrainian man believed to be one of the world's top traffickers in selling stolen account information. He was arrested in Turkey and indicted in the U.S. for his role in the TJX breach, among others. One of his leading customers, known online as "Lord Kaisersose," had been previously arrested in France as the result of a cooperative effort between the U.S. Secret Service and French National Police.[34]

In 2009, Yastremskiy was sentenced to 30 years in prison in Turkey for his hacking crimes there. The U.S. is awaiting his possible extradition to prosecute him for his role in the TJX breach – it's believed he led the sale of data stolen from the retailer – as well as his contribution to the hacking of eight other major U.S. retailers.[35] One of Yastremskiy's accomplices, U.S. citizen Albert Gonzalez, pleaded guilty in 2010 to his roles in the TJX breach as well as other data breaches, including the Heartland Payment Systems breach. He was sentenced to a "record-breaking" 20 years in prison, though now he has petitioned the court to throw out his plea and sentence on the basis of his undercover work for the Secret Service.[36]

Yastremskiy and Gonzalez are two of 11 members in an international hacking ring that was investigated by the Department of Justice. The investigation resulted in "the largest hacking and identity theft case ever prosecuted," Glavin said. Defendants in the case include citizens from the U.S., Ukraine, Estonia, the People's Republic of China, and Belarus and are charged with the theft of credit and debit card information from numerous retailers, including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave & Buster's, and DSW.[37]

The co-founder and administrator of a carding forum, Max Ray Butler a.k.a. "Iceman," was arrested in late 2007 for wire fraud and identity fraud. At the time of his arrest, the carding forum – CardersMarket – was "the largest marketplace for stolen credit and debit card information in the world." [38] The carding ring is thought to have stolen about 2 million credit card numbers that resulted in $86 million in fraudulent purchases.[39] Previously convicted of hacking into the Department of Defense in 2001, Butler pleaded

---

[33] Ibid.

[34] Ibid.

[35] "TJX hacker gets 30-year prison sentence," Angela Moscaritolo, SC Magazine, Jan. 9, 2009, available at http://www.securecomputing.net.au/News/132551,tjx-hacker-gets-30year-prison-sentence.aspx

[36] "In Surprise Appeal, TJX Hacker Claims U.S. Authorized His Crimes," Kim Zetter, Wired, April 7, 2011, available at http://www.wired.com/threatlevel/tag/albert-gonzalez/

[37] Glavin.

[38] "Criminal hacker 'Iceman' gets 13 years," Robert McMillian, Computer World, Feb. 12, 2010, available at http://www.computerworld.com/s/article/9156658/Criminal_hacker_Iceman_gets_13_years

[39] "Hacker Max Ray Butler Pleads Guilty," Brian Prince, Eweek, June 30, 2009, available at http://www.eweek.com/c/a/Security/Hacker-Max-Ray-Butler-Pleads-Guilty-522493/

guilty in 2009 and was sentenced in 2010 to 13 years in a minimum-security prison, five years of supervised release and was ordered to pay $27.5 million in restitution to his victims.[40]

The FBI and USAO for the Eastern District of Virginia led Operation CardKeeper, which resulted in 21 arrests – 13 in Poland and eight in the U.S. In 2007, one U.S. carder arrested during the operation was sentenced to 94 months in prison for numerous crimes associated with his carding activities, including aggravated identity theft, access device fraud, and conspiracy to commit bank fraud.[41]

More recently, two men – self-described Internet "trolls" – from the U.S. were arrested for hacking into AT&T's server and stealing email addresses and other personal information of about 120,000 iPad users. Andrew Auernheimer and Daniel Spitler were arrested Jan. 18, 2011, and charged with conspiracy to access a computer without authorization and fraud in connection with personal information.[42]

The above are just eight of the numerous cases that the Department of Justice and other government agencies, both nationally and internationally, have had their resources devoted to in the world of data breaches.

Through organizations

As noted by Glavin during the hearing, "keeping credit, debit, and other financial account information out of the hands of criminals in the first place is an essential first step in reducing the frequency, and minimizing the impact, of large-scale data compromises." One way the private credit card sector has sought to do this has been to develop security standards, known as the Payment Card Industry Data Security Standards. Glavin, during the hearing, recommended "all entities that store, process, or transmit credit, debit, and other financial account information should ensure they comply with all the requirements of the PCI DSS… ."[43] According to the Payment Card Industry Security Standards Council, the PCI DSS "provides an actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents." The PCI Security Standards Council aids institutions so they can comply with the best practices of PCI DSS, which include assessing vulnerabilities, remediating those vulnerabilities, and reporting regularly to specified professionals, though providing security questionnaires, professionals, and training.[44]

While defiance of the PCI DSS doesn't directly result in the issuance of fines, the Financial Industry Regulatory Authority does have the power to levy monetary punishment in response to a data breach among its members. "FINRA is the leading non-governmental regulator for all securities firms doing business with the U.S. public," according to its website[45], and "fines are an important sanction in FINRA's arsenal of tools to deter misconduct."[46] FINRA levied $41.1 million in fines in 2010,[47] with a fraction of that resulting from data breaches. Fine money is kept separate from the organization's operating budget and

---

[40] "Criminal hacker 'Iceman' gets 13 years"

[41] Glavin

[42] "Two Men Charged in New Jersey With Hacking AT&T's Servers," Department of Justice, Jan. 18, 2011, available at http://www.justice.gov/criminal/cybercrime/auernheimerArrest.pdf (hereinafter "Hacking AT&T's servers)

[43] Glavin

[44] "Getting Started with the PCI Data Security Standard," PCI Security Standards Council, LLC., available at https://www.pcisecuritystandards.org/security_standards/getting_started.php

[45] "FINRA Leadership," Financial Industry Regulatory Authority, available at http://www.finra.org/AboutFINRA/Leadership/

[46] "FINRA Fines Policy," Financial Industry Regulatory Authority, available at http://www.finra.org/Industry/Enforcement/SanctionGuidelines/FinesPolicy/ (hereinafter "FINRA Fines Policy")

[47] "FINRA 2010 Year in Review," Financial Industry Regulatory Authority, available at http://www.finra.org/Newsroom/NewsReleases/2010/P122662

revenue, and its uses are "limited to capital expenditures and specified regulatory projects that have a clear and direct nexus to protecting investors and ensuring market integrity."[48]

In the workplace

Training and awareness programs are an organization's most popular remedy following a data breach; nearly two-thirds of organizations in the Ponemon study that experienced a data breach responded with such programs. Almost the same amount responded to a breach with increased use of encryption – though as noted earlier, the "human factor" may undermine this. More than half of the organizations added more manual procedures and controls as well as identity and access management solutions after a data breach. Other less popular remedies included data loss prevention solutions and endpoint security solutions. According to the Ponemon report, "Taken together, these figures may indicate that companies continue to rely upon educating their workforce and enabling it to personally help stop future data breaches. At the same time, though, companies are increasingly aware of, and willing to implement, technological solutions designed to help prevent and mitigate breaches."[49]

In response to its recent breach, Epsilon has said it will increase its security, although details have yet to be released. The CEO of Epsilon's parent company has said some flexibility and user-friendliness will be sacrificed, though, and the company will come out to be the industry's leader in security.[50]

To comply with legal and commercial regulations, companies are reacting more quickly to data breaches than in previous years. While this may seem to be a step in the right direction, the rapid response time is one reason why costs associated with data breaches rose in 2010. According to the Ponemon report, "For the second year in a row, these 'quick responders' paid significantly more per record than companies that moved more slowly … Breaches for companies that took longer [to notify] cost $94 (35 percent) less this year than quick-response breaches." Because data breach legislation and regulations continue to change and grow, and the media is becoming more conscientious about the response time associated with breached information, Ponemon has said it will continue to study its effects on breach costs.

In conjunction with public scrutiny and both legal and commercial regulations, companies may be decreasing notification time also because they, too, are recognizing breaches sooner and have allocated more money to ex-post responses. According to the Ponemon study, "organizations became much more proactive in finding and starting their response to data breaches in 2010." Compared to 2009, companies reserved 72 percent more funds in 2010 to detection and escalation costs and 15 percent more money to ex-post response. While companies have "devoted noticeably more resources to contacting and helping data breach victims," this is most likely tied to a company's fear of litigation following a data breach.[51] In the case of Heartland Payments Systems, Inc., about one-third of its total breach costs, as of 2010, had been allocated to litigation settlements.[52]

However, some are contending that fines and lawsuits filed on behalf of the state, rather than those whose information had been breached, is counterproductive. "…Some experts now question whether the government is penalizing one of the victims in a crime, rather than helping to mitigate the risk of identity theft – as the laws were first intended," reports CSO's George V. Hulme. In the article, Spire Security's Research Director Pete Lindstrom said fines deter businesses from self-regulating and reporting

[48] "FINRA Fines Policy"
[49] "U.S. Cost of a Data Breach"
[50] "Epsilon"
[51] "U.S. Costs of a Data Breach."
[52] "Heartland breach."

breaches to government agencies, as Enloe Medical Center in California did after it found, through its own monitoring and investigation, a breach of a single patient's records. Once Enloe acknowledged the breach and informed the California Department of Public Health, the CDPH reacted with a fine of $130,000. In this case, "the lesson to others is to hide their incidents," Lindstrom said.[53]

A new internal study by Verizon, in partnership with the U.S. Secret Service, may indicate that it's becoming harder to even detect malicious attacks, though. While the Verizon 2011 Data Breach Investigation showed an increase in the number of breaches from 2009 – the Secret Service contributed to the majority of these – the number of lost records dropped an astounding 97 percent. Verizon has several hypotheses to explain their results: caseload variation, the absence of large breaches such as TJX's, a customer base that's less representative of overall breach activity, among others. The leading theory, though, "is that prosecution of data thieves is working as intended." However, "some outside security experts with hands on experience investigating data breaches say the reports unusual findings only underscore the difficulty of tracking the data theft crimes across the public and private sectors."[54]

Ending the Epidemic

Glavin said it best during her remarks to the Homeland Security's congressional subcommittee: "Perfect security is impossible."[55] However, as noted by the ITRC, "breaches don't just happen, they are allowed to happen."[56] But the losses posed by and the sheer number of data breaches can be limited to a smaller scope than what is currently being achieved. Numerous government agencies, private companies and organizations, including NSCI, agree that some sort of federal legal action must be taken.

Not only is there currently no national standard as to what constitutes a data breach, there is no mandate on reporting a breach. When breaches go unreported, government agencies are unable to investigate and, if warranted, prosecute criminals to stop future breaches from occurring. "We know from experience that prompt detection will not itself result in a report from the victim company," Glavin told Congressional members, which is why "data breaches are significantly underreported." Glavin went on to say, "Because only a handful of state laws currently require reporting to law enforcement and because private sector rules are neither universal nor consistently enforced across the various companies, we urge Congress to consider requiring security breach reports to federal law enforcement using a mechanism that ensures that the USSS and FBI have access to the reports."[57] Chief of the FBI's Cyber Criminal Section, Jeffrey Troy, agreed with Glavin and said he supports a federal data breach law as it "would help us tremendously, particularly in terms of efficiency in conducting investigations."[58] The FTC also endorses federal legislation regarding data breaches. During the 111th Congress, the FTC said it "strongly supports" the Data Security and Breach Notification Act of 2010; the bill has yet to become a federal law.[59]

It's not only government agencies that are urging Congress to act. The Identity Theft Research Center and Symantec both support national data breach legislation. According to the ITRC: "It is clear that

---

[53] "Data breach fines can risk more harm than good, experts say," George V. Hulme, CSO online, April 21, 2011, available at http://www.csoonline.com/article/680211/data-breach-fines-can-risk-more-harm-than-good-experts-say

[54] "Weird Science: Verizon Finds Stunning Drop in Data Theft," Paul Roberts, The Kaspersky Lab Security News Service, April 19, 2011, available at http://threatpost.com/en_us/blogs/weird-science-verizon-finds-stunning-drop-data-theft-041511

[55] Glavin.

[56] "Hackers: Duhhh, Winning"

[57] Glavin.

[58] "FBI: National Data-breach Law Would Help Fight Cybercrime," Grant Gross, IDG News, Oct. 28, 2009, available at http://www.pcworld.com/article/174584/fbi_national_databreach_law_would_help_fight_cybercrime.html

[59] "FTC Endorses Federal Data Breach Law," Jeff Nickles, INSURICA, Sept. 27, 2010, available at http://technology.blog.insurica.com/ftc-endorses-federal-data-breach-law/

without a mandatory national reporting requirement, that many data breaches will continue to be unreported, or under-reported." This claim is substantiated by the 38.5 percent of breaches listed in the ITRC's 2010 report that didn't disclose how the data was leaked as well as the 49 percent of breaches that withheld the amount of data that was compromised. ITRC goes on to state, "the nation needs a centralized, publicly available, data breach reporting site" that would allow seekers to openly access information about breaches as well as "allow law enforcement to better address this type of crime."[60] Symantec's CTO Mark Bregman testified before a Congressional subcommittee to also endorse the Data Security and Breach Notification Act of 2010[61] – a law that would answer what Symantec has said the nation has needed for years.

After Sony went public with its breach of personal information associated with 77 million user accounts at the end of April and Epsilon announced 130 million email addresses had been compromised in March, members of Congress intensified the conversation on Capitol Hill about national data breach regulations. "(The Sony breach) reinforces my long-held belief that much more needs to be done to protect sensitive consumer information," Rep. Mary Bono Mack, R-Calif., chairwoman of the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade, said in a statement. She said she plans to introduce a bill that would protect consumers and regulate data breaches soon. Bono Mack isn't the only Congressional member to have heightened worries, though. Rep. Bobby Rush, D-Ill., who also sits on Energy and Commerce and chaired Bono Mack's subcommittee in the last Congress, offered a data breach bill in the past that was approved by the House, and he plans to reintroduce that bill during this Congress.[62] Action by the federal government will provide an across-the-board definition of what is included in a data breach and provide organizations clearer direction on what legal actions must be taken when a breach occurs.

However, federal legislators should keep in mind that punishing a data breach with a fine, such as state governments and organizations like FINRA have done, may be counterproductive. If a fine is to follow, institutions may be less likely to be forthcoming about known breaches, as noted by Pete Lindstrom.[63] Rather than having a blanket fine, the law should consider whether the industry's best security practices were met or if the breach occurred because of obvious negligence and inadequate security precautions. This approach may be less discouraging to organizations when relying on industry to self-regulate. And rather than having fines masked within the government's overall budget, perhaps the government should imitate FINRA in how it allocates its fine monies. Fine revenues going to the federal government could be allocated to funding grants for institutions seeking to improve data security.

Federal law would also aid when the investigations and prosecutions of data breaches cross national borders. There is a growing global scope of data breaches, as is demonstrated by online carding forums, international hacking rings and specific cases, such as the TJX breach. Because of this, Glavin said, "coordination and cooperation from foreign law enforcement is vital to the success of carding investigations and prosecutions,"[64] – the same could be said for all types of international data breaches.

---

[60] "Data Breaches in 2010"

[61] "Symantec CTO Mark Bregman Testifies on Data Security and Breach Legislation," Symantec, Sept. 22, 2010, available at http://www.symantec.com/about/government/recentactivities/activities.jsp?prid=20100922_01

[62] "Lawmakers say Sony data breach underscores need for legislation," Juliana Gruenwald, National Journal, April 28, 2011, available at http://www.nextgov.com/nextgov/ng_20110428_6991.php

[63] "Data breach fines can risk more harm than good, experts say"

[64] Glavin.

Kandice McKee, NSCI
May 4, 2011

Nations across the globe addressed the growing complexity of data breaches early this millennium with the Convention on Cybercrime. The Council of Europe drafted the Convention in 2000, and nations began adding signatures in late 2001. President George Bush signed the treaty in 2001, though the Senate didn't ratify it until 2006.[65] According to the Convention's Explanatory Report: "The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society."[66] While some U.S. groups, like EPIC and the ACLU, have expressed concern with the implications this treaty will have on personal liberties,[67] several institutions supported its ratification, including the Business Software Alliance and Information Technology Association of America.[68] Because only about half of the 46 countries that signed the treaty have also ratified it, there is more work to be done to further international cooperation[69] – but "the Convention at least gives us a place to start."[70] The Convention on Cybercrime isn't the only international effort that has or should take place, though. The U.N. has also addressed the internationality of cybercrime, and countries continue to work with each other when dealing with such cases.[71] However, this cooperation must continue and grow to accurately counter cybercrime threats.

While the National Security Cyberspace Institute supports federal legislation and international cooperatives, to best limit the number and effect of data breaches, NSCI believes industry and governments need to work together and become more proactive rather than reactive. Government could be more proactive by offering incentives for tighter security, such as tax incentives and tax breaks. The PCI DSS is an example of industry being proactive in the fight against data breaches. With private industry adopting security protocols and standards, the government influence is kept to a minimum. However, "even if 100 percent compliance with PCI DSS were achieved, it is likely that hackers will continue to develop techniques to exploit the computer systems of companies holding cardholder data."[72]

Before his arrest for hacking into AT&T's servers, Auernheimer told *The New York Times* in 2008: "I hack, I ruin, I make piles of money."[73] The reality of this statement, as well as the "human factor" with data breaches, is why reactive measures need to be in place as well.

---

[65] "Senate Ratifies Convention on Cybercrime," Tech Law Journal, Aug. 3, 2006, available at http://www.techlawjournal.com/topstories/2006/20060803b.asp (hereinafter "Senate Ratifies Convention on Cybercrime")

[66] "Explanatory Report to the Convention on Cybercrime," Council of Europe, available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (hereinafter "Explanatory Report")

[67] "World's Worst Internet Law," Nate Anderson, Arstechnica, August 2006, available at http://arstechnica.com/old/content/2006/08/7421.ars

[68] "Senate Ratifies Convention on Cybercrime"

[69] "A Global Convention on Cybercrime?" Brian Harley, *The Columbia Science and Technology Law Review,* March 23, 2010, available at http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (hereinafter "A Global Convention on Cybercrime?")

[70] "Senate Ratifies Convention on Cybercrime"

[71] "A Global Convention on Cybercrime?"

[72] Glavin.

[73] "Hacking AT&T's Servers"