Data Breaches in the Government Sector

A Rapid7 Research Report

RAPID7

Summary of Report

Across all industries, data breaches and the protection of business-critical data remain a top concern. While the government sector has remained committed to making investments to prevent data breaches – implementing rigid security best practices, undergoing comprehensive product testing, developing compliance regulations, etc. – government agencies are not immune to breaches. In fact, according to a recent report by the Government Accountability Office (GAO), 18 out of 24 major federal agencies in the United States reported inadequate information security controls for reporting.

Rapid7 has found that the government sector has experienced a steady increase in the number of records exposed, and a fluctuating number of incidents over the last three years. From January 1, 2009 to May 31, 2012, there have been 268 breach incidents in government agencies with more than 94 million records[1] containing personally identifiable information (PII) exposed.

Rapid7, the leading provider of security risk intelligence solutions, analyzed data collected and categorized by the Privacy Rights Clearinghouse Chronology of Data Breaches. Using this data, which includes information from The Open Security Foundation, the company outlined patterns for government data breaches, including year, month, location and breach type patterns. This information and tips for protecting infrastructure can ensure that government IT environments stay protected against malicious attacks and unintended disclosure.

Key Findings:

Cost of Breaches – According to the Ponemon Institute's 2011 Cost of Data Breach Study, the cost per record has declined from $214 to $194.

Number of Breach Incidents by Year –

- 2009: 53
- 2010: 102
- 2011: 82
- January – May 31, 2012: 31

Incidents by Breach Type – Types of breaches, number of incidents and reported PII records exposed between January 2009 – May 2012:

- Unintended disclosure – 78 incidents exposing 11,783,776 records
- Portable device – 51 incidents exposing 80,706,983 records
- Physical loss – 46 incidents exposing 296,710 records
- Hacking or malware – 40 incidents exposing 1,082,749 records
- Insider – 39 incidents exposing 177,399 records
- Stationary device – 6 incidents exposing 250,650 records
- Unknown or other – 8 incidents exposing 5,906 records

Locations of Breach Incidents – Top three locations with the highest number of reported incidents:

1. California – 21 incidents exposing 799,849 records (PII)
2. District Of Columbia – 20 incidents exposing 76,126,807 records (PII)
3. Texas – 16 incidents exposing 10,005,910 records (PII)

Number of Records Exposed by Year – Year-by-year comparison of reported breaches (by PII only):

- 2009 – 79,109,971
- 2010 – 1,505,877
- 2011 – 4,046,163
- 2012 – 9,642,162

1 According to the Privacy Rights Clearinghouse: www.privacyrights.org, which includes information from The Open Source Foundation

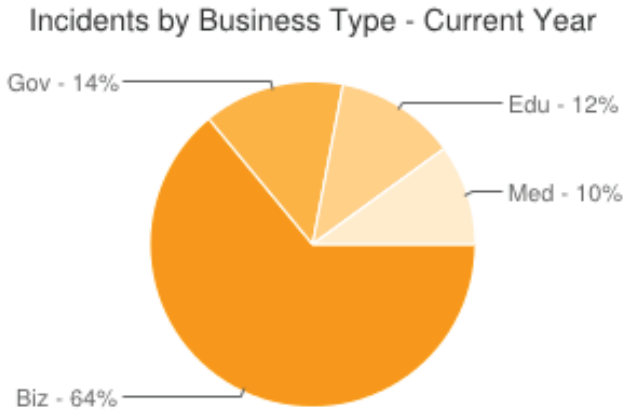
Overview

Today, data breaches have gone mainstream. Whether it's the LinkedIn password breach or Sony PlayStation Network attack, more consumers than ever have received notifications from companies stating that sensitive, personally identifiable information may have been exposed, and detailing next steps for protecting identities, bank and credit card accounts, and other critical applications.

As the number of data breaches has increased, so too has the government's interest in protecting citizens. Following California's data breach notification law, SB 1386, which went into effect in 2003, all 50 states have adopted laws requiring that businesses notify their residents when their personal information may have been breached. Most recently, Senate Republicans have introduced draft legislation known as the "Data Security and Breach Notification Act of 2012 (S.3333)" to create a single, national standard for reporting data breaches. In addition to standardizing the notification process for a breach, the draft bill will also require that businesses and government agencies "take reasonable measures to protect and secure data in electronic form containing personal information" or face a $500,000-per-incident fine.

However, it's not just the private sector that is responsible for reporting on information security. The Federal Information Security and Management Act (FISMA), enacted in 2002 under the E-Government Act of 2002, required regular reporting from federal agencies regarding their information security practices. FISMA was then revamped in 2009 to mandate real-time reporting rather than the previously-required annual reports. This new type of reporting would be facilitated by CyberScope, an online reporting tool.

While headlines about exposed records by credit card companies, social media sites, and retailers are more common, breaches of government records with personally identifiable information continue to increase as well. In fact, according to The Open Security Foundation's DataLossDB, government is the second highest industry to report data breaches in 2012.



Data and Image Credit: The Open Security Foundation's DataLossDB

Each year, federal agencies are evaluated on their security measures in seven areas, and given scores to illustrate their level of compliance with FISMA to determine whether the agency had, "established and maintained a program that was generally consistent with NIST and OMB's FISMA requirements, and included the needed attributes; the agency had established and maintained a program that needed significant improvements; (or that) the agency had not established a program for the area." According to the Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002, eight federal agencies scored less than 65 percent.

Agency	FY11 (%)	FY10 (%)	Change
National Science Foundation	98.8	98.9	-(0.1)
Social Security Administration	96.9	100	-(3.1)
Environmental Protection Agency	94.9	99.2	-(4.3)
Nuclear Regulatory Commission	94.8	96.7	-(1.9)
Department of Homeland Security	93.4	92.5	0.9
National Aeronautics and Space Administration	92.9	60.8	32.1
Department of Justice	91.2	85.8	5.4
Department of Energy	84.3	84.6	-(0.3)
General Services Administration	84.2	87.6	-(3.4)
Department of Commerce	81.4	77.9	3.5
Department of the Treasury	79.4	86.4	(-7.0)
Office of Personnel Management	78.6	57.8	20.8
Department of Labor	71.6	44.5	27.1
Small Business Administration	68.7	50.3	18.4
Department of Housing and Urban Development	66.1	87.3	-(21.2)
Department of State	63.2	79.4	-(15.2)
Department of Education	57.5	71.9	-(14.4)
United States Agency for International Development	53.8	90.4	-(36.6)
Department of Veterans Affairs	52.8	57.0	-(4.2)
Department of Health and Human Services	50.9	64.7	-(13.8)
Department of Transportation	44.2	29.8	14.4
Department of the Interior	42.2	24.6	17.6
Department of Agriculture	32.5	13.7	18.8
Department of Defense	N/A	N/A	N/A*

*DOD did not provide the answers with the detail required for scoring in FY 2010 or FY 2011

Credit: Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002

In that same report, the United States Computer Emergency Readiness Team (US-CERT) received a total of 107,439 reports, 41,776 of which impacted federal government departments and agencies in fiscal year 2010. That number increased the following year (FY 2011) to a total of 107,655 reports, 43,889 of which impacted federal government departments and agencies. For incidents that were part of an outside attack, malicious code was the most widely reported incident type by the federal government in fiscal year 2011.

One factor in that increase may be the abrupt rise of hacktivism in 2011. Defined as "the use of computers and computer networks as a means of protest to promote political ends," hacktivism pre-dates 2011. However, its impact on government infrastructure captured widespread attention when the Tunisian government websites were attacked in January 2011 following its censorship of the Wikileaks documents, and the Tunisian protests. That same year, a variety of government agencies were attacked and/or their records were exposed, including the Federal Bureau of Investigation, the Government of Brazil, the United States Marine Corp, the United States Department of Homeland Security, NATO, and the California Department of Justice, among others. While these activities encompassed more than data breaches, including denial-of-service attacks, the hacktivism exposed the vulnerability of websites, networks, and databases of government agencies.

In addition to hacktivism, government infrastructure comes under attack by other forces, including foreign hackers, and cyberespionage by nation states. Richard Clarke, former White House counter-terrorism adviser, stated in 2011 that "the Chinese have attacked every major U.S. company, every government agency, and [nongovernmental organizations] NGOs" following reports that hackers associated with the Chinese military attacked the Chamber of Commerce.[2] In October 2011, the Office of the National Counterintelligence Executive, which focuses on espionage against the United States,

2 ABC News Report, "Chinese Hack Into US Chamber of Commerce, Authorities Say," December 2011

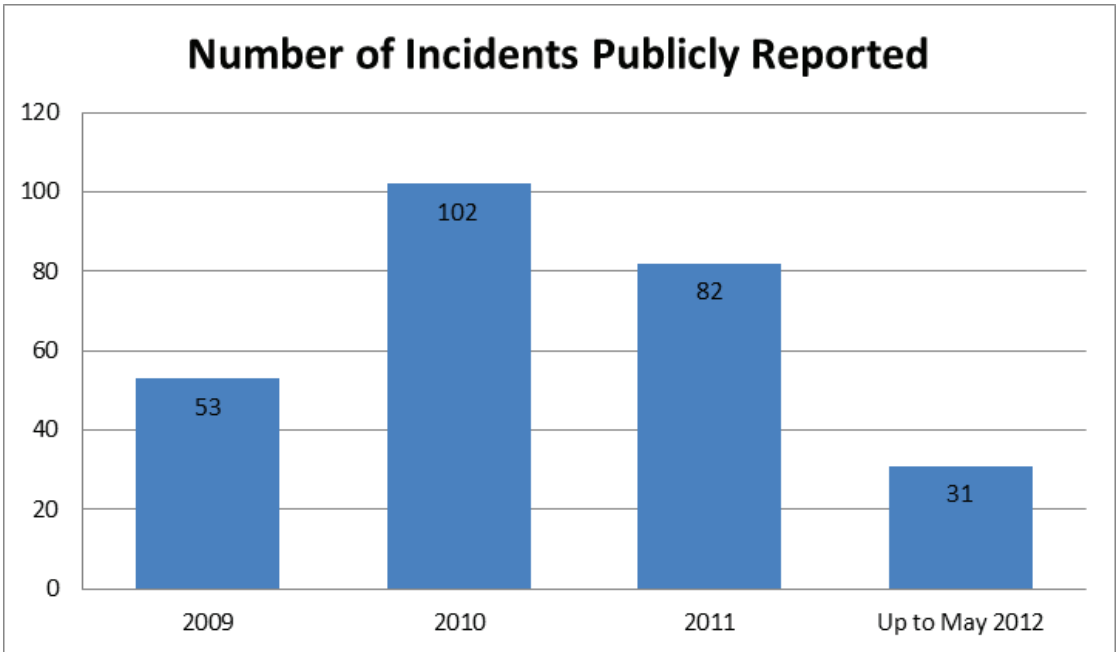
released a report titled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace"[3] to Congress. This report publicly stated that China and Russia were responsible for stealing trade secrets, technology, and intellectual property. For many of these attacks, the amount of records breached remains unknown.

With employee error, malicious insider threats, and outside attacks, including hactivism and cyberespionage, the United States government infrastructure faces increased exposure.

Details on Findings

I. Number of Incidents by Year

For this report, Rapid7 analyzed government data breaches between January 1, 2009 and May 31, 2012. Based on the data provided by the Privacy Rights Clearinghouse, which includes information from The Open Source Foundation, there were a total of 268 incidents during this time frame. Among those incidents, 67 list the number of records exposed as unknown. For the purpose of this report, Rapid7 included those occurrences as part of its analysis for number of incidents, breach location and type, but not for number of records exposed.

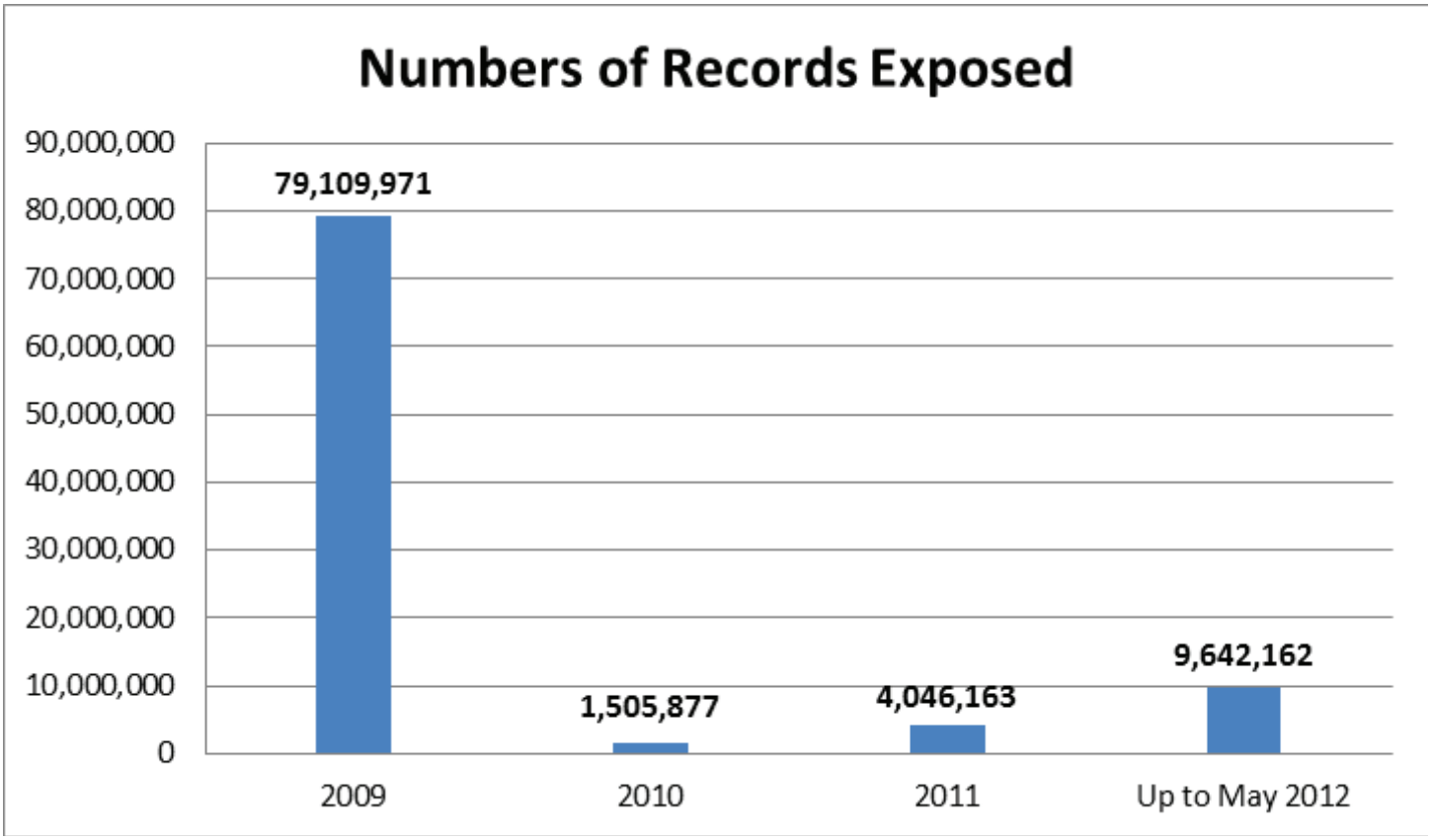


Based on the time frame, there were more incidents of data breaches in 2010 compared to other years – with a near double year-over-year comparison to 2009 – yet 2010 included the lowest number of PII records exposed, with less than 2 million. During 2011, there were 82 incidents with more than 4 million PII records breached (more than doubling 2010) and by May 2012, there were 31 incidents with more than 9 million PII records exposed.

Though 2009 may have led with the greatest number of records exposed for the analyzed time frame, most occurred during the month of October, when more than 76 million records were breached. This was a result of one of the largest government data breaches in history, when 76 million US veterans' personally identifiable information was exposed after a defective hard drive was sent to a government vendor for repair and recycle before the data was erased. The hard drive hosted a database of military veterans' information, (including social security numbers), which according to various reports, potentially dated back to records from 1972. Leading up to that month and specific incident, September of 2009 had no incidents of data breaches.

3 http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Even though less than half of 2012 is being reviewed for this report, the number of records exposed so far has already doubled the total from 2011. As of May 31, 2012, 2012 has reported an estimated 9,642,162 of PII records stolen and 10,816,795 total records (PII and non-PII) breached. When looking at the data from January 2012 to May 31, 2012, April is the highest reported month for breaches. The majority of breaches for the 5-month time frame occurred in this month, which reported approximately 6,780,000 PII and 7,280,000 total records exposed.



Throughout each of these years, one group of government employees remained particularly at risk both at the federal and state/local levels: U.S. veterans. From January 1, 2009-May 31, 2012, there were 14 incidents impacting veterans, with more than 76.2 million records with personally identifiable information exposed. The Department of Veteran Affairs experienced multiple breaches (the same agency that scored less than 65 percent in the 2011 FISMA scores). A few of these breaches include:

- October 2, 2009: U.S. Military Veterans (District of Columbia)
- May 14, 2010: Department of Veterans Affairs (District of Columbia)
- November 16, 2010: Education Department, Department of Veterans Affairs (New York)
- December 21, 2010: Department of Veterans Affairs (Texas)
- January 29, 2011: Veterans Affairs Medical Center (Vermont)
- January 20, 2012: Department of Veteran Affairs (District of Columbia)

II. Types of Data Breaches

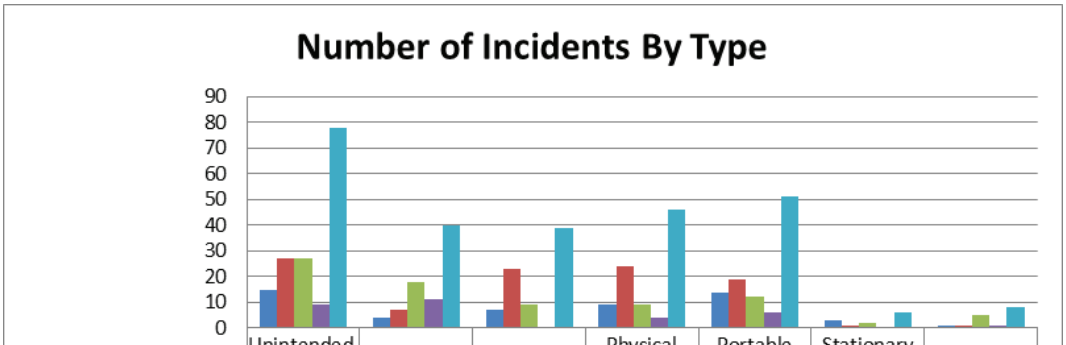
For this report, the types of data breaches are divided into eight categories, per the Privacy Rights Clearinghouse, and are defined as:

- Unintended disclosure – Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail.
- Hacking or malware – Electronic entry by an outside party, malware, and spyware.
- Insider – Someone with legitimate access intentionally breaches information – such as an employee or contractor.
- Physical loss – Lost, discarded, or stolen non-electronic records, such as paper documents.
- Portable device – Lost, discarded, or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
- Stationary device – Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.
- Unknown or other.

From January 2009 through May 31, 2012, employee error and device theft caused the majority of data breaches. Combining unintended disclosure, insider threats, physical losses, the loss/theft of portable devices, and the loss/theft of stationary devices, the total number of incidents reached 214 (out of 268), exposing more than 93 million PII records.

Of those individual categories, unintended disclosure was the reported leading cause of incidents by type, with 78 occurrences that exposed the second highest number of records at more than 11 million. This category was followed by portable devices (50), physical loss (46), hacking/malware (40) and insider threat (39). The theft/loss of stationary devices and unknown categories were the smallest with 6 and 8 incidents.

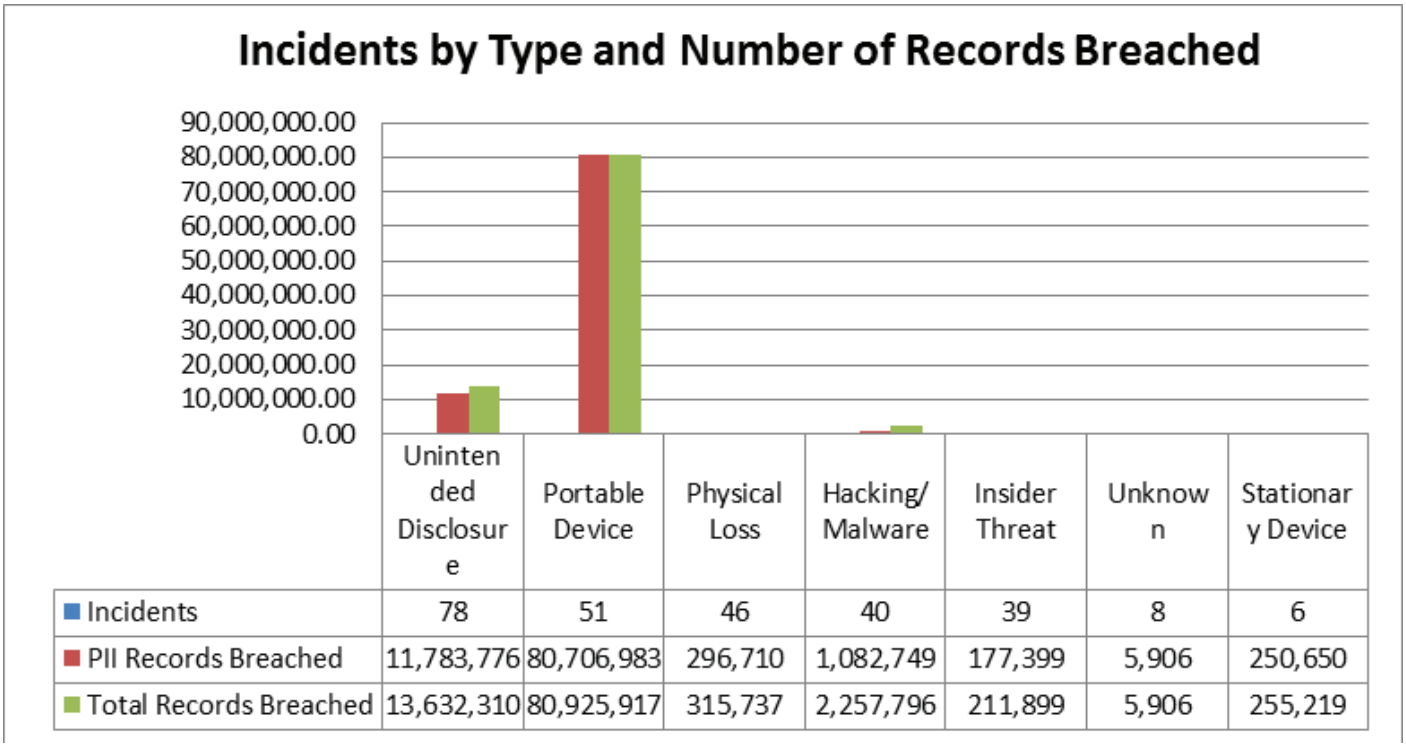
The analysis also shows that the number of incidents caused by hacking is on a steady rise. A year-over-year comparison shows a nearly 50 percent increase from 2009 to 2011. Between January 1, 2012 and May 31, 2012, government agencies reported more hacking incidents than any other category.



	Unintended Disclosure	Hacking	Insider	Physical Loss	Portable Device	Stationary Device	Unknown
2009	15	4	7	9	14	3	1
2010	27	7	23	24	19	1	1
2011	27	18	9	9	12	2	5
Up to May 31, 2012	9	11	0	4	6	0	1
Total Cases	78	40	39	46	51	6	8

In terms of the type of breach that compromised the greatest amount of PII records, portable devices were at the top, with more than 80 million PII records exposed. The largest case in the portable device category is the incident in October 2009, when 76 million US veterans' data was exposed as a result of a hard drive that wasn't erased before being sent out for repair and recycle.

The second and third most common types of breaches were unintended disclosure and hacking or malware. Unintended disclosure reported an estimated more than 11.7 million PII and 13.6 million total records exposed. Hacking and malware reported approximately 1.1 million PII and 2.3 million total records exposed. For hacking, the total number of records exposed actually puts the files at additional risk, since hackers and malware use phishing schemes to then convert those public records into PII. In fact, one of the larger reported hacking cases, a hack into the Utah Department of Health computer server, involved 280,000 PII records and 780,000 total records exposed, which was not the initially reported number (25,096 PII records and 181,604 total records) when the breach was officially filed.



	Unintended Disclosure	Portable Device	Physical Loss	Hacking/ Malware	Insider Threat	Unknown	Stationary Device
Incidents	78	51	46	40	39	8	6
PII Records Breached	11,783,776	80,706,983	296,710	1,082,749	177,399	5,906	250,650
Total Records Breached	13,632,310	80,925,917	315,737	2,257,796	211,899	5,906	255,219

It's important to note that the hacking category contains many breaches where the number of records exposed was reported as unknown. This makes it impossible to accurately measure the damage. These incidents include many hacking events claimed by Anonymous and Lulzsec, including an attack on the Arizona Department of Public Safety (AZDPS), the Texas Police Chief Association, California Statewide Law Enforcement Association (CSLEA), and the United States Bureau of Justice Statistics (BJS). One incident that was reported involved the Federal Aviation Administration; in 2009 hackers attacked the agency's computer system, accessing the names and Social Security numbers of employees and retirees. The U.S. Army was also hacked in 2009, when a database of personal information about nearly 1,600 soldiers was penetrated by unauthorized users.

Aside from unknown types of breaches, which were the lowest recorded number of breaches, the number of insider attacks or errors which led to breaches were actually relatively small, with approximately 177,399 PII records stolen and 211,899 total records exposed.

By analyzing the data, it's clear to see that the number of cases or data breach events remains relatively consistent across the largest categories for records exposed. In other words, while the portable devices category accounts for the largest amount of *records* breached, the number of *incidents* involving portable devices (48) is lower than that of unintended disclosure (59). Also, the number of cases in the insider and hacking category is the same, while records breached by an employee or contractor is relatively low (177,399 of PII records and 211,899 total records) compared to records breached by a hacker or malware (1,082,749 PII records and 2,257,796 total records).

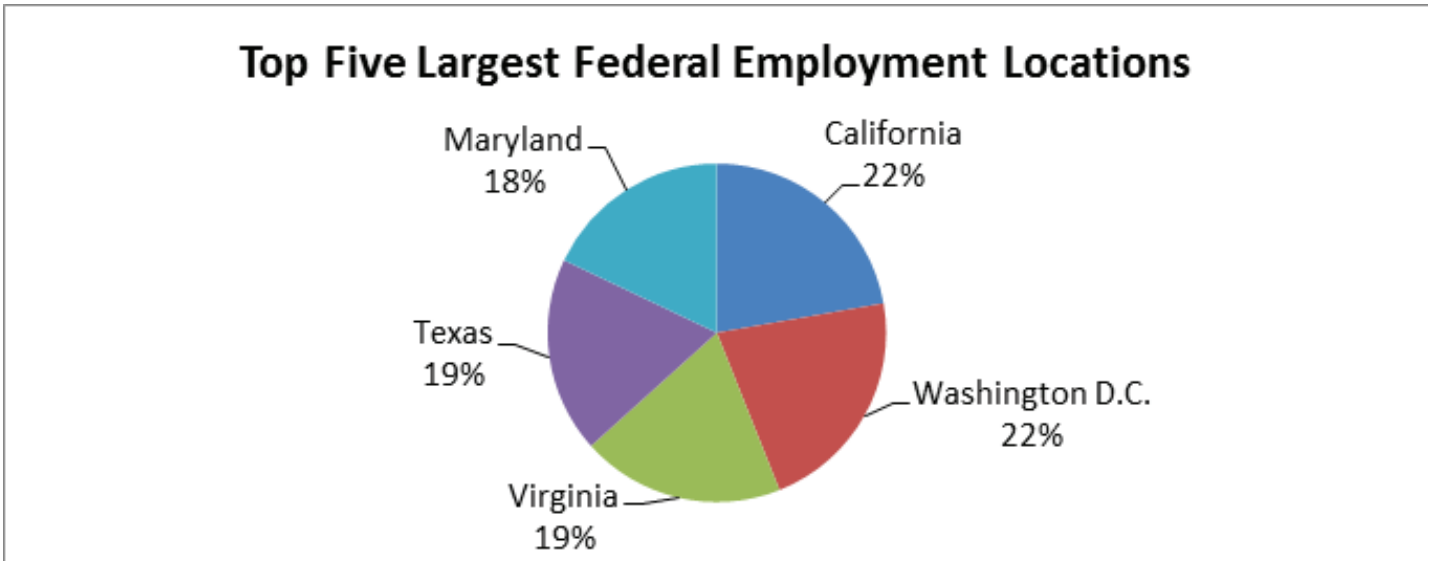
III. Location of Breaches

Among the locations that lead the nation in largest number of breach incidents, California is the highest with 21 events between January 1, 2009 and May 31, 2012. California is followed by the District of Columbia (20) and Texas (16).

In terms of size of breaches, the District of Columbia experienced the greatest amount of PII records exposed, with approximately 76 million records exposed during the analyzed time period. Considering the number of federal agencies located in the D.C. area, including high-profile organizations, it's not surprising that the location was the highest in number of breaches. However, despite its concentrated area of government offices and proximity to D.C., Virginia was not the second highest state for the number of records breached. The state that reported the second highest number of breached records was Texas, with approximately 10 million records breached. The top three locations in the United States with the highest number of records breached was rounded out by Oklahoma, with 1.36 million records breached (followed closely by New York with 1.35 million records).

There are a number of states that reported no breaches at all, including Kentucky, Montana, Nevada, North Dakota and South Dakota. Alaska, Delaware, Idaho, New Hampshire, Rhode Island and West Virginia reported one incident each, which exposed fewer than 75,000 records combined.

According to the most recent Fedscope data, compiled by the U.S. Office of Personnel Management, the top five largest federal employment locations in the nation include California, Washington D.C., Virginia, Texas, and Maryland.



Conclusion:

Government agencies are facing an increase in data breaches as a result of cyber attacks, weaknesses in federal information security controls, and poor best practices for protecting data on portable devices. At the same time, an increase in regulations has led to a rapid rise in IT and security certification costs. For example, costs for FISMA compliance auditing have risen to $1 billion annual and FISMA accreditation costs to $1.3 billion annually. According to the OBM fiscal year

2011 report to Congress on the implementation of FISMA (March 2012), federal agencies are spending $13.3 billion on IT security each year.

With this in mind, there are clear steps to ensure that an environment meets compliance regulations as well as company policies on security and risk intelligence. Steps include:

1. Vulnerability Management (Risk Assessment)

Federal agencies must discover, assess, prioritize, and mitigate vulnerabilities in both physical and virtual federal computing infrastructures. Best practices include mapping vulnerabilities to alerts generated by IAVA, as required by DISA.

2. Penetration Testing (Risk Validation)

After vulnerabilities are discovered and prioritized, IT administrators must validate actual exploitability in federal computing infrastructure to document real, contextual risk through penetration tests and social engineering.

3. Regulatory Compliance (FISMA)

Meeting FISMA requirements includes testing security controls that map to NIST SP 800-53 Rev.4 and automating CyberScope reporting, required to submit monthly FISMA metrics.

4. Configuration Compliance

IT administrators must perform security audits to establish and maintain compliance with the United States General Configuration Benchmarks (USGCB), the Federal Desktop Core Configuration (FDCC) and other SCAP guidelines.

5. Continuous Monitoring

As a final step, government IT departments must address NIST SP 800-137 requirements for continuous monitoring and risk-guided decision making.