# Towards a Model for Data Breaches: a Universal Problem for the Public

Robert E. Holtfreter
School of Business
Central Washington University
doctorh007@gmail.com

Adrian Harrington
Yakima, Washington
aaharrington87@gmail.com

## Abstract

The topic of data breaches, protection of information and data security salient to business and criminal justice researchers, practitioners in all profit and nonprofit organizations, consumer advocate groups and legislators throughout the world. This article analyzes the trends in data breaches in the United States and classifies them into five general industry sectors and eighteen sub-sectors using a new model recently developed by the authors and also provides basic recommendations for information and security personnel in every industry throughout the world to use to improve data protection and thus help protect public information for consumers and all types of organizations. The 2,280 data breaches tracked by the Privacy Rights Clearinghouse from 2005 through 2010 were used in the study. The findings indicate that the trends for the annual number of data breaches for the five general industries and their sub-sectors have increased, although inconsistently, over the six-year period. The analysis and classification of data breaches by general and sub-sector industries with the use of this new data breach model provides an awareness of the data breach problem for information managers and security personnel in public and private sector organizations throughout the world and also provides a workable methodological framework to help them develop innovative and useful policies for safeguarding personal information of consumers, clients, employees and other entities. The topic of data breaches and information management remains salient to business and criminal justice researchers, practitioners in all profit and nonprofit organizations, consumer advocate groups and legislators throughout the world.

Keywords – Data breaches, public information, data protection, identity theft.

## 1. Introduction

This article will help to protect organizations involved in the public sector by developing a methodological framework for classifying and analyzing data breaches in a number of general and sub-sector industries. As a result, this will be useful in allowing comparisons between public sector breaches and those in various other industries, which in turn provides a pathway for determining the applicability of private sector solutions to private sector problems.

We critique the recent data breach case for Heartland Payments Systems, a major credit card processor in the United States, which finally admitted after months of denial due to their investigation of the case that their processing system was intruded by hackers who stole personal data for over 130 million credit and debit card holders. The compromised data included card numbers, expiration dates and some but not all names of cardholders. To date, Heartland Payments Systems has paid out approximately $140 million in settlements, including over $100 million with Visa, MasterCard, American Express and Discover.

In terms of compromised records and individuals effected, the above noted data breach case is one of the largest on record although not representative in magnitude of the thousands that have been identified and tracked by various organizations in the past seven years. Entities in every type of general industry including business, education, government, healthcare and non-profit have suffered data breaches. The problem is that for many of the data breaches that are discovered are found at a point in time far beyond when they actually happened. In addition, most of the data breaches are not reported to consumers. As a result, identity theft incidents continue and victims suffer the consequences.

When a consumer or other entity becomes aware that personal information in electronic or paper format, including Social Security numbers, individual names, passwords, user names, bank account or other financial account numbers, email addresses or debit/credit card numbers etc. is compromised and exposed to risk of unauthorized use, a data or security breach has occurred. This may lead to identity theft which occurs when a criminal uses another person's personal information to commit fraud.

As of December 31, 2013, through their Consumer Sentinel Network Data Book, the Federal Trade Commission (FTC) has reported more than 9 million identity thefts, fraud and other complaints since 1997, which are collected directly from consumers, law enforcement agencies and other organizations on a voluntary basis. Many of these identity theft complaints are the result of data breaches. Based on their surveys the FTC estimates that the actual number of identity cases in the U.S. are greater than 10 million per year, most of which go unreported. (Federal Trade Commission, 2012).

## 1.1. Public awareness of data breaches

To create public awareness of data breaches, three major organizations in the United States track them throughout the year. They are the Privacy Rights Clearinghouse (PRCH), Verizon Business and the Identity Theft Resource Center and each of them use entirely different sources and methodologies to identify, collect, track, and classify data breaches according to types and industry and make their data available to the public in some type of annual or ongoing report. By comparing the data breach information in the reports allows business and criminal justice researchers, law enforcement officials, data managers in all profit and nonprofit organizations of all types and legislators in every country throughout the world to view the data breach problem from different perspectives. As a result, data managers and law enforcement personnel will be able to improve their development of strategies to enhance the protection of personal data of consumers, customers, clients and others and subsequently reduce identity theft. Because this article focuses on the classification of data breaches by industries, the classification of data breaches by types or causal factors will not be reported. *(See Privacy Rights Clearinghouse (PRCH).*

This organization is known as "A nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' *privacy rights* in public policy proceedings". From January 1, 2005 through December 31, 2013 they have compiled and reported more than 4000 data breaches and over 621 million related compromised records in their "Chronology of Data Breaches" document. (PRCH, 2013).The PRCH methodology currently classifies data breaches into industry sectors that include businesses -financial services, businesses – retail/merchant, businesses – other, government and military, nonprofit organizations, educational institutions and healthcare – medical provider. (Privacy Rights Clearinghouse, 2013).

*Verizon Business*. Since 2004 this organization's "Risk Team" has produced their annual "Data Breach Investigations Report" and through 2013 3 they have reported over 1.2 billion compromised records and thousands of data breaches included in their caseload. In 2011 alone they reported 855 data breaches and over 174 million compromised records. They currently classify data breaches into industry sectors that include accommodation and food services, retail trade, finance and insurance, healthcare and social assistance, information and other and other. (Verizon Business, 2013)

*Identity Theft Resource Center® (ITRC).* This is a "nonprofit, nationally respected organization dedicated exclusively to the understanding and prevention of identity theft". From January 1, 2005 and through December 31, 2013 3 the ITRC has reported well over 4200 data breaches and substantially more than 551 million compromised records. The ITRC classifies data breaches into five industry categories including business, banking/credit/financial/, educational, governmental/military and medical/health care. (Identity Theft Resource Center, 2013)

## 1.2. Holtfreter and Harrington data breach model

Continuing with the work provided by the three data breach reporting organizations noted above, the purpose of this study was to develop a new data breach model that classifies data breaches and their related compromised records by (1) different causal factors or types and (2) industry sectors.

The classification of data breaches by types of causal factors was the focus of the first part of the model and resulted in five internal, four external and one non-traceable categories. This was first reported in a recent article (Holtfreter & Harrington, 2012) where the annual total data breaches and compromised records for a six-year period for each of the categories were provided. Here are the types of data breaches identified in the study:

**Internal Breaches**

- Improper protection or disposal of data.
- Theft of data by a current or former employee with absolute or high probability of fraudulent intent.
- Theft of data by a current or former employee with low or no probability of fraudulent intent.
- Hacking or unauthorized intrusion of a network by a current or former employee.

**External Breaches**

- Partner/third party theft or loss of data by improper exposure or disposal.
- Theft of data by a non-employee with absolute or high probability of fraudulent intent.
- Theft of data by a non-employee with low or no probability of fraudulent intent.
- Hacking or unauthorized intrusion of a network by a non-employee.

**Non-traceable Breach**

- Unable to determine the data breach as internal or external**.**

External hackers have accounted for about 20 percent of the data breaches and approximately 59 percent of the compromised records compiled the Privacy Rights Clearinghouse from January 1, 2005 up until December 31, 2013. For an analysis of this data and the steps hackers take to carry out a data breach, see (Holtfreter and Harrington, 2014).

Two of the main problems caused by data breaches involve the cost to consumers when recovering from a data breach and the cost to an organization to recover from one. For an analysis of these costs as well as other general data breach problems see (Holtfreter & Harrington, 2011).

Although some states in the United States have passed data notification and data protection laws to help prevent consumers and organizations for data breaches and identity theft, the U.S. Congress has yet to do so. For an analysis of these legislative issues see (Holtfreter & Harrington, 2012). Although some non-U.S. countries have passed such laws, they weren't considered as part of this study.

The purpose of this article is twofold. We will (1) report on the second part of the development of the data breach classification model that expands the industry classifications created by the three reporting agencies noted above and (2) analyze the data breach trends for each general industry sector and related sub-sectors. This expansion process resulted in five general industry categories and eighteen related sub- sectors or industry categories. As such, the findings of this paper will complement and expand the findings of the previous fore-mentioned article and the three reporting agencies mentioned earlier in this paper.

## 2. Methodology

Five general industry categories and eighteen related sub-sectors or industry categories were identified after analyzing a random sample of 300 of the 2,280 data breaches and their 512,289,020 compromised records reported by the Privacy Rights Clearinghouse for the six-year period from 2005 through 2010. (Beth Givens, PRCH's director, granted us permission to use its data.)

The classification process was then completed by examining all of the 2,280 data breaches for the six-year period and placing them into five general industry categories, including "business", "government", "education", "healthcare" "nonprofit", and their following eighteen sub-sector categories, including nine for "business", five for "government", two for "education" and one each for" healthcare" and "nonprofit" . The cases included with each of the sub-sectors or industry categories noted below were taken from the PRCH "Chronology of Data Breaches.

**BFIN: Business finance – investments,** which mainly consists of asset and hedge fund

management and custodial and brokerage services. For example, it was reported on April 30, 2008 that a computer hacker broke into a database at Davidson Companies and obtained the names and Social Security numbers of virtually all of the company's 226,000 clients. The database also included information such as account numbers and balances.

**BFB: Business finance– banking,** which includes banks, credit unions, consumer finance, pay day loan and other financial companies involved in the lending of money and the issuance and processing of debit/credit bank cards. For example, on March 26, 2008 it was reported that the Bank of New York Mellon lost a box of computer data tapes storing personal information of 12.5 million name, Social security numbers and possibly bank account numbers.

**BFIS: Business finance– insurance,** which consists mainly of insurance underwriters, carriers, insurance agencies and brokerages involved in annuity, life, health, property/casualty retirement products. For example, on July 21, 2010 it was reported that Lincoln National Life Insurance company exposed personal information, including names, Social Security numbers, addresses, credit information etc., of 26,840 life insurance applicants on their web site after a vendor included the login information e.g. user names and passwords for agents and authorized brokers on a brochure that was posted on the agent's public website.

**BPS: Business – professional services**, which includes auditing, tax and legal services. For example, on July 30, 2010 First Advantage Tax Consulting Services reported that a laptop containing the Social Security numbers of 32,842 employees was lost or stolen during an airport layover.

**BM: Business – manufacturing,** which is most commonly applied to industrial production where raw materials and labor are transformed into finished goods. For example, it was reported on April 4, 2008 that Harley-Davidson determined that a laptop containing the names, addresses and credit card numbers of 60,000 of its members was missing.

**BR: Business – retail** or individuals and companies engaged in the selling of finished products to end consumers. For example, on September 15, 2008 debit and credit card information and, in some cases, expiration dates and other card information of 98,930 customers were hijacked from the retailer Forever21.

**BTM: Business – telecommunications/media,** which consists of all media technology companies including telephone, radio/TV, Internet, newspapers and film. For example, it was reported on February 23, 2007 it was reported that a laptop containing the personal information, including names, Social Security numbers etc., of 63,400 current and former employees was stolen from ADC Telecommunications.

**BH: Business – hospitality,** including lodging, restaurants, event planning, theme parks, transportation and cruise lines. For example, Starbuck's Corp reported that a laptop containing the names, addresses and Social Security numbers of 97,000 employees was stolen.

**BO: Business – other,** including all businesses not included in the other business sub-type categories. For example, on June 4, 2010 Digital River Inc. reported that hackers stole personal information personal information of 200,000 individuals.

**EHE: Education – higher,** which includes all post high school educational institutions. For example, on December 15, 2010 the Ohio State University said a hacker infiltrated their computer network and stole name, Social Security numbers and other personal information of 65,663 current students and 226,000 alumni.

**EK12: Education – K-12** or kindergarten through high school academic institutions. For example, on May 16, 2008 Chester County School District reported that a student gained access to files on a computer that contained personal information of more than 40,000 taxpayers and 15,000 students.

**GF: Government – federal,** including all agencies, excluding the military, funded by the Federal government. For example, it was reported November 6, 2009 that the National Archives & records Administration reported that it returned failed hard drives that contained personal information of 250,000 current employees and military veterans back to vendors rather than destroying them internally.

**GM: Government – military**, including all military agencies and installations funded by the Federal government**.** For example, on March 5, 2010 by the Arkansas Army National Guard that a hard drive containing the names, Social Security numbers and other personal information of 35,000 current and former members was missing.

**GS: Government – state,** which includes all non-educational entities funded by a state government. For example, on July 6, 2010 the Massachusetts Secretary of State Office improperly released the Social Security numbers and driver's license information of 139,000 investment advisors included on a CD-ROM to an investment industry publication called IA Week.

**GK: Government – county,** which includes all non-educational entities funded by a county government. For example, on April 4, 2010 it was reported that the Kern County Employee's Retirement Association convicted a former employee of using the Social Security number to create a fake identity of a member after gaining access to 37,000 records.

**GC: Government – city,** including all non-educational entities funded a city government. For example, on March 4, 2009 the New York police Department reported that a civilian employee stole eight tapes containing the Social Security numbers and direct deposit information of 80,000 current and retired cops.

**HC: Healthcare,** including doctors, nurses and other healthcare practitioners/professionals and physical facilities such as hospitals, medical clinics and pharmacies. For example, on April 26, 2005 the Lincoln Medical and Mental Health Center reported that multiple CD's containing personal medical information of 130,495 patients was lost in transit by FedEx and was never found.

**NP: Nonprofit**, which are formal organizations in the United States that qualify for tax-exempt status under the Internal Revenue Code. For example, a hard drive belonging to College-Invest, a not-for-profit division of the Colorado Department of Higher Education disappeared during a recent move and it contained the personal information of 200,000 customers.

## 2.1. Results

The results of this study and subsequent analysis will focus on the trends for (1) total 2,280 reported data breaches and (2) each of the five general industries and their eighteen sub-sectors over a six-year period from 2005 through 2010. Overall, as shown below, the results or findings indicate that although the trends for the annual number of data breaches for each of the five general industry categories and their eighteen sub-sector categories have increased over the years, the changes have been inconsistent from year to year.

*Data breach trend categories.*

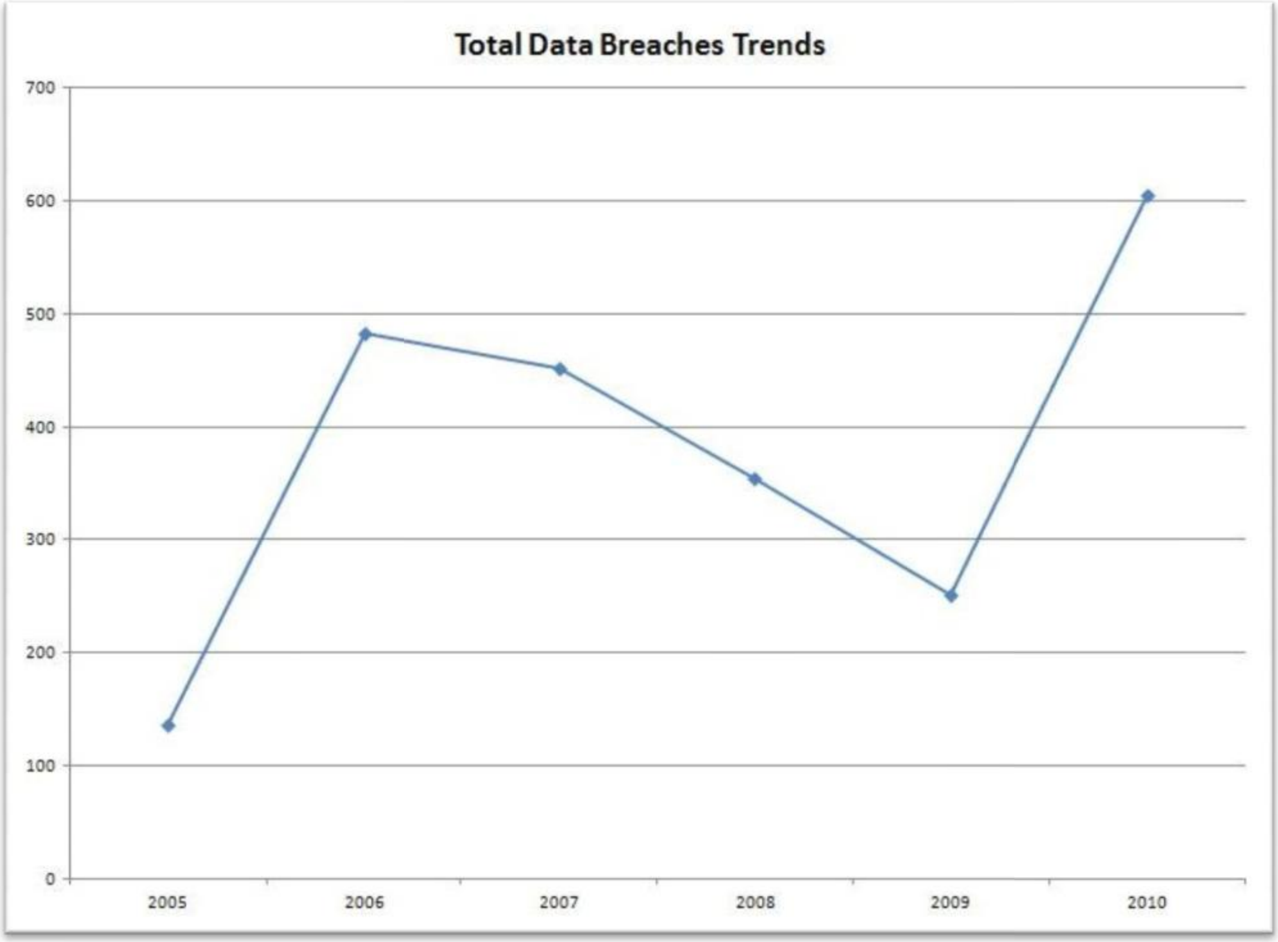


Figure1. Total Data Breaches Trend

In figure 1, Total Data Breaches –Trend, the trend for the total annual reported data breaches are shown. A total of 2,280 data breaches were reported for the six-year period. They started with their low point in 2005 when 136 were reported and then jumped to 482 in 2006 before beginning a downslide for three years with 451 reported in 2007 and 355 in 2008 and 251 in 2009 after which they hit their high point with 605 in 2010.

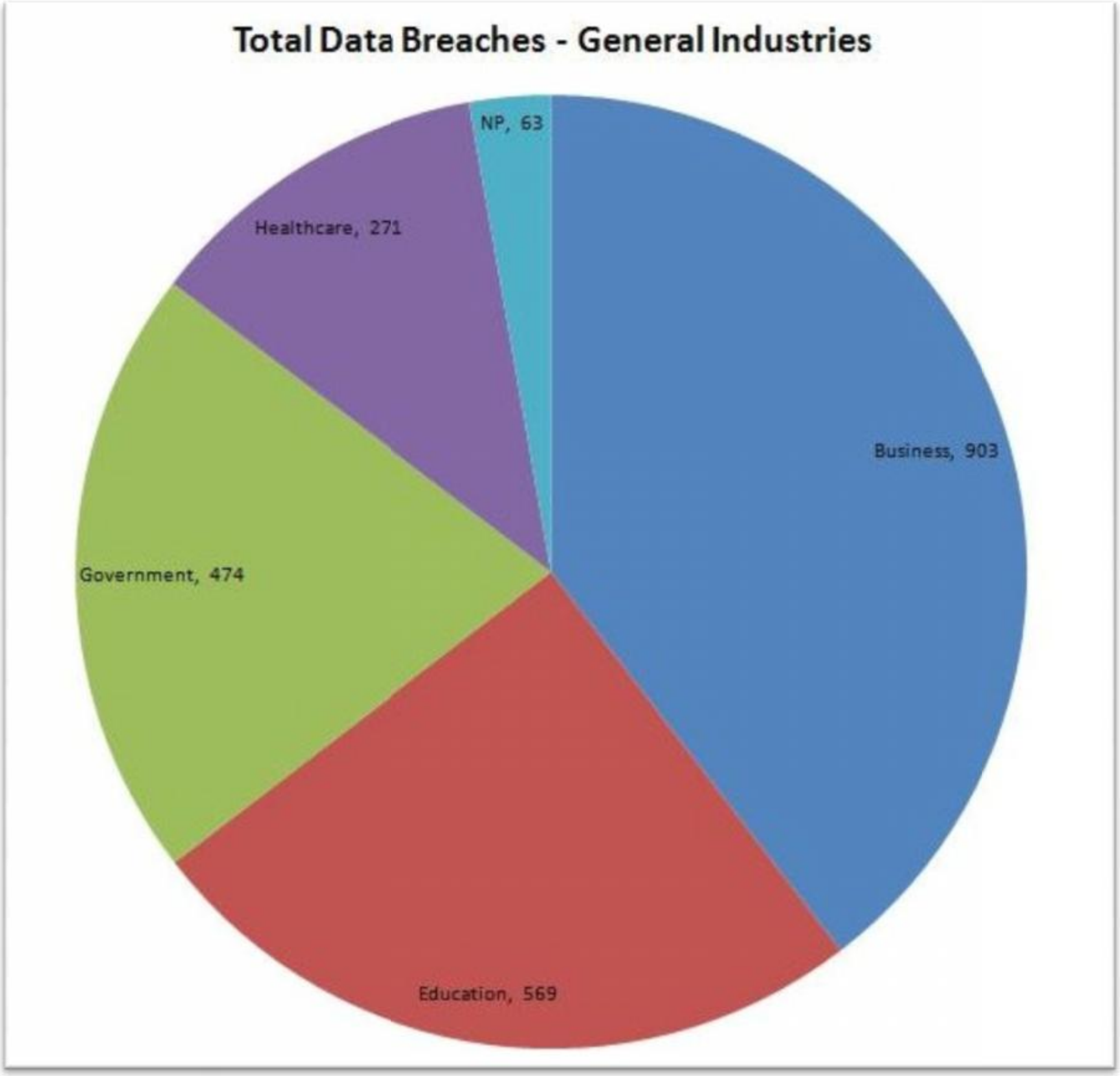
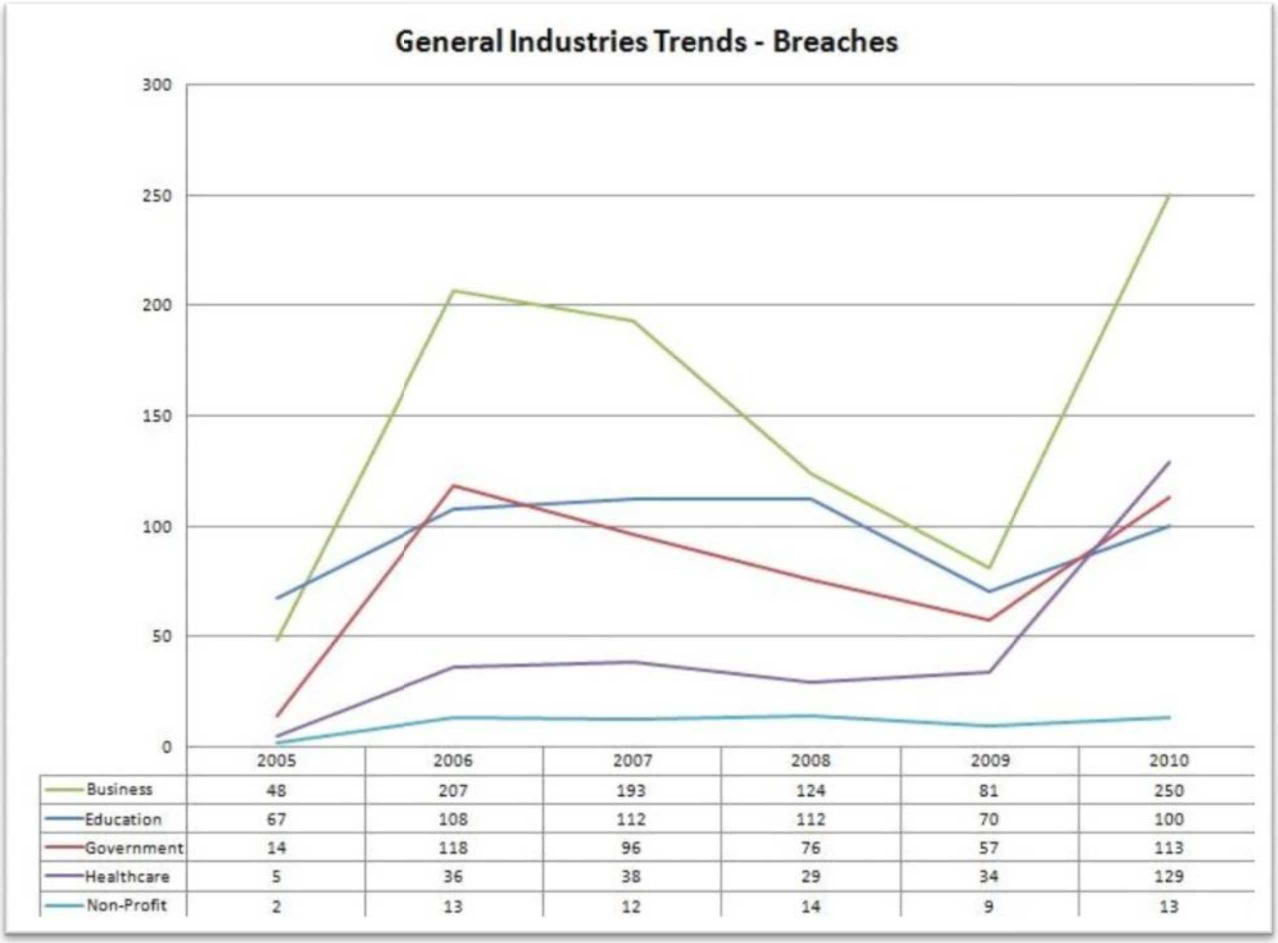


Figure 2. Total Data Breaches – General Industry Sectors

In Figure 2, Total Data Breaches – General Industry Sectors, it shows that for the 2,280 total data breaches reported for the six-year period, 903 were traced to the "business", 569 to "education", 474 to "government", 271 to "healthcare" and 63 to the "non-profit" general industry sectors.



| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| Business | 48 | 207 | 193 | 124 | 81 | 250 |
| Education | 67 | 108 | 112 | 112 | 70 | 100 |
| Government | 14 | 118 | 96 | 76 | 57 | 113 |
| Healthcare | 5 | 36 | 38 | 29 | 34 | 129 |
| Non-Profit | 2 | 13 | 12 | 14 | 9 | 13 |

Figure 3. General Industry Sectors – Data Breach Trends

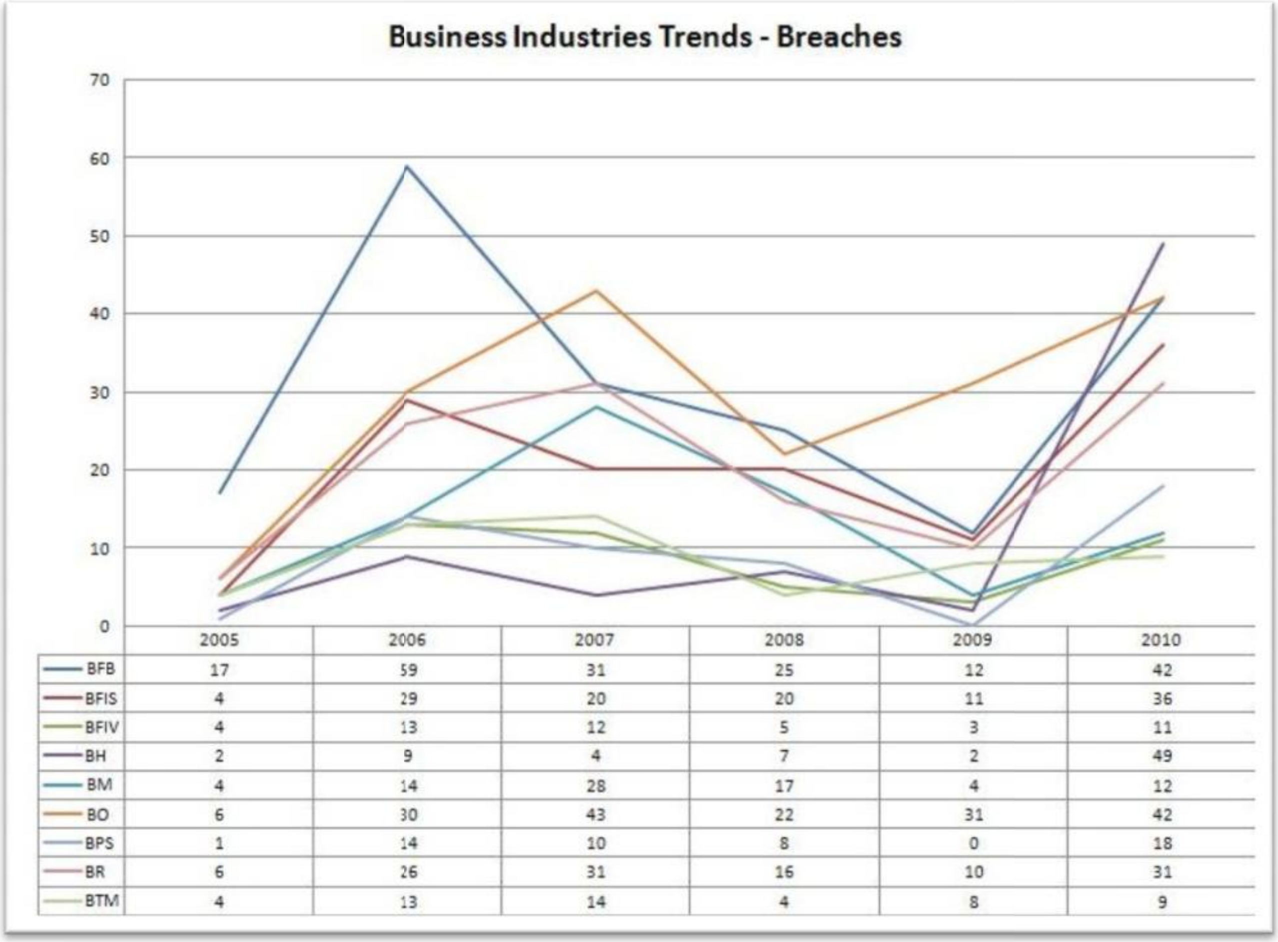
In Figure 3, General Industry Sectors –Data Breach Trends, the six-year trend for annual total data breaches for each of the five general industry sectors are shown and overall they closely resemble the trends for the annual total data breaches reported in Figure 1.The trend for the general "business" industry started with its low in 2005 with 48 data breaches reported, then leaped to 207 in 2006 before sliding down for three years with 193 in 2007, 124 in 2008 and 81 in 2009. They then jumped to their high in 2010 when 250 data breaches were reported.

The trend for the general "education" industry started with its low in 2005 with 67 reported data breaches and then they increased to 108 in 2006 and 112 in each of the years 2007 and 2008 before sliding down to 70 in 2009 and finished with its high in 2010 with 250 reported data breaches.

For the general "government" industry the trend started in 2005 with 14 data breaches reported, then rose up to 118 in 2006 before starting a three-year downslide with 96, 76 and 57 respectively for the years 2007 through 2009 after which they hit their high in 2010 with 113 reported data breaches.

The data breach trend for the general “healthcare”  industry started with 5 in 2005 and they increased to 36 in 2006 and 38 in 2007 at which time they went down to 29 in 2008 and climbed back up to 34 in 2009 before hitting their high point in 2010 with 129 data breaches.

The general “non-profit” industry  started off with its low in 2005 with 2 data breaches, climbed to 13 in 2006 before dipping down to 12 in 2007 but rose back up to 14 in 2008 before sliding back down to 9 in 2009 after which they hit their high point with 13 in 2010.



| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| BFB | 17 | 59 | 31 | 25 | 12 | 42 |
| BFIS | 4 | 29 | 20 | 20 | 11 | 36 |
| BFIV | 4 | 13 | 12 | 5 | 3 | 11 |
| BH | 2 | 9 | 4 | 7 | 2 | 49 |
| BM | 4 | 14 | 28 | 17 | 4 | 12 |
| BO | 6 | 30 | 43 | 22 | 31 | 42 |
| BPS | 1 | 14 | 10 | 8 | 0 | 18 |
| BR | 6 | 26 | 31 | 16 | 10 | 31 |
| BTM | 4 | 13 | 14 | 4 | 8 | 9 |

Figure 4. Business Industry Sectors – Data Breach Trends

In Figure 4, Business Industry Sectors - Data BreachTrends, the data breach trends for each of the nine “business” industry sub-sectors are shown.  The trend for the “business finance – banking” (BFB) sub-sector started with 17 data breaches in 2005 and then jumped its high point in with 59 in 2006 after which they declined for the years 2007, 2008 reaching their low point 2009 with 31, 25, and 12 respectively before climbing back up to their high point with 42 in 2010.

For the most part, the trend for the "business finance – insurance" (BFIS) sub-sector mirrored the trend for the "business finance – banking" sector noted above. It started at its lowest point with 4 data breaches in 2005 and then climbed to 29 in 2006 before declining again to 20 in each of the years 2007 and 2008 and 11 in 2009 after which they climbed to their peak with 36 in 2010.

The trend for the "business finance-investments" (BFV) sub-sector followed the "business finance – banking" sector exactly as it started with 4 data breaches in 2005 and climbed to its peak with 13 data breaches in 2006 before starting a three-year decline to its low point with 12, 5, and 3 in 2007, 2008 and 2009 respectively after which they went back up to 11 in 2010.

The data breach trend for the "business hospitality" (BH) sub-sector zigzagged by starting at its low point with 2 data breaches in 2005 then jumped to 9 in 2006 before going back down to 4 in 2007 after which they rose to 7 in 2008 and declined again to match their lowest level with 2 in 2009 before peaking with 49 in 2010.

The data breach trend for "business manufacturing" (BM) sub-sector started with its low point with 4 data breaches in 2005 before rising to 14 in 2006 and peaked with 28 in 2007 after which they started a two-year decline for years 2008 and 2009 with 17 and 4 data breaches respectively and went up from there with 12 in 2010.

The data breach trend for "business – professional services" (BPS) sub-sector opened with 1 in 2005 and then rose to 14 in 2006 before sliding downward to their low point with 10, 8 and 0 data breaches in the years 2007, 2008 and 2009 after which they climbed to its peak with 18 in 2010.

The data breach trend for "business – retail" (BR) sub-sector started with its low point with 6 data breaches in 2005 and then climbed in the years 2006 and 2007 with 26 and 31 respectively before declining to 16 in 2008 after which they rose again with 10 in 2009 before hitting its high point with 31 in 2010.

The trend for "business - telecommunications and media" sub- sector started with its low point with 4 data breaches in 2005 and then rose for the year 2006 and peaking in 2007 with 13 and 14 respectively after which they declined by matching their low point with 4 in 2008 before rising back with 8 and 9 in 2009 and 2010 respectively.

The data breach trend for the "business –other" sub-sector started its low point with 6 in 2005 and rose with 30 and 43 respectively in 2006 and 2007 before going down to 22 in 2008 after which they climbed back up to 31 in 2009 and then peaked with 42 in 2010.

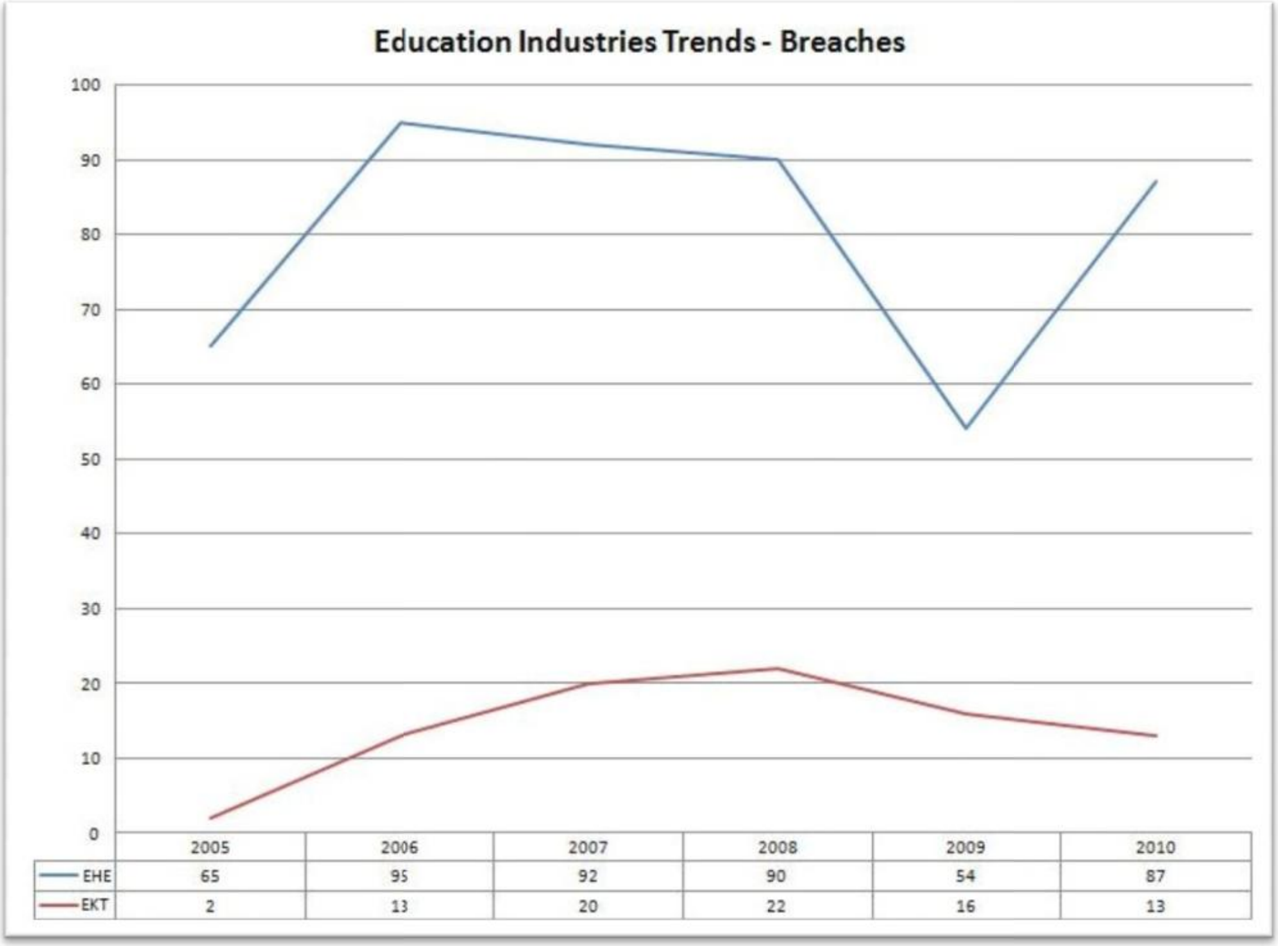
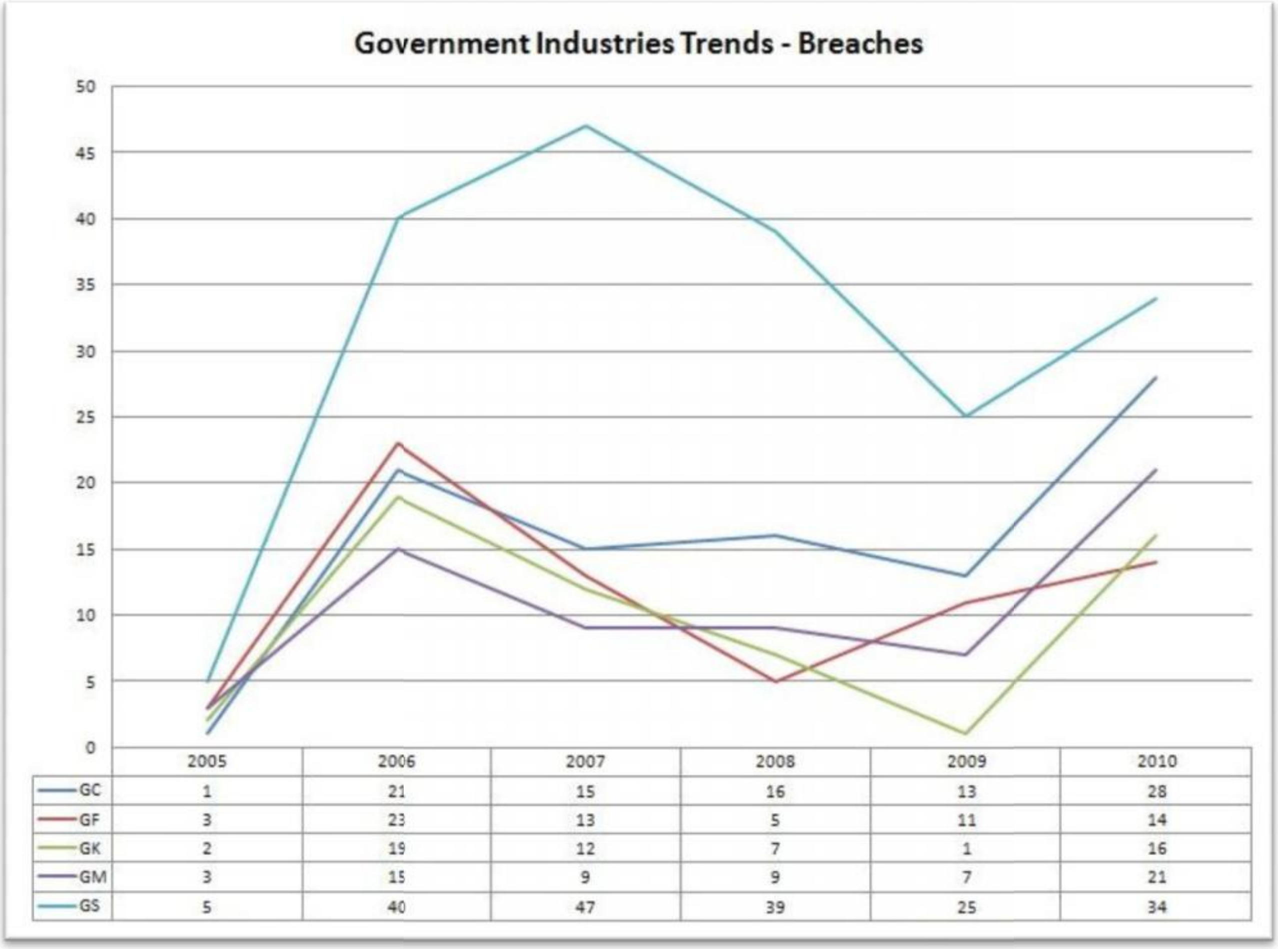


Figure 5. Education Industry Sub-sectors – Data Breach Trends

In Figure 5, Education Industry Sectors – Data Breach Trends, the data breach trends for the two general "education" industry sub-sectors are shown. The trend for the "education – higher ed" industry sub-sector started with 65 data breaches in 2005 and then rose to their high point in 2006 with 95 before falling in the years 2007 and 2008 with 92 and 90 and then falling again to their low point in 2009 with 54 after which they climbed up to 87 in 2010.

The data breach trend for the "education – K-12" industry sub-sector started with its low of 2 in 2005 and then climbed upward for the years 2006, 2007 with 13 and 20 data breaches respectively at which point they went up again to their peak in 2008 with 22 and proceeded downward for the years 2009 and 2010 with 16 and 13 data braches accordingly.



| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| GC | 1 | 21 | 15 | 16 | 13 | 28 |
| GF | 3 | 23 | 13 | 5 | 11 | 14 |
| GK | 2 | 19 | 12 | 7 | 1 | 16 |
| GM | 3 | 15 | 9 | 9 | 7 | 21 |
| GS | 5 | 40 | 47 | 39 | 25 | 34 |

Figure 6. Government Industry Sub-sectors – Data Breach Trends

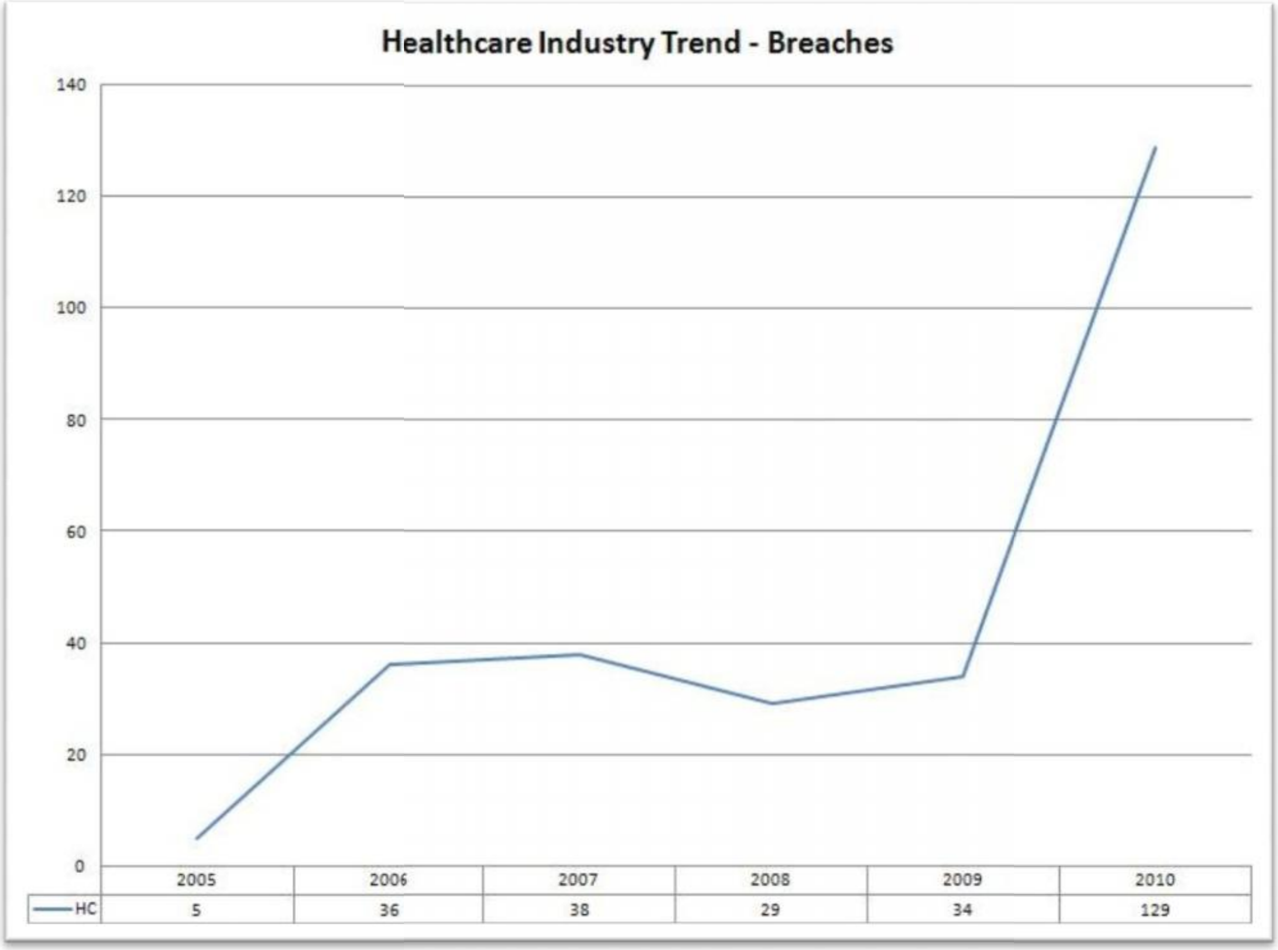
In Figure 6, Government Industry Sectors – Data Breach Trends, the data breach trends for each of the five “government” industry sub-sectors are shown. The data breach trend for the “government - military” (GM) sector started with its low of 3 in 2005 and then rose to 15 in 2006 before registering 9 in each of the years 2007 and 2008 after which they moved to 7 in 2009 before climbing back to their high with 21 in 2010.

The trend for the “government – federal” (GF) sub-sector started with its low of 3 data breaches in 2005 after which they rose to their high point in 2006 with 23 before sliding down to 13 and 5 for the years 2007 and 2008 before moving back up with 11 data breaches in 2009 and 14 data breaches in 2010.

For the subtype “government – state level” (GS) sub-sector the trend started with 5 data breaches in 2005 and then went up to 40 in 2006 before continuing to their high point in 2007 with 47 and then slide down to 39 in 2008 and 25 in 2009 and then finished with 34 in 2010.

The data breach trend for the “government – county” (GK) sub-sector initiated its’ trend with 2 breaches in 2005, jumped to its’ peak in 2006 with 19 data breaches before starting a downward trend for the years 2007, 2008 and 2009 with 12, 7 and 1 (their low point) and then went back up to 16 in 2010.

For the “government – city” (GC) sub-sector the trend zigzagged starting with its low point with 1 data breach in 2005 and then rose to 21 in 2006 before going back down to 15 in 2007 and then back up to 16 in 2008 after which they slid down to 13 in 2009 and finished up to their high point with 28 in 2010.



| | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---|---|---|---|---|---|---|
| HC | 5 | 36 | 38 | 29 | 34 | 129 |

Figure 7. Healthcare Industry Data Breach Trend

In Figure 7, Healthcare Industry Data Breach Trend, the trend for the "healthcare" industry is shown. It started with a low point in 2005 with 5 data breaches and then moved up for the years 2006 and 2007 with 36 and 38 respectively before rising to 36 and 38 in the years 2006 and 2007 before going down to 29 in 2008 after which they went up to 34 in 2009 and then peaked with 129 in 2010.

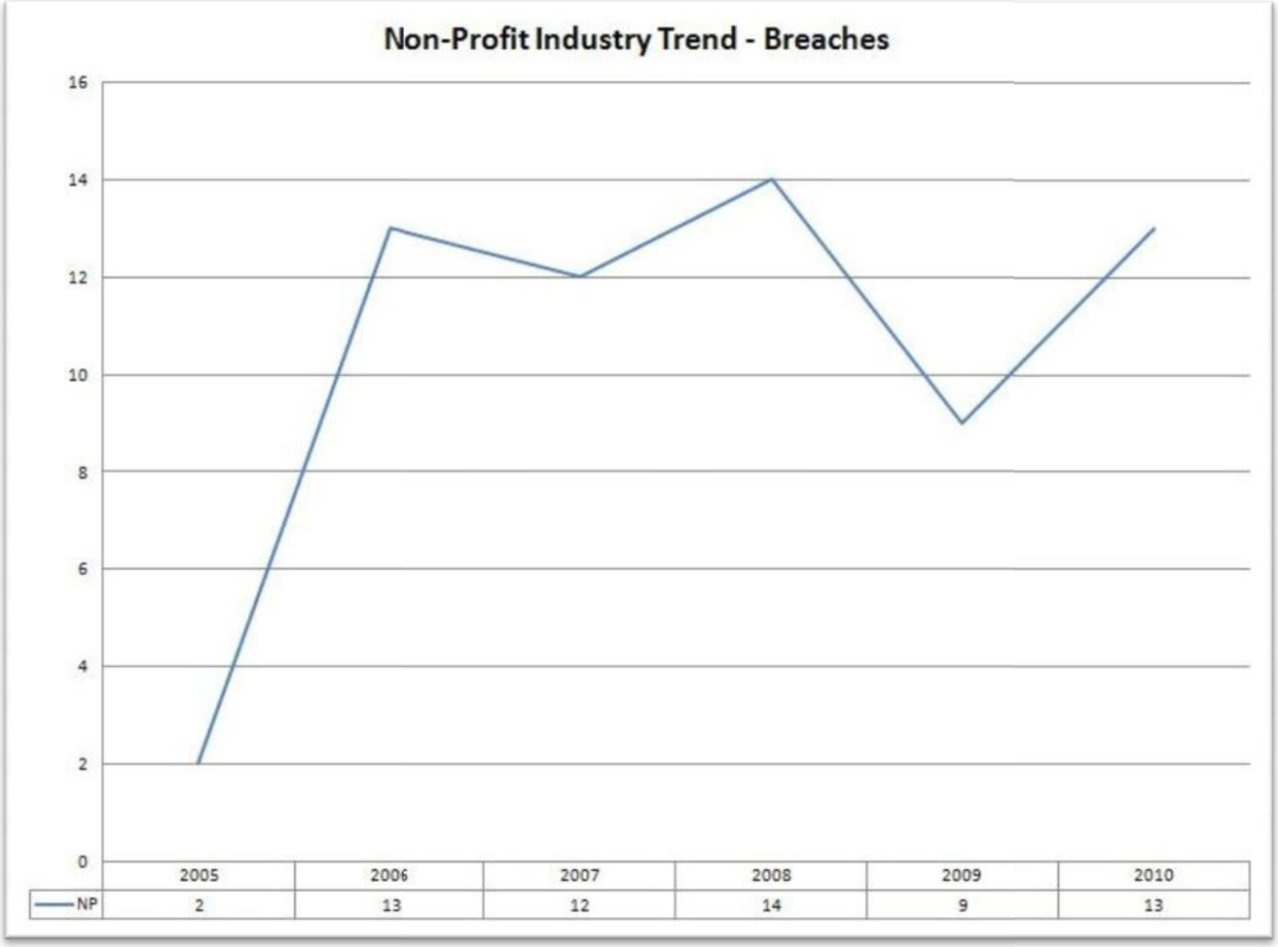


Figure 8. Non-Profit Industry Data Breach Trend

In Figure 8, Non-Profit Industry Data Breach Trend, the data breach trend for the "non-profit" (HC) industry is shown. Like most of the other general industries, the trend started in 2005 with its low point of 2 data breaches and zigzagged back and forth with 13 in 2006 and 12 in 2007 before peaking in 2008 with 14 at which point they went down again with 9 in 2009 before finishing with 13 in 2010.

## 2.2. Analysis

Information managers and security personnel in all public and private organizations should be concerned because it is obvious from the results of this study that data breaches are common to all the industry sectors examined in this study. The results show that the data breach trends for most of the industry sectors mirror the data breach trend for the total data breaches but in some cases they are inconsistent. Approximately forty percent of the data breaches were incurred by the general business industry with about twenty-five percent traced to the general education industry. The healthcare, nonprofit and government industries accounted for the rest of the data breaches. The banking/finance sectors are getting hit the hardest as they incurred approximately fifty-five percent of the general business industry's data breaches. This is because fraudsters go where the money is and, as a result, the banking/ finance sectors are ripe for exploitation.

The situation is much worse than indicated because the data breaches analyzed in this study represent only a very small but representative sample of the actual data breaches incurred according to the Privacy Rights Clearinghouse. This is because most organizations that incur a data breach are reluctant to report it and take advantage of loopholes in State data notification laws in the United States that allow them to opt out. Fortunately the data breach reporting organizations mentioned in this article gain access to unreported data breaches from outside sources that discover them. As a result, they then become public information.

Data breaches are caused by a variety of internal and external causal factors. Internal and external hackers represent a major common threat. In addition, current and former employees are a constant threat as they as well as third party contractors, e.g. outside auditors/lawyers etc. or those who are giving the responsibility to dispose of it properly, because they all have access to data records containing sensitive personal information and are entrusted to use it in a professional capacity. Thus, all parties with access to data records run the risk of it being stolen or lost accidently if it is not properly protected.

## 3. Recommendations

Avoiding a data breach is a tremendous challenge and many organizations in every industry have accomplished this feat but again, as this study has shown, many haven't. The successful organizations have separated themselves form others by putting in place educational programs for their employees, third party contractors, customers/clients and others that have included basic data security policies that help to properly manage and safeguard sensitive personal information. The following basic security measures and guidelines, although not comprehensive in scope, are some examples that represent a starting point for information managers and security specialists to consider for reducing the risk of a data breach and, thus, help to protect public information.

Employees should be required to complete a security awareness program that outlines the various internal and external threats to the network and personal information records.

Terminated employees should be required to turn in any records or devices containing personal data. Data on all devices should be safeguarded with the use of current encryption standards.

Employees should be required to use complex passwords for all their devices and change them at proper intervals.

If data is transported by employees off of the facilities extra precautions should be put in place to protect it especially if it is being moved in portable devices like a laptop, smart phone or tablet.

Third party contractors should be screened and be required to take part in a security awareness program. Background criminal checks should be required of those with unknown reputations. Up-to-date firewalls and virus software should be utilized.

Employees and third party contractors should be required to inform the organization if data records in their possession are lost or stolen. Restrict the entry of individuals into the data center to those with the proper credentials.

## 4. Conclusions

The data breach trends reported in this study strongly indicate that organizations in every type of industry are experiencing serious long-term problems with data breaches and are giving up millions of compromised records in the process. As mentioned earlier in this paper, the Privacy Rights Clearinghouse has discovered and tracked more than 4,000 data breaches and over 621 million compromised records from January 1, 2005 through December 31, 2013 and they mention on their web site that this is a small fraction of the actual activity that is occurring. The two other data breach organizations mentioned in this study echo the results of the Privacy Rights Clearinghouse. This helps to explain why identity theft complaints account for over 30 percent of the total identity theft and fraud complaints reported by the Federal Trade Commission every year.

Organizations in the private and public sectors need to step up to the plate and develop a comprehensive data protection plan to protect the personal data of their customer, clients and employees. The recommendations provided in this paper represent a starting point that should lead to positive improvements. If this can be accomplished then the effect on reducing identity theft throughout the world will occur.

# References

Federal Trade commission (2014), “Consumer Sentinel Network Data Book”, available at

http://www.ftc.gov/opa/2014402/2013complaints.shtm *accessed on February 14, 204.*

Holtfreter, R. & Harrington, A. (2012), “Breaking Breach Secrecy, Part 3”, Fraud Magazine, Vol. 27, No. 1, pp. 40-50.

Holtfreter, R. & Harrington, A. (2011), “Breaking Breach Secrecy, Part 1 – Corporations Need to Publicize  Breaches”, Fraud Magazine, Volume 25, No. 5, September/October, 2011.

Holtfreter, R. & Harrington, A. (2012), “Breaking Breach Secrecy, Part 2 - Gauging the Effectiveness of Data Breach Notification Legislation” Fraud Magazine, Volume 25, No. 6, November/December, 2011.

Identity Theft Resource Center® (ITRC, “Data Breaches”, available at www.idtheftcenter.org.

Privacy Rights Clearinghouse (2014), “Chronology of Data Breaches”, Privacy Rights Clearinghouse, available at http://www.privacyrights.org/data-breach.

Verizon Business (2014), “Data Breach Investigations Report”, available at www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2014_en_xg.pdf, *accessed on* December 31, 2013.

Holtfreter, R. & Harrington, A. (2014), “Will Hackers Win The Battle?”, Strategic Finance, January, 2014