NAVIGANT

Information Security & Data Breach Report

March 2011 Update

DISPUTES & INVESTIGATIONS • ECONOMICS • FINANCIAL ADVISORY • MANAGEMENT CONSULTING

A recent headline entitled "Feds Probe '100 site' Data Breach" highlighted a data breach involving McDonald's, deviantART and Walgreen's.[1] All of these companies, according to media reports, were clients of Silverpop, an Atlanta based email marketing firm. deviantArt, the largest online community for artists, had 13 million records breached, including email addresses, user names and birth dates. The Federal Bureau of Investigation (FBI) is still reviewing the scope and extent of this cyber crime. The size of this data breach alone underscores the importance of maintaining both electronic and physical records in a secure manner. Understanding the various breaches affecting companies, healthcare organizations, educational institutions and government entities is vital intelligence for organizations of all types.

Navigant is pleased to release the inaugural issue of the Information Security and Data Breach Report. This report is designed to keep the legal community apprised of new data breaches, spotlight notable breaches, and identify trends and other major changes taking place in the information security arena. The primary goal of this publication is to answer the following principal questions:

1. What is the total number of breaches per quarter?
2. Which types of entities are experiencing breaches?
3. What is the average number of days between discovery and disclosure of a data breach?
4. What types of data are being compromised?
5. What is the average number of records per breach?
6. How are records being breached?
7. What is the average total cost of a data breach?

METHODOLOGY USED FOR IDENTIFYING DATA BREACHES

Navigant has captured all major data breaches disclosed publicly during the third and fourth quarters of 2010 (July 1, 2010 – December 31, 2010).

DATA BREACH DASHBOARD

- Healthcare entities accounted for the largest percentage (Q3: 57% vs. Q4: 42%) of data breaches in either quarter.
- There was a 38% increase in the number of records breached from quarter to quarter (Q3: 2,083,742 million records vs. Q4: 2,881,360 million records)
- The average number of days between discovery and disclosure varied widely by type of entity. Corporate was unchanged at 47 days while Healthcare entities decreased from 57 days in Q3 to 51 days in Q4. Alternatively, Education and "Other" entities saw increases from 23 to 42 days and 10 to 18 days, respectively.
- The average number of records breached per incident jumped 105% from quarter to quarter (Q3: 27,062 vs. Q4: 55,411).
- Theft and Public Access/Distribution accounted for roughly half of all types of data breaches that occurred in either Q3 or Q4.
- The average total cost of a data breach, according to Navigant's analysis, increased from $5.5 million in Q3 to over $11.3 million in Q4.[2]

We evaluated major websites, blogs, government sources and news articles to compile a list of breaches that took place in the United States involving a minimum of 1,000 exposed or potentially exposed records. The incidents identified in this report involve breaches in which physical records were stolen, lost, improperly disposed of or distributed and those in which electronic records were hacked, lost, stolen or improperly exposed.

1. WHAT IS THE TOTAL NUMBER OF BREACHES PER QUARTER?

We identified 52 major data breaches in the Q4 compared to 77 in the previous quarter, representing a 32% decrease between reporting periods. The total number of individual records breached in the Q3 was 2,083,742. Q4 saw 2,881,360 records breached, a 38% increase from quarter to quarter. Seven out of ten of the largest breaches took place in the fourth quarter, all involving educational institutions.

One of the largest data breaches identified in the second half of 2010 took place at a prominent Midwestern university, where one of its computer servers was hacked. The server in question stored 760,000 records of current and former faculty, staff members, student and applicants. The hacked data contained names, Social Security numbers, dates of birth and addresses. The university discovered the breach in early October 2010 as part of a routine security review but did not notify those impacted until December 15, 2010. No explanation was provided as to why it took almost two months for the disclosure to take place. The university, according to news reports, is spending several million dollars for a forensic investigation and providing free credit monitoring to those affected.

2. WHICH TYPES OF ENTITIES ARE EXPERIENCING BREACHES?

The types of organizations that experienced a data breach, for purposes of this report, are divided into five main categories including Healthcare, Corporate, Education, Government and "Other".[3] These designations provide an accurate overview of the organizations that experienced a physical or electronic records breach.

Healthcare related entities, across both quarters, accounted for the majority of all breaches identified in this report.

- Healthcare entities, in Q4, experienced 42% of the data breaches identified, followed by Education (21%), Government (17%), Corporate (16%) and "Other" (4%) *(see Figure 1).*
- In Q3, Healthcare entities, accounted for roughly 57% of all breaches tracked, followed by Education (16%), Corporate (16%), Government (13%) and "Other" (4%) *(see Figure 2).*

A notable data breach occurred at a nonprofit charitable hospital based in the northeastern U.S. The data breach included roughly 800,000 records, on backup tapes that were shipped to a third-party vendor for disposal in February 2010. The tapes were not confirmed missing until June 2010. There

FIGURE 1: Q4 2010 BREACHES BY TYPE OF ENTITY

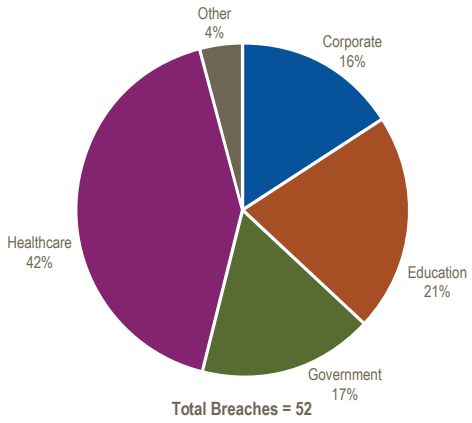
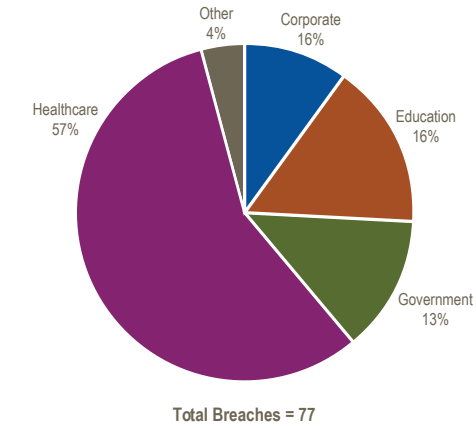


FIGURE 2: Q3 2010 BREACHES BY TYPE OF ENTITY

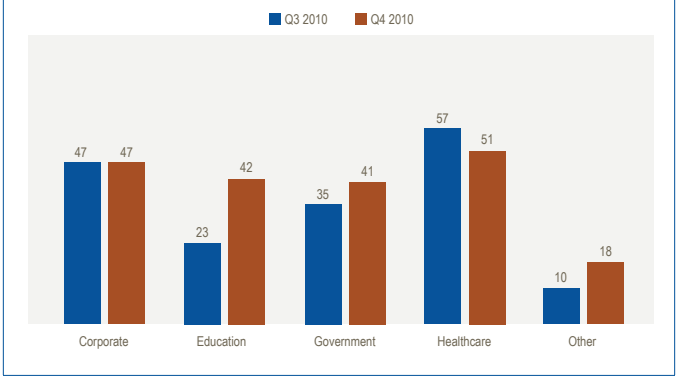


is no indication, based on a review of public information, what contributed or caused the delay in discovery time. The breached records in question were not encrypted and contained patient and financial information.

3. WHAT IS THE AVERAGE NUMBER OF DAYS BETWEEN DISCOVERY AND DISCLOSURE OF A DATA BREACH?

The danger of identity theft and increases in regulatory mandates have elevated the importance of timely response and disclosure after the discovery of a data breach. Discovery usually takes place when either electronic or physical records are confirmed to be lost or stolen or data is otherwise identified as compromised. Disclosure can be made through notification to those affected by the data breach or to a regulatory agency; or news of the breach can be disclosed by the media through websites, blogs and traditional news sources. Some states, such as Florida, Wisconsin and Ohio, have a 45-day notification rule. Several other states are considering similar measures. The changing regulatory landscape mandating the disclosure of a data breach beyond personal health information has led

FIGURE 3: AVERAGE DAYS BETWEEN DISCOVERY AND DISCLOSURE BY TYPE OF ENTITY



Navigant to track this metric using public sources, news and government websites. The average number of days between discovery and disclosure for all breaches was 45 days in Q4 compared to 46 days in Q3.

Navigant has also tracked the average number of days between discovery and disclosure by entity *(see Figure 3)*.

- Between Q3 and Q4, Corporate entities were unchanged in the average number of days between discovery and disclosure at 47 days.
- Healthcare entities saw a decrease between discovery and disclosure from 57 days in Q3 to 51 days in Q4.
- The number of days between discovery and disclosure for Government entities was 35 days in Q3 versus 41 days in Q4.
- "Other" entities increased 80% from quarter to quarter (Q3: 10 days vs. Q4: 18 days)
- Education entities, similarly, had an 82% increase between discovery and disclosure from 23 days in Q3 to 42 days in Q4.

The significant increase in time between discovery and disclosure for Education entities can be largely attributed to a single breach. According to news reports, over 3,000 records that contained Social Security numbers of students, faculty, staff and alumni were located on a publicly searchable server at a small college in New Mexico. The college was alerted to the breach in January 2010 but public disclosure did not occur until October, some 271 days later. There is no indication, from a review of public sources, that the college has taken any steps to increase the security of its records or notify those affected.

Currently both federal and state authorities require entities that hold personal health information to disclose when a data breach has occurred. The Department of Health & Human Services (DHHS) issued data breach regulations in August 2009. Similar breach notification regulations were issued by the Federal Trade Commission (FTC). As part of directives under the Health Information Technology for Economic and Clinical Health (HITECH) Act, both DHHS and FTC require HIPAA-covered entities to provide notification following a breach of unsecured protected health

information no later than 60 days following the incident.[4] Our analysis, using public sources, shows that the average number of days between discovery and disclosure for medical records in Q4 was 55 days, an increase of four days from the previous quarter.

4. WHAT TYPES OF DATA ARE BEING COMPROMISED?

The types of data being compromised range from personal identifiable information (PII) such as date of birth, name or Social Security number to financial information such as bank accounts or credit card numbers. We identified several categories of data commonly at risk in data breaches *(see Figure 4)* including: Name, Contact Information, Social Security Number (SSN), Date of Birth (DOB), Medical, Credit Card, E-Mail, Financial and Miscellaneous. Many of the incidents identified in this report have multiple types of data associated with each breach. Names, Contact Information and Social Security Number were part of the records breached in over 50% of the reported incidents in both quarters..

A laptop computer, according to a state university in Florida, was stolen from an employee's rental car in San Francisco, CA. The laptop contained 8,300 records of current and former students as well as employee information dating back to the year 2000. These records included Social Security numbers, Florida driver's license numbers, employee payroll identification numbers and, potentially, contact information. In response, the university sent letters to those affected and installed encryption software on all laptops that contain confidential data.

5. WHAT IS THE AVERAGE NUMBER OF RECORDS PER BREACH?

Navigant has endeavored to calculate the overall average number of records per breach as well as the average number of records per breach by type of entity *(see Figure 5)*. Our calculations revealed that the average number of records per breach was 105% higher in Q4 than the previous quarter (Q3: 27,062 vs. Q4: 55,411).

- The average number of records per breach for Corporate entities was 100,304 records in Q4 versus 21,746 records in Q3.
- Education entities saw a 372% increase from 31,096 records in Q3 to 146,900 records in Q4.
- The average number of records per breach remained unchanged from Q3 to Q4 for Government entities.
- Healthcare entities, on the other hand, experienced a significant decline in the average number of records per breach from 26,146 records in Q3 to 3,899 records in Q4.
- The final category, "Other" entities, saw a large increase in the average number of records per breach from 9,604 records in Q3 to 22,800 records in Q4.

6. HOW ARE RECORDS BEING BREACHED?

We also tracked the methods by which records are breached and organized them into seven major categories. These categories include Virus, Hack, Loss, Theft, Public Access/Distribution, Unauthorized Access/Use or Improper.[5] In Q4 *(see Figure 6),* the most common methods used to breach data were:

- Theft (29%)
- Public Access/Distribution (28%)
- Hack (15%)
- Loss (11%)
- Improper Disposal (7%)
- Unauthorized Access/Use (7%)

FIGURE 4: BREACHES BY TYPE OF INFORMATION

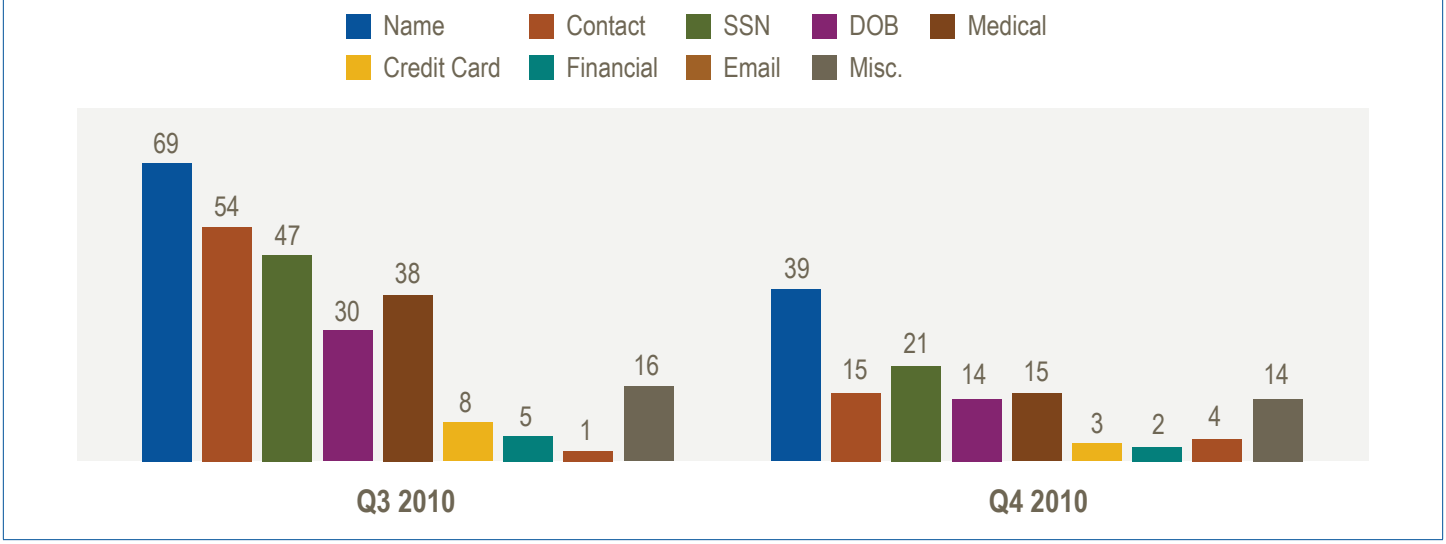


FIGURE 5: AVERAGE RECORDS PER BREACH BY TYPE OF ENTITY

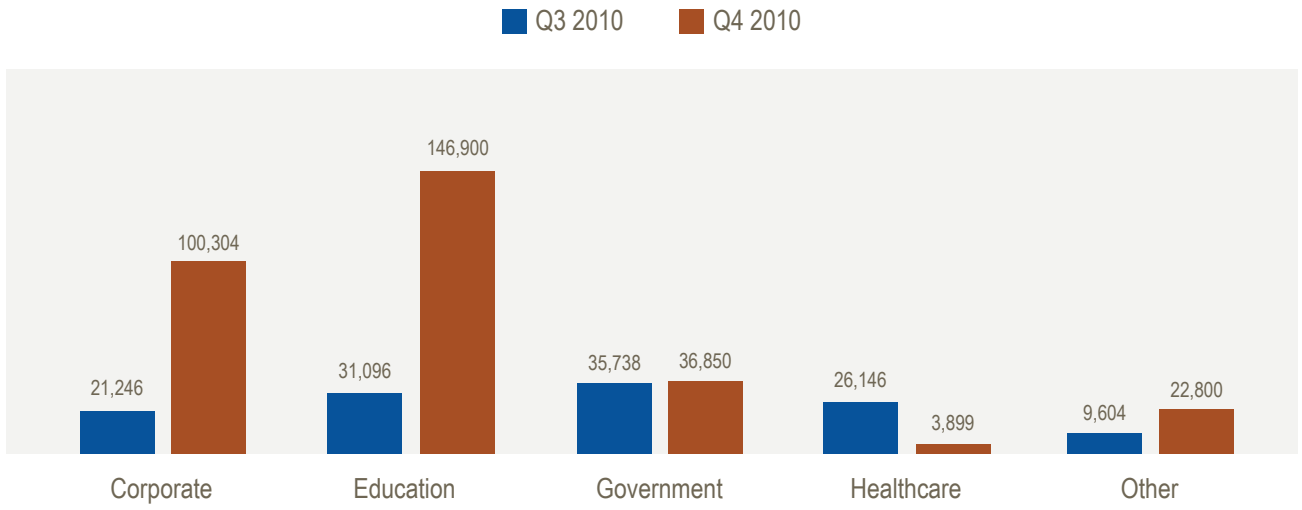


FIGURE 6: Q4 2010 BREACHES BY TYPE OF METHOD

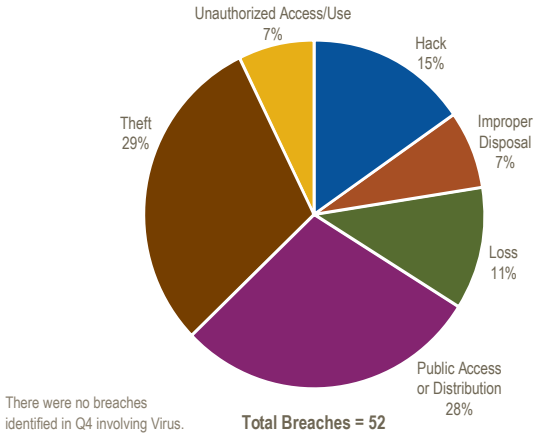
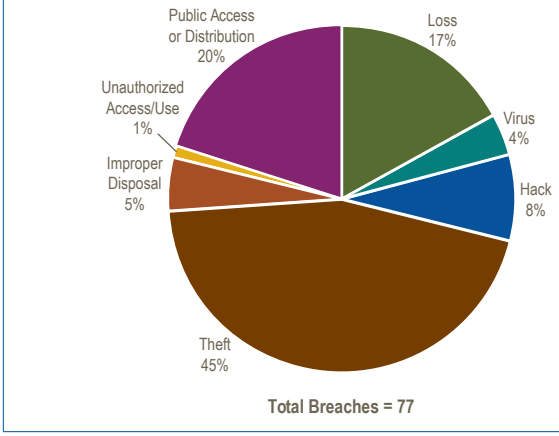


FIGURE 7: Q3 2010 BREACHES BY TYPE OF METHOD



The third quarter *(see Figure 7)* had a much different break-out. Theft was the most common type of breach (45%) followed by Public Access/ Distribution (20%), Loss (17%), Hack (8%), Improper Disposal (5%), Virus (4%) and Unauthorized Access/Use (1%).

Looking at the data by method of breach and type of entity we identified some interesting statistics:

» 38% of Corporate breaches in Q4 were Unauthorized Access/Use incidents. 45% of breaches involving Education and Government entities in Q4 2010 were accomplished through Public Access/Distribution. This type of breach usually takes places when records are made publicly accessible via a server or website.

» In Q3, 50% of both Corporate and Government breaches involved Public Access/Distribution.

» Theft was the method of breach in 60% of incidents involving Healthcare entities in both quarters.

A data breach involving the theft of patient records took place at a Los Angeles, CA based ambulatory care center. The facility discovered that 14 boxes of patient records were missing and presumed stolen. The boxes contained the following demographic information: name, address, date of birth, medical record number, finance batch number and gender of the patients. The 33,000 patient records were from January – October 2008. An investigation by the Los Angeles County Sheriff Department determined that a janitor had illegally removed the records and sold them to a paper recycling center for $40.

We also tracked the format of records being breached as part of this report. The format of records being breached falls into three main categories: physical, electronic or a combination of both. Electronic records may be

accessed via CD-ROM, laptop, thumb drive, other media devices, e-mail, website or server. In Q4, 82% of identified breaches were comprised of electronic records and 18% were comprised of physical records. Q3 saw electronic records account for 87% of the breaches while 13% represented physical records. No breaches identified in either the quarter, based on a review of public sources, had a combination of both types of records.

7. WHAT IS THE AVERAGE TOTAL COST OF A DATA BREACH?

One of the most important questions being asked concerns the total cost to the entities involved in a data breach. One of the foremost studies on this issue was published by the Ponemon Institute. The most recent study entitled 2009 Annual Study: Cost of a Data Breach provides some statistics on the total costs of a data breach.[6] For purposes of this quarterly report we identified the average total cost of a data breach by type of entity and type of breach.

A tour company's website was recently hacked using a SQL injection attack. The hackers were able to access 110,000 records with names, addresses, e-mail addresses, credit card numbers and the security code. The total cost of this data breach, using the Ponemon Institute study estimates, might be as high as $22.4 million. These costs include detection, discovery, notification, potential legal costs, ex-post costs and loss of customers and/or brand damage. The hack, according to news reports, took place in late September 2010 but was not detected until a month later when a web programmer for the company discovered the unauthorized script. As a result of this data breach, the tour company has sent out notifications, installed an application firewall on its servers and limited future access to its servers.

Based on our calculation, the average total cost of a data breach in Q4 was $11,303,797 versus $5,520,563 in Q3, a 105% increase from quarter to quarter. Some notable results from the average total cost of a data breach by entity were identified as part of this report *(see Figure 8).*

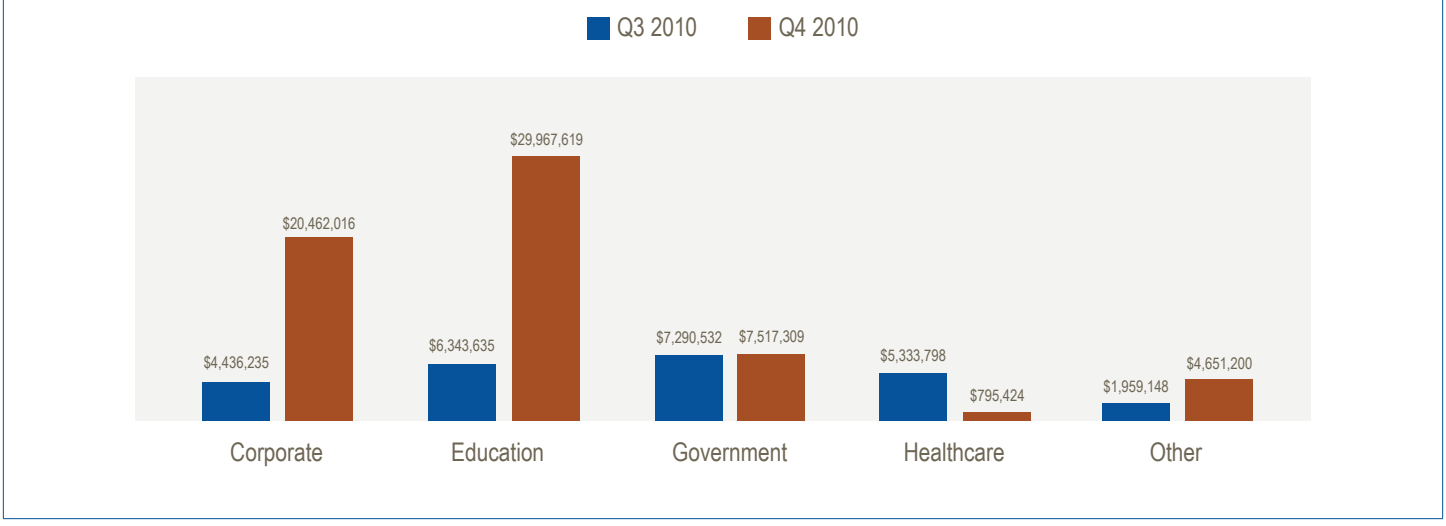
- Government ($7,517,309), Healthcare ($795,424) and "Other" ($4,651,200) entities in the fourth quarter were well below the average total cost in Q4.
- Both Education ($29,967,619) and Corporate ($20,462,016) entities, in Q4, were well above the average total cost of a data breach by type of entity.
- In Q3, Corporate ($4,436,235), Healthcare ($5,333,798) and "Other" ($1,959,148) entities were below the average total cost of $5.5 million.
- Both Education and Government entities were above the average total cost of a data breach in Q3 by 15% and 32% respectively.

The average total cost of a data breach varied widely by type of entity between quarters.

- Corporate, Education and "Other" entities had large increases from quarter to quarter.
- Education entities logged the largest change in the average total cost of a data breach from $6.3 million to over $29.9 million, a 372% increase.
- Corporate entities, similarly, saw the average cost of a data breach increase over 360% from $4.4 million to over $20 million.
- "Other" entities, compared to Education and Corporate organizations, showed a 137% increase from quarter to quarter.
- Government entities remained largely unchanged between quarters (Q3: $7,290,532 vs. Q4: $7,517,309).
- Healthcare, on the other hand, posted an 85% decrease from $5.3 million to $795,000.

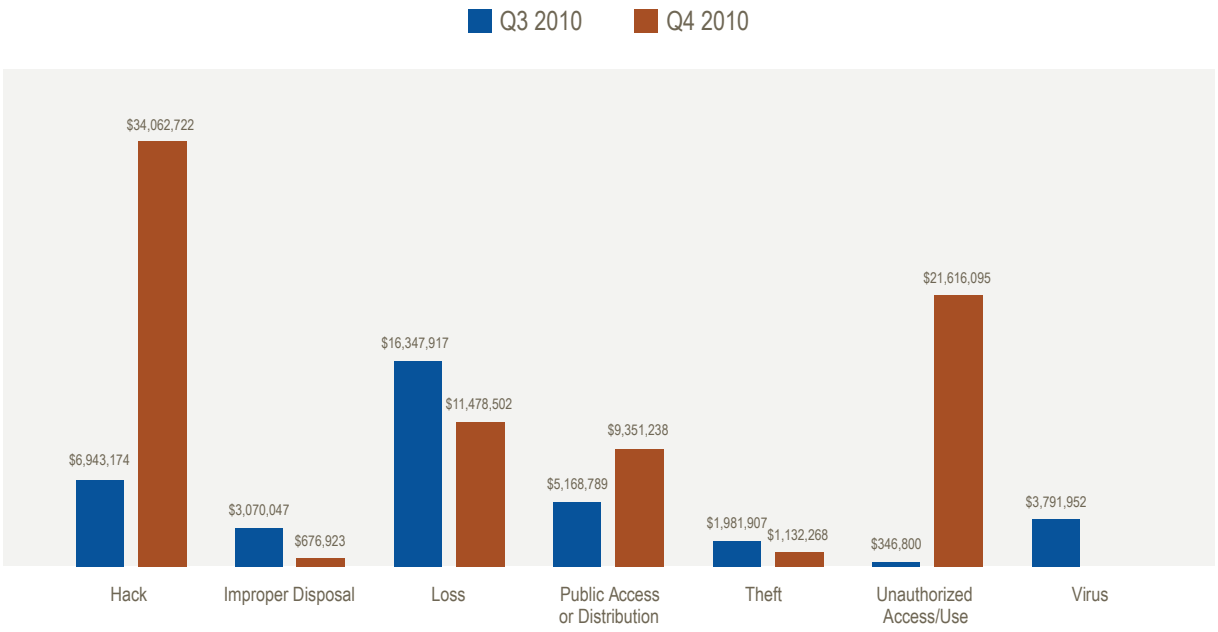
We also calculated the average total cost of a data breach by method of breach *(see Figure 9)*. For the most part, the breaches identified from quarter to quarter saw a decrease in the average total cost with three notable exceptions: Hack, Public Access/Distribution and Unauthorized Access/Use. The type of breach with the largest increase in average total cost from quarter to quarter was Unauthorized Access/Use with a 6,133% increase from quarter to quarter (Q3: $346,800 vs. Q4: $21,616,095).

FIGURE 8: AVERAGE TOTAL COST BY TYPE OF ENTITY



This increase in average total cost was due, in large part, to two breaches totaling over 500,000 records. This method was closely followed by Hack, which increased by a factor of almost four from quarter to quarter. Public Access/Distribution saw an 81% increase from $5.1 million in Q3 to $9.3 million. The other types of breach including Improper Disposal, Loss, Theft and Virus had varying decreases in the average total cost by type of breach from Q3 to Q4. Based on the data reviewed, the most expensive methods of breaches were Hack, Loss and Public Access/ Distribution. Hack ($34,062,722), in Q4, was the most expensive, followed by Unauthorized Access/Use ($21,616,095), Loss ($11,478,502) and Public Access/Distribution ($9,351,238). In Q3, Loss ($16,347,917) was the most expensive type of breach, followed by Hack ($6,943,174), Public Access/ Distribution ($5,168,789) and Virus ($3,791,952).

FIGURE 9: AVERAGE TOTAL COST BY TYPE OF BREACH



SPOTLIGHT ON NOTABLE DATA BREACHES

American Honda Motor Company

Industry: Automotive
Record Type: Electronic
Breach Method: Hack
Type of Media: N.A.
Size of Breach: 4.9 Million Records
Type of Data Breached: Name; Contact; E-Mail

American Honda Motor Co., a subsidiary Japanese automaker Honda, alerted 4.9 million customers of a potential data breach in late December 2010. American Honda warned 2.2 million customers that its e-mail database containing names, logins, e-mail addresses and vehicle identification numbers was hacked. The company also warned an additional 2.7 million My Acura owners who were also affected by the same breach. The My Acura account holders, according to public disclosures, only had their e-mail addresses breached. The e-mail database suffering the breach is used to send welcome messages to new customers who registered for an Owner Link account. The breach of these records was the result of a hack on an e-mail marketing firm that worked with American Honda.

deviantArt

Industry: Retail
Record Type: Electronic
Breach Method: Hack
Type of Media: N.A.
Size of Breach: 13 Million Records
Type of Data Breached: E-Mail; User Names; Date of Birth

deviantArt, the largest online social networking site for artists, had its user database hacked via its e-mail marketing provider Silverpop. Silverpop, an Atlanta based firm, was hacked in early December 2010. This hack exposed up to 13 million records. deviantArt sent e-mails to users informing them that e-mail addresses, user names and birth dates were potentially exposed. deviantArt, in an e-mail to users, stated the breach did not involve user passwords. The company further stated the security of its servers was not compromised and has since stopped using Silverpop as a vendor.

SPOTLIGHT ON NOTABLE DATA BREACHES *(CONTINUED)*

Gawker Media

Industry: Online Publishing
Record Type: Electronic
Breach Method: Hack
Type of Media: N.A.
Size of Breach: 1.3 Million Records
Type of Data Breached: E-Mail; User Names; Passwords

Gawker Media, a news, pop-culture and gossip site, informed its readers in a blog posting it had been hacked. The breach took place in December 2010 with 1.5 million accounts compromised. The hack, according to public sources, was done by a group called Gnosis. This group hacked the site and took source code, account information and e-mail addresses. The hack also harvested personal passwords of employees as well as internal staff conversations. The source code of Gawker was also taken and uploaded to a controversial file sharing site. The company urged all users to change their passwords for any accounts registered with Gawker.

1. Dan Goodman, "Feds Probe '100 site' Data Breach," *The Register,* 15 Dec. 2010. While no numbers were disclosed in the McDonald's breach, there were three separate breaches involving more than 1,000,000 records in Q4. These were considered outliers and thus not reported as part of the quarterly data. These three breaches are reviewed as part of this study under the Notable Data Breaches section of this report.
2. "2009 Annual Study: Cost of a Data Breach," *The Ponemon Institute LLC,* January 2010. The total average cost per record, according to the study, was $204. For purposes of this study, we estimated the total cost of each data breach using this figure calculated in the study.
3. Insurance companies are classified as Corporate entities for the purposes of this study, although protected health information may be breached in incidents involving insurance companies.
4. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
5. A Virus is an intrusive malware that infects computers, servers and networks. A virus often carries out unwanted operations on a host computer. A virus could be used for hacking or it could be unintentionally loaded into a system and cause damage. A Hack occurs when a group or individual attempts to gain, unauthorized access to computers or computer networks and tamper with operating systems, application programs, and databases. Unauthorized Access/Use is designated when an employee, contractor or volunteer of an organization wrongfully accesses or uses records. Unauthorized Access/Use is designated when an employee, contractor or volunteer of an organization wrongfully accesses or uses records. Improper Disposal is when either physical records or electronic media are not properly disposed and could become accessible to other parties. A Theft involves physical records or electronic media which have been stolen or taken from an organization without permission by an employee or other party. Loss is designated when either physical records or electronic media have been lost and cannot be located by the organization. Public Access or Distribution occurs when records or data are made available publically or to inappropriate parties. This includes data made accessible via a server, website or network and sent to inappropriate recipients via paper or electronic methods.
6. See Footnote #2.

ABOUT NAVIGANT

Navigant (NYSE: NCI) is a specialized independent consulting firm providing dispute, financial, investigative, regulatory and operations advisory services to government agencies, legal counsel and large companies facing the challenges of uncertainty, risk, distress and significant change. The Company focuses on industries undergoing substantial regulatory or structural change and on the issues driving these transformations.

CONTACT »

For questions related to the data presented herein:

Atlanta
Bill Jennings
404.602.5002
wjennings@navigant.com

Austin
Todd Lester
512.493.5420
tlester@navigant.com

Chicago
Kristofer Swanson
312.583.5784
kswanson@navigant.com

Denver
Steven Visser
303.383.7305
svisser@navigant.com

New York
Richard T. Faughnan
646.227.4234
rich.faughnan@navigant.com

Todd Marlin
646.227.4357
todd.marlin@navigant.com

Palo Alto
Rick Ostiller
650.849.1171
rostiller@navigant.com

Philadelphia
Tony Creamer
215.832.4444
acreamer@navigant.com

San Francisco
Aaron Philipp
415.356.7149
aphilipp@navigant.com

Toronto
Jennie Chan
416.777.2479
jchan@navigant.com

Washington, D.C.
Steven Stanton
202.481.8430
sstanton@navigant.com

Business Development Contacts
Scott Paczosa
312.583.2150
scott.paczosa@navigant.com

Jonathan Drage
312.583.2157
jonathan.drage@navigant.com

Research Lead
Bill Schoeffler
202.973.3140
bschoeffler@navigant.com

www.navigant.com

The authors would like to thank Vanessa Nelson for her invaluable assistance. Vanessa is a Research Coordinator specializing in practice specific and general business development research in the firm's Chicago office.