NAVIGANT

Information Security & Data Breach Report

June 2012 Update

DISPUTES & INVESTIGATIONS • ECONOMICS • FINANCIAL ADVISORY • MANAGEMENT CONSULTING

Data breaches continue to be one of the Achilles' heels for corporations as these incidents become the new normal. Due to the sensitivity of the information involved, the responsibilities of a company after a data breach continue to evolve. New rules and regulations require public disclosure when information is compromised, sometimes with specific timelines for notification. In response, companies are putting together tactical plans to handle potential data breaches along with other risk management plans. In this new environment, companies must protect themselves both externally and internally from these type of issues.

Navigant is pleased to release the June 2012 update of its Information Security and Data Breach Report. This report is designed to keep the legal community apprised of data breach activity, spotlight notable breaches, and identify trends and other major changes taking place in the information security arena. The goal of this publication is to answer the following principal questions:

1. What is the total number of breaches per quarter?
2. What 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. What are the leading causes of data breaches?
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 fourth quarter of 2011 and first quarter of 2012 (October 1, 2011 – March 31, 2012). 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.[1] The incidents reported involve physical or electronic records which were hacked, lost, stolen, or improperly exposed or discarded.

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

Navigant identified 60 major data breaches in Q1 compared to 62 in the previous quarter.[2] The total number of individual records breached in Q4 was 1,926,284 records. Q1 saw 2,591,434 records breached, a 35% increase from quarter to quarter. The top ten breaches in Q1 represented 2.3 million records.

DATA BREACH DASHBOARD

- Healthcare entities accounted for the largest percentage of the data breaches identified in either quarter (Q1: 33% vs. Q4: 40%).
- Healthcare entities showed the largest decrease in the number of days between discovery and disclosure of a data breach, from 97 days to 65 days. 'Other' entities showed the largest increase from quarter to quarter (Q4: 6 days vs. Q1: 44 days).
- 62% of breaches in Q4 and 41% in Q1 involving Education and Government entities were caused by Public Access or Distribution.
- The most commonly breached Corporate entities in both quarters were in the Services industry (Q4: 41% vs. Q1: 42%).
- The average number of records per breach increased 39% from quarter to quarter (Q4: 31,069 vs. Q1: 43,191).
- There was a 35% increase in the number of records breached from quarter to quarter (Q4: 1.93 million records vs. Q1: 2.59 million records).

One of the largest data breaches identified in either quarter involved a state agency that handled child support issues. The agency, which provides foster care and other services for children, disclosed that four computer storage devices went missing on March 12, 2012 while being transported back to the department from an off-site location following a disaster preparedness drill. The storage devices contained information on 800,000 people, including Social Security numbers (SSNs), names, addresses, driver's license numbers and names of health insurance providers. Other information contained on the missing devices included details on employers of custodial and non-custodial parents. Once the breach was identified, the department notified all those affected as well as the three major credit reporting agencies. The state attorney general and office dealing with privacy issues were also notified of this breach. The state did not offer credit monitoring or remediation services, but advised those affected to place a fraud alert on their credit cards and obtain copies of their credit report.

2. WHAT TYPES OF ENTITIES ARE EXPERIENCING BREACHES?

This report divides organizations into five main categories: Healthcare, Corporate, Education, Government and "Other."[3] These designations provide an overview of the entities that experienced a physical or electronic records breach.

Across both quarters, Healthcare entities had the largest percentage of breaches.

» In Q1, Healthcare entities accounted for 33% of all breaches tracked, followed by Corporate (20%), Education (20%), Government (17%), and "Other" (10%) *(See Figure 1).*

» In Q4, Healthcare entities experienced 40% of the data breaches identified, followed by Corporate (27%), Education (16%), Government (10%), and "Other" (7%) *(See Figure 2).*

As part of Navigant's analysis, we further parsed the Corporate entities to get a better sense of the industries experiencing data breaches. The most common types of Corporate entities experiencing a data breach in Q3 and Q4 are shown below.

Q1 2012	Q4 2011
Services (42%)	Services (41%)
Retail & Wholesale Trade (33%)	Insurance & Finance (41%)
Manufacturing (17%)	Retail & Wholesale Trade (12%)
Transportation, Utilities & Public Services (8%)	Manufacturing (6%)

A notable Corporate breach occurred at a West Coast company that reviewed medical records for workers compensation and auto casualty claims for insurers and employers across the United States. The breach occurred on New Year's Eve at the company's California headquarters. Thieves broke into the office overnight and took electronic equipment, including back up computer hardware. The theft was discovered the morning of January 3, 2012, following the holiday weekend. The incident was reported to the local police, who are still investigating. The computer hardware taken during the break-in contained detailed medical information on 14,000 people. The information included patient addresses, SSNs and medical diagnoses. The company sent a letter to those affected informing them of the breach. Shortly after this incident, the company filed for bankruptcy protection, citing the prohibitive cost of dealing with the data breach. The company has shut down and is selling its remaining assets to pay debts.

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

Data security regulations and the increasing danger of identity theft have elevated the importance of a timely response and disclosure after the discovery of a data breach. Discovery 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.

FIGURE 1: Q1 2012 BREACHES BY TYPE OF ENTITY

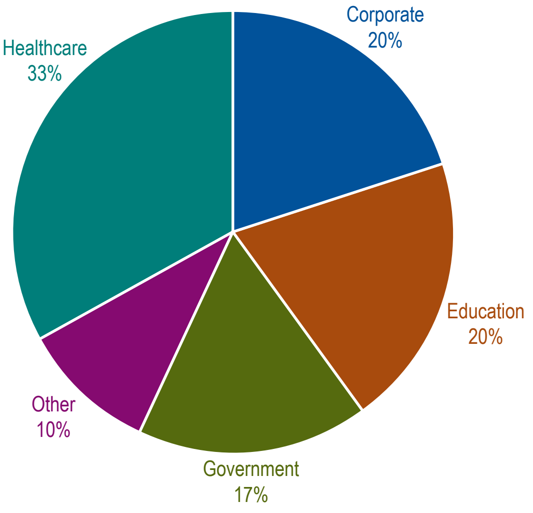
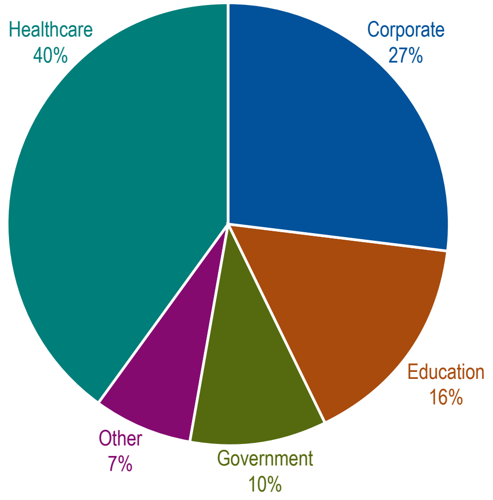


FIGURE 2: Q4 2011 BREACHES BY TYPE OF ENTITY



Forty-six states have enacted data breach reporting requirements for different types of data. Some states allow for a company to conduct a reasonable investigation regarding the incident while other states have established specific timelines for notification. The Senate Judiciary Committee recently approved three data security and privacy bills for consolidation and consideration that would require businesses to safeguard personal data collected from consumers and would establish a national data breach notification law. The increasing regulatory oversight regarding the disclosure of a data breach has prompted 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 48 days in Q1 compared to 60 days in Q4.

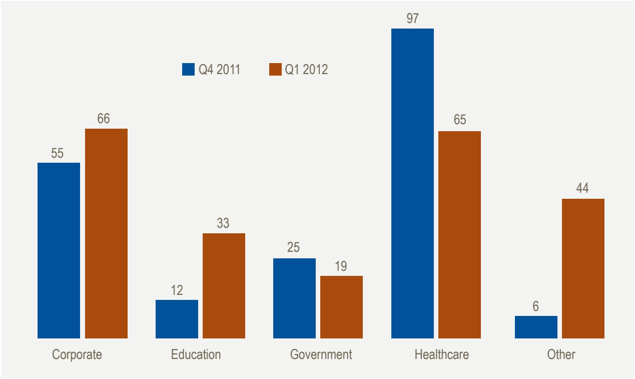
Currently both federal and state authorities require entities that hold personal health information to disclose when a data breach has occurred. The Department of Health & Human Services (DHHS) issued data breach regulations in August 2009. Similar breach notification regulations were issued by the Federal 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] From public sources, our analysis shows the average number of days between discovery and disclosure for medical records in Q4 was 101 days compared to 71 days in Q1, representing a 30% decrease from the previous quarter.[5]

We also track the average number of days between discovery and disclosure by entity *(See Figure 3).*

- Corporate entities increased 20% from quarter to quarter (Q4: 55 days vs. Q1: 66 days).
- Healthcare entities registered a 33% decrease between discovery and disclosure from 97 days in Q4 to 65 days in Q1.
- Education entities saw an increase between discovery and disclosure from 12 days in Q4 to 33 days in Q1.
- The number of days between discovery and disclosure for Government entities decreased from 25 days in Q4 to 19 days in Q1.
- "Other" entities registered 6 days in Q4 and 44 days in Q1.

The significant increase in time between discovery and disclosure for "Other" entities can be attributed to three incidents where the breach was reported 49 days, 57 days and 101 days after being discovered. According to news articles, one of these breaches occurred at a Veteran's Administration (VA) medical center. It was discovered that on January 9, 2012, information containing the names, SSNs and discharge dates of 1,182 veterans was found unattended in the facility lobby. According to a news report, after this discovery, the information was secured by the medical center's privacy officer and an investigation was launched. The incident was then reported to the DHHS. Following its review of this breach, the medical center offered affected veterans credit monitoring services as a precautionary measure. The facility also published a bulletin to all staff members reminding them of ways to safeguard and protect sensitive information.

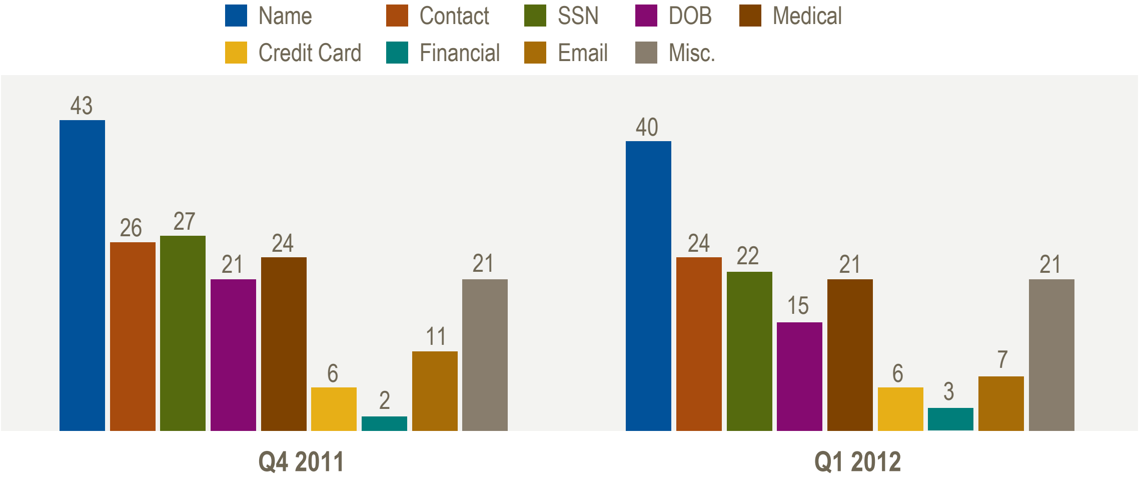
FIGURE 3: AVERAGE NUMBER OF DAYS BETWEEN DISCOVERY AND DISCLOSURE BY TYPE OF ENTITY



4. WHAT TYPES OF DATA ARE BEING COMPROMISED?

The types of data being compromised range from personally identifiable information (PII), such as date of birth (DOB), name or SSN, 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, SSN, 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, SSNs and DOBs were the types of data breached in

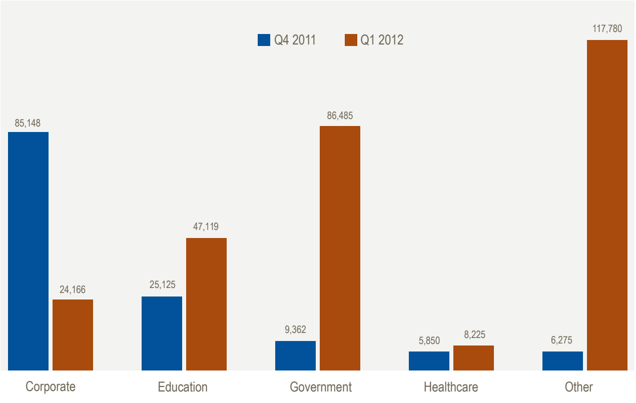
FIGURE 4: BREACHES BY TYPE OF INFORMATION



over 64% of the reported incidents in Q1 and 65% in Q4. Some of the most sensitive data, including SSNs and DOBs, were included in the types of data breached 23% of the time in Q1 and 27% of the time in Q4.

> A breach that involved personally identifiable information and other patient data was posted on the internet by a West Coast health system for nearly a year before being discovered. The records of over 31,000 patients were part of several files posted online. The patient information included names, ethnicity, race, gender, DOBs and medical data such as body mass index, blood pressure, allergies, lab results and diagnoses. The records cover patients who sought care from February 2011 – August 2011. The data was searchable online due to incorrect security settings allowing the records to be accessed using Google and other search portals. The health system set up a toll free 800 number and is providing free identity theft monitoring to those affected. As a result of this breach, the health system is facing several class action lawsuits alleging negligence and failure to comply with state medical information laws. The lawsuits are seeking over $30 million in damages as a result of this data breach.

FIGURE 5: AVERAGE RECORDS PER BREACH BY TYPE OF ENTITY



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

Navigant has calculated the average number of records per breach by type of entity *(See Figure 5)*. This analysis revealed that the average number of records per breach was 39% higher in Q1 2012 than in Q4 2011 (Q4: 31,069 vs. Q1: 43,191).

- Education entities saw a change from 25,125 records in Q4 to 47,119 records in Q1, an 88% increase from quarter to quarter.
- The average number of records per breach increased 824% from Q4 to Q1 for Government entities (Q4: 9,362 vs. Q1: 86,485).
- Healthcare entities experienced an increase in the average number of records per breach from 5,850 records in Q4 to 8,225 records in Q1.
- The average number of records per breach for Corporate entities was 24,166 in Q1 versus 85,148 in Q4, a decrease of 72%.
- "Other" entities averaged 6,275 records in Q4 and 117,780 records in Q1, a 1,777% increase quarter to quarter.

6. WHAT ARE THE LEADING CAUSES OF DATA BREACHES?

The different causes of a data breach are summarized into seven major categories. These categories are Virus, Hacking, Loss, Theft, Public Access or Distribution, Unauthorized Access/Use, and Improper Disposal.[6] In Q1 *(See Figure 6),* the most common methods used to breach data were:

- Theft (28%)
- Hacking (23%)
- Public Access or Distribution (23%)
- Unauthorized Access/Use (7%)
- Improper Disposal (7%)
- Virus (5%)
- Loss (4%)
- Unknown (3%)

Q4 *(See Figure 7)* had a similar break-out. Theft was again the most common type of breach (40%) followed by Hacking (23%), Public Access or Distribution (23%), Loss (8%), Unauthorized Access/Use (3%), and Improper Disposal (3%).

FIGURE 6: Q1 2012 Breaches by Type of Method

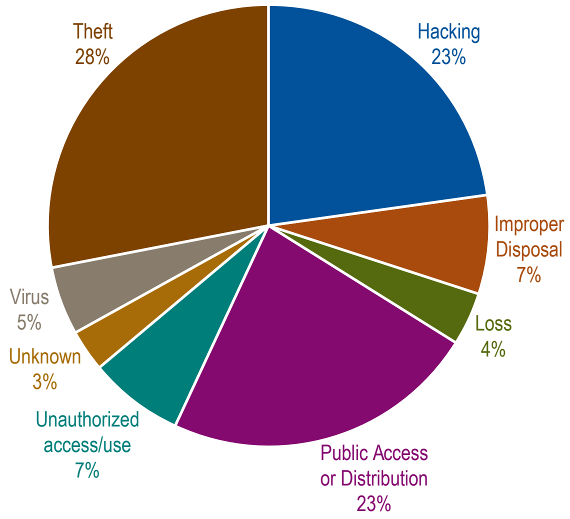
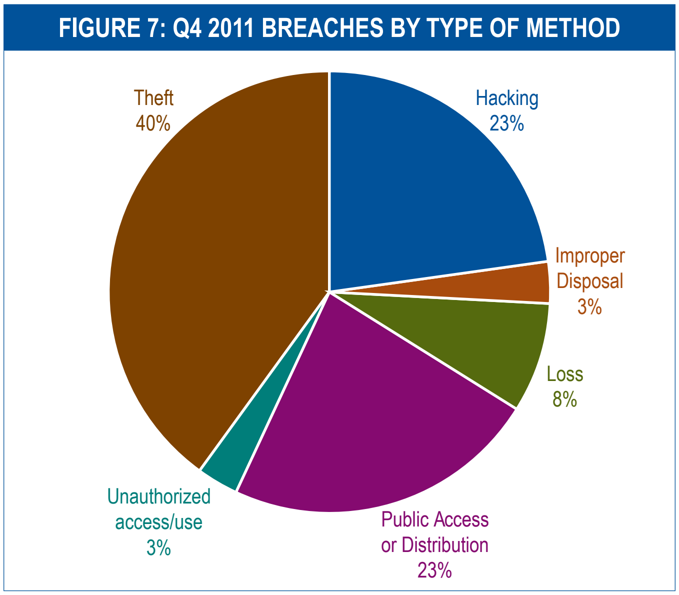


FIGURE 7: Q4 2011 BREACHES BY TYPE OF METHOD



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

- 62% of breaches involving Education and Government entities in Q4 and 41% in Q1 were caused by Public Access or Distribution.
- 59% of the data breaches involving Theft targeted Healthcare entities in Q1, while 68% of Theft incidents targeted Healthcare entities in Q4.
- The majority of breaches involving Corporate entities in either quarter were committed by Hacking or Theft (Q4: 71% vs. Q1: 67%).
- 83% of breaches involving improper disposal took place at Healthcare entities across both quarters.

A mid-Atlantic based hospital experienced a data breach when a former contractor's laptop was stolen. The former contractor had downloaded files to his personal laptop, which was stolen around January 25, 2012. The data of roughly 35,000 patients included names, addresses, SSNs, medical record numbers, birthdates, admission dates and diagnosis related information. The contractor alerted the police to the theft, who in turn notified the hospital. The hospital then launched an investigation culminating in notification letters being sent to patients. The letter recommends patients contact their banks and credit card companies to notify them of a potential disclosure of personal information. Those patients whose SSNs were on the stolen laptop will receive identity theft protection for one year.

Navigant also tracked the format of breached records. We divided the types of records into three main categories: physical, electronic and a combination of both. Electronic records may be accessed via CD-ROM, laptop, thumb drive, other media devices, e-mail, website or server. In Q1, 78% of the records compromised were electronic, while 20% were physical records. 2% of compromised records were classified as a combination of electronic and physical records. In Q4, 72% of the records compromised were electronic while 24% were physical records. 2% of the records breached in Q4 were classified as a combination of both types and 2% as unknown.

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

One of the most critical questions being asked relates to the total cost of a data breach for the entities involved. One of the foremost studies on this issue was published by the Ponemon Institute.[7] The most recent information released provides some statistics on the total costs of a data breach. For purposes of this quarterly report, Navigant identified the average total cost of a data breach by type of entity and type of breach.

A major university in the southeastern United States discovered a data breach in March 2012. An in-class project on advanced internet search techniques discovered three text files containing information on over 29,000 current and former students. One of the text files, including the information of 6,800 students who were enrolled in the university the previous year, contained names, SSNs and DOBs. The other two files contained similar data on faculty, staff and students. All three files were placed online during a server migration that took place in July 2011. Using the Ponemon Institute study estimates, the total cost of this data breach might be as high as $5.7 million. These costs include detection, discovery, notification, potential legal costs, ex-post costs, loss of customers, and/or brand damage. Once the university was alerted to this data breach, the files were removed and all information was deleted from search engines. According to news reports, the first text file of 6,800 students was indexed by Google while the other two files were not. Following this incident, the university offered credit monitoring services for those affected whose information was indexed by Google.

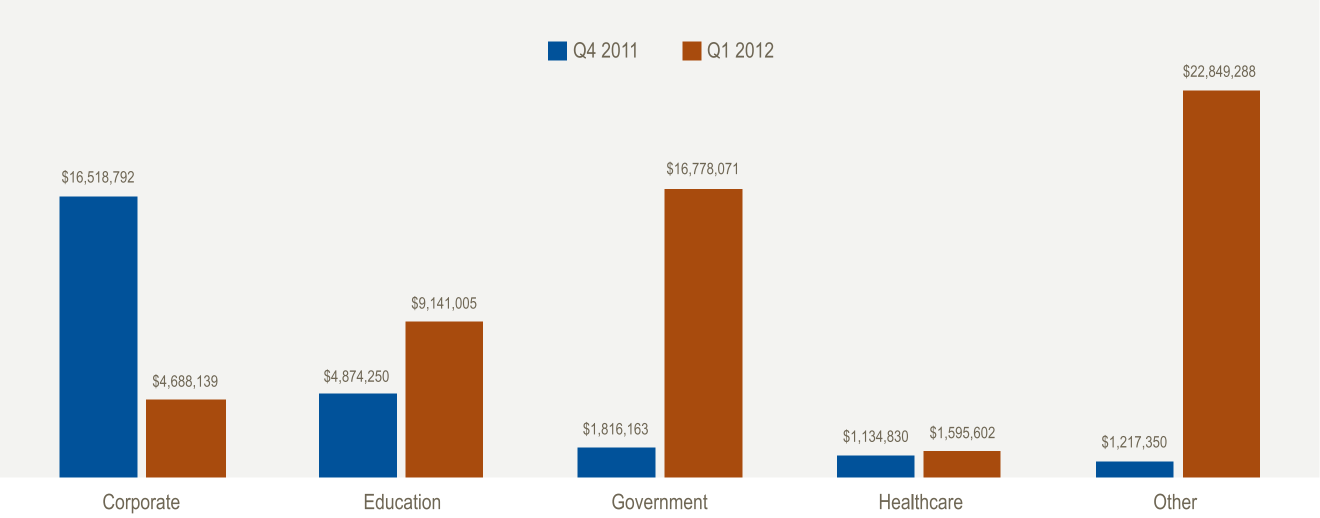
The average total cost of a data breach in Q4 was $6,027,405 and in Q1 was $8,378,970, a 39% increase. Some notable results from our analysis of the average total cost of a data breach by entity were *(see Figure 8):*

- In Q1, Corporate ($4,688,139) and Healthcare ($1,595,602) entities were below the average total cost of $8,378,970. Education, Government, and 'Other' entities were above the average total cost of a data breach by 9%, 100%, and 173% respectively.
- In Q4, Corporate ($16,518,792) entities were 174% above the average total cost of $6,027,405. Education, Government, 'Other' and Healthcare entities were below the average total cost of a data breach by 19%, 70%, 80% and 81% respectively.

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

- 'Other' entities had the largest increase from Q4 to Q1. The average total cost of a data breach increased from $1,217,350 to $22,849,288 million.
- Corporate entities' average total cost of a data breach decreased 72% from quarter to quarter (Q4: $16,518,792 vs. Q1: $4,688,139).

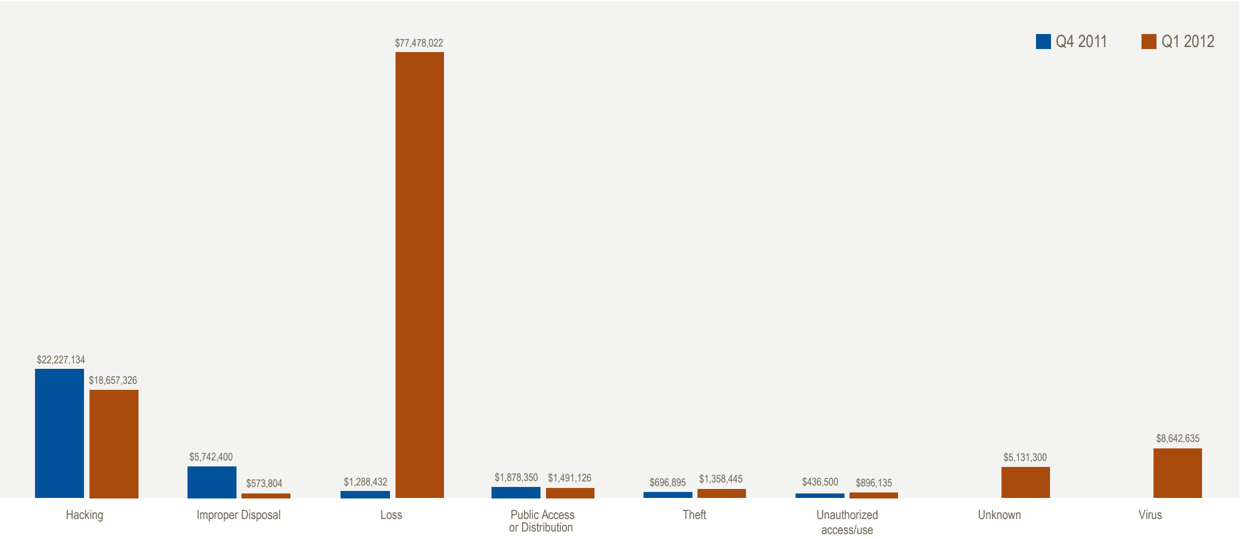
FIGURE 8: AVERAGE TOTAL COST BY TYPE OF ENTITY



- Education, Government and Healthcare entities showed increases in the average total cost of a data breach from quarter to quarter. Education entities increased from $4,874,250 to $9,141,005. Government entities increased from $1,816,163 to $16,778,071. Healthcare entities increased from $1,134,830 to $1,595,602.

Navigant also calculated the average total cost of a data breach by method of breach *(See Figure 9)*. Loss (Q4: $1,288,432 vs. Q1: $77,748,022) showed the most significant increase. Other categories with quarter to quarter increases were Theft and Unauthorized Access/Use. The type of breach with the largest decrease from quarter to quarter was Improper Disposal, which saw a 90% reduction (Q4: $5,742,400 vs. Q1: $573,804), followed by Public Access or Distribution (21%) and Hacking (16%). The methods of breach that cost the most across both quarters were Loss and Hacking. In Q1, Loss ($77,748,022) was the most expensive type of breach, followed by Hacking ($18,657,326) and Virus ($8,642,635). In Q4, Hacking ($22,227,134) was the most expensive type of breach, followed by Improper Disposal ($5,742,400) and Public Access or Distribution ($1,878,350).

FIGURE 9: AVERAGE TOTAL COST BY TYPE OF BREACH



SPOTLIGHT ON NOTABLE BREACHES

Company/Organization: Nemours
Industry: Hospital System
Record Type: Electronic
Method: Loss
Type of Media: Backup Tapes
Size of Breach: 1.6 Million Records
Type of Data Breached: Names, Contact Information, DOBs, SSNs, Financial Information

Nemours, one of the largest operators of pediatric clinics and hospitals in the country, had several backup tapes reported missing containing the data of over 1.6 million patients, guarantors, vendors and employees. The backup tapes were being stored in a locked filing cabinet that was reported missing on September 8, 2011. The company suspects the tapes were misplaced during a facility remodeling project the previous month. The potentially compromised data includes names, addresses, DOBs, SSNs, insurance data, medical treatment data and bank account information. The data contained information for the time period 1994 – 2004 on individuals at its five major facilities in Delaware, Florida, New Jersey and Pennsylvania. In response to this breach, Nemours is offering one year of paid credit monitoring and identity theft protection to those affected. The company is also moving to encrypt all backup tapes and moving other tapes to secure off-site storage.

Company/Organization: New York State Electric & Gas / Rochester Gas & Electric
Industry: Utility
Record Type: Electronic
Method: Improper Access
Type of Media: N.A.
Size of Breach: 1.8 Million Customers
Type of Data Breached: SSNs, DOBs, Financial Information

According to several news stories, a data breach took place at New York State Electric & Gas (NYSEG) and Rochester Gas & Electric involving the records of 1.8 million customers. The companies are owned by Spanish energy giant Iberdrola S.A. Both companies released a press release stating a subcontractor at a software consulting firm was allowed unauthorized access to customer information. The information breached included SSNs, DOBs and some customers' bank account numbers. The breach took place in early January 2012, and those affected by the incident began to receive notification within several weeks. The companies reported the incident to law enforcement and hired computer forensic experts to review the breach. Customers are also being offered one year of free credit monitoring services.

SPOTLIGHT ON NOTABLE DATA BREACHES *(CONTINUED)*

Company/Organization: Zappos
Industry: Retail
Record Type: Electronic
Method: Hacking
Type of Media: N.A.
Size of Breach: 24 Million Customers
Type of Data Breached: Names, Contact Information, Passwords, Financial Information

According to several news stories, Zappos, an online shoe retailer owned by Amazon, suffered a data breach affecting 24 million customers. Zappos customers were informed of the data breach by the retailer in a January 15, 2012 e-mail. The e-mail advised users the site had been hacked and customer information including their name, e-mail addresses, billing and shipping addresses, the last four digits of the user's credit card and a scrambled version of their password was likely stolen. The hackers gained access to the company's internal network through computer servers located in Kentucky. Following this incident, the company reset all customer passwords and urged users to change passwords on any website where they use the same or similar password. Zappos has not offered identity theft monitoring services to affected customers. Several days after the hack, the company also announced it was working with the FBI and undergoing digital forensics. The company has not disclosed how the breach took place, when it took place or the extent of the data stolen.

[1] For purposes of this study, Global Payments, Nemours, New York State Electric & Gas/Rochester Gas & Electric and Nemours were considered outliers and thus not reported as part of the quarterly data. Nemours and New York State Electric & Gas/Rochester Gas & Electric data breaches are reviewed as part of this study under the Notable Data Breaches section of this report.

[2] Quarterly data reported in prior studies may change when information regarding breaches is identified or amended.

[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] New information was discovered about several existing breaches in Q4 2011 which changed the statistics. One such incident had a lag of 582 days before discovery while another was 241 days.

[6] 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. Hacking 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. Improper Disposal occurs when either physical records or electronic media are not properly disposed and could be accessed by other parties. A Theft involves physical records or electronic media that 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 publicly 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.

[7] "Cost of Data Breaches Falls for First Time in Seven Years," PC World, March 20, 2012. The total average cost per compromised record was $194. For purposes of this study, we estimated the total cost of each data breach using this figure calculated by the Ponemon Institute.

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

Houston
Steve McNew
713.646.5015
steve.mcnew@navigant.com

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

Palo Alto
Rick Ostiller
650.849.1171
rostiller@navigant.com

Philadelphia
Tony Creamer
215.832.4444
acreamer@navigant.com

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

Strategic Initiative 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 Meihaus for her invaluable assistance. Vanessa is a Research Coordinator specializing in practice specific and general business development research in the firm's Chicago office.

Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. See www.navigant.com/licensing for a complete listing of private investigator licenses.