NAVIGANT

Information Security & Data Breach Report

April 2012 Update

DISPUTES & INVESTIGATIONS • ECONOMICS • FINANCIAL ADVISORY • MANAGEMENT CONSULTING

Electronic and traditional media continue to highlight the increasing scope and size of data breaches affecting millions of users. News headlines across CNET and PC World read, "Hackers Accessed Steam Users' Encrypted Passwords, Credit Cards[1]" which showed the continuing efforts by hackers to target videogame distribution services. According to several news stories, Valve, a video game company, suffered a data breach at its popular game service Steam. Hackers broke into a company database with customer information and accessed user forum accounts. The database contained information including user names, passwords, game purchases, e-mail addresses, billing addresses and encrypted credit card information. The hackers also defaced the user forum site, flooding it with advertisements for a group called FknOwned. Valve has over 35 million registered account users on its site. Gabe Newell, Valve CEO, told users of the hack via an announcement on the company's user forum message board. The company required users to change their forum passwords as well as encouraged users to change their Steam account passwords, but did not require it. The size, scope and potential liability of the Steam hack emphasizes the importance of understanding the various breaches affecting companies, healthcare organizations, educational institutions and government entities.

Navigant is pleased to release the April 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 primary 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?

DATA BREACH DASHBOARD

» Healthcare entities again accounted for the largest percentage of the data breaches identified in either quarter (Q3: 39% vs. Q4: 40%).

» There was an 88% increase in the number of records breached from quarter to quarter (Q3: 1.02 million records vs. Q4: 1.93 million records).

» Healthcare entities showed the largest increase in the number of days between discovery and disclosure of a data breach, from 51 days to 94 days. Education entities, on the other hand, showed the largest decrease from quarter to quarter (Q3: 41 days vs. Q4: 12 days).

» 50% of Hacking incidents targeted Corporate entities in Q3, while 67% targeted Corporate entities in Q4.

» The most common types of breaches involving Government or Education entities was Hacking and Public Access or Distribution.

» The average number of records breached per incident increased 71% from quarter to quarter (Q3: 18,253 vs. Q4: 31,069).

METHODOLOGY USED FOR IDENTIFYING DATA BREACHES

Navigant has captured all major data breaches disclosed publicly during the third and fourth quarters of 2011 (July 1, 2011 – December 31, 2011). 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 and electronic records were hacked, lost, stolen, or improperly exposed or disposed of.

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

Navigant identified 62 major data breaches in Q4 compared to 56 in the previous quarter, representing an 11% increase between reporting periods.[2] The total number of individual records breached in Q3 was 1,022,166 records. Q4 saw 1,926,284 records breached, an 88% increase from quarter to quarter. The top ten breaches in Q4 represented 1.68 million records and were primarily concentrated in Corporate entities.

One of the largest data breaches identified in either quarter involved a geopolitical intelligence firm. The firm, which provides analysis of geopolitical issues to both military and corporate clients, disclosed that a hacker collective broke into several servers and accessed information on over 860,000 users. The hackers obtained data including names, e-mail addresses, credit card numbers and passwords for anyone who ever registered on the company's website. The hackers also disclosed they had over 75,000 unencrypted credit card numbers. Once the breach was identified, the company took their website offline and contacted the Federal Bureau of Investigation (FBI), who is still investigating this incident. The company is offering to pay for one year of identity theft protection for anyone affected by the breach. The company reported $2.7 million in losses and fraudulent credit activity identified since the hack on Christmas Eve 2011. In the aftermath of this breach, the company now faces a lawsuit seeking $50 million in damages on behalf of customers whose personal credit card information was lost.

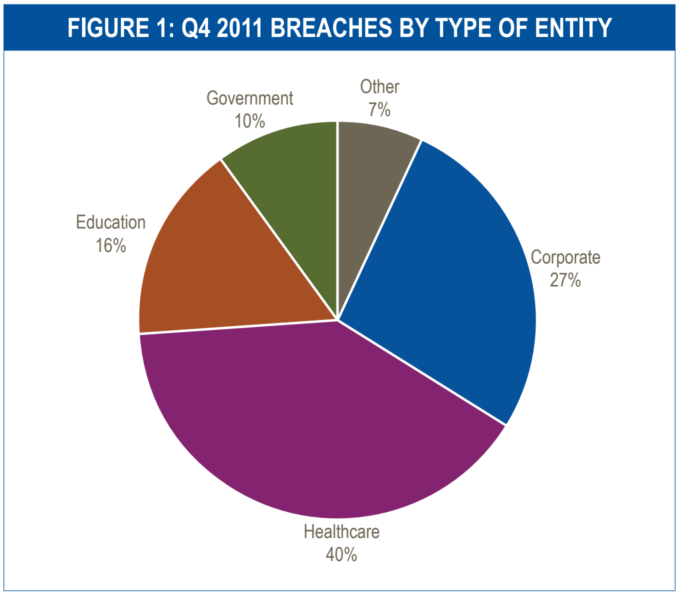
2. WHAT TYPES OF ENTITIES ARE EXPERIENCING BREACHES?

For purposes of this report, the types of organizations that experienced a data breach are divided into five main categories including 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 identified in this report.

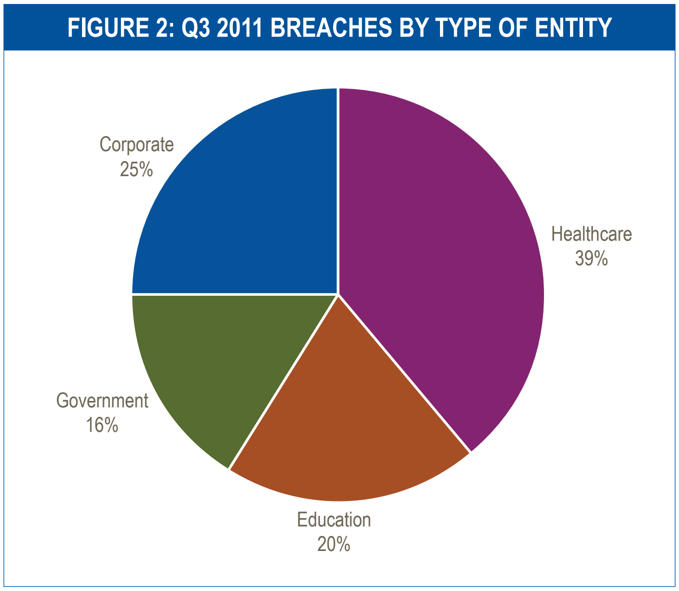
» In Q4, Healthcare entities accounted for 40% of all breaches tracked, followed by Corporate (27%), Education (16%), Government (10%), and "Other" (7%) (*See Figure 1*).

FIGURE 1: Q4 2011 BREACHES BY TYPE OF ENTITY



» In Q3, Healthcare entities experienced 39% of the data breaches identified, followed by Corporate (25%), Education (20%) and Government (16%) (*See Figure 2*).

FIGURE 2: Q3 2011 BREACHES BY TYPE OF ENTITY



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

Q4 2011	Q3 2011
Physicians Office (38%)	Hospital (57%)
Hospital (29%)	Health System (18%)
Clinic (13%)	Treatment Facilities (13%)
Health System (8%)	Surgery Center (4%)
Dental Practice (8%)	Physicians Office (4%)
Treatment Facilities (4%)	Clinic (4%)

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

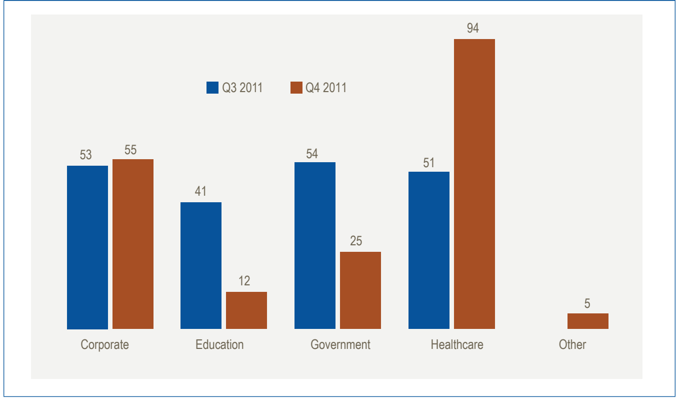
Data security regulations and the increasing danger of identity theft have elevated the importance of a timely response and disclosure after the discovery of a data breach. Discovery takes place when either electronic or physical records are confirmed to be lost or stolen, or data is otherwise identified 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 through websites or blogs. 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 59 days in Q4 compared to 50 days in Q3.

A notable healthcare-related data breach occurred at a medical clinic specializing in Nephrology, Geriatrics, Diabetes and Gastroenterology. The medical clinic notified patients of a data breach that occurred following Tropical Storm Lee. The breach occurred in early September 2011, but was not discovered until late October. A server had data on over 55,000 patients and was operated from the on-site lab, which was flooded with more than 100,000 gallons of water during the storm. As part of the cleanup process, the clinic mistakenly disposed of the server. Once the breach was discovered, the clinic took steps to notify its patients. In a letter posted on its website to patients, the clinic stated the server was no longer in use and the protected health information was likely inaccessible. Information contained on the server included full names, Social Security numbers (SSNs), dates of birth, home addresses, account numbers, diagnoses, laboratory test results and medical insurance information. The clinic has been unable to locate the missing server and did not offer its patients free credit monitoring or other remediation options.

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

- Corporate entities increased over 4% from quarter to quarter (Q3: 53 days vs. Q4: 55 days).
- Healthcare entities registered an 84% increase between discovery and disclosure from 51 days in Q3 to 94 days in Q4.
- Education entities, on the other hand, had a decrease between discovery and disclosure from 41 days in Q3 to 12 days in Q4.
- The number of days between discovery and disclosure for Government entities decreased from 54 days in Q3 to 25 days in Q4.
- "Other" entities registered 5 days in Q4, but no data was available for Q3.

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



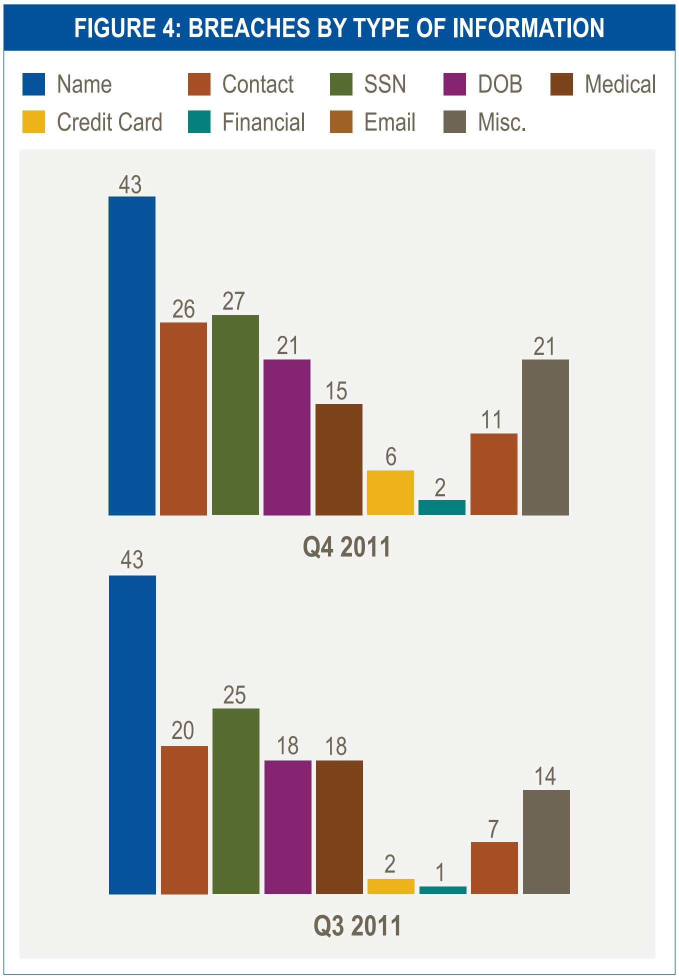
The significant increase in the time between discovery and disclosure for Healthcare entities can be attributed to several breaches. There were eleven breaches with over 90 days between discovery and disclosure in Q4 for Healthcare entities. According to news articles, one such breach occurred at an opera house where an emergency room physician stored patient records in boxes. The loss of 4,200 medical records took place following a fire at the opera house. The records were burned and scattered across the building following the fire. It took the physician several months to go through the debris and remove all the patient records that could be located. Those records that were located were buried 8-10 feet underground on a local farm. The records contained names, birth dates, SSNs as well as personal medical and psychiatric information. There is no indication from public sources that the patients whose records were compromised were notified or that any additional remediation has taken place.

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 Q3 was 63 days compared to 65 days in Q4, representing a 3% increase from the previous quarter.

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, 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, 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, SSNs and dates of birth were the types of data breached in over 68% of the reported incidents in Q4 and 71% in Q3. Some of the most sensitive data, including SSNs and dates of birth were included in the types of data breached 28% of the time in Q4 and 29% of the time in Q3.

FIGURE 4: BREACHES BY TYPE OF INFORMATION



A breach that involved personally identifiable information and other data took place when a hard drive containing patient information was stolen following a home invasion of a physician working for a major west coast university health system. During the robbery, the hard drive containing information on over 16,000 patients was taken along with the password to access the drive. The drive contained patient information including first name, last name, dates of birth, medical record number, address and medical information. The information on the stolen hard drive was from July 2007 to July 2011. The drive was taken in early September 2011. The university health system conducted an investigation and notified those affected by the breach with a letter and posted a notice on the system's web site. The system set up Identity Theft consultation and restoration services if a patient's credit was affected by the incident. The health system also undertook changes in its policies by providing additional education and awareness training to its staff on storing patient information. Following this incident, the university health system was sued in state court alleging violations of state laws related to the confidentiality of patient information. The suit seeks $16 million in damages.

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

Navigant has endeavored to calculate 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 70% higher in Q4 2011 than in Q3 (Q3: 18,253 vs. Q4: 31,069).

- The average number of records per breach for Corporate entities was 85,148 in Q4 versus 34,259 in Q3.
- Education entities saw an increase from 21,959 records in Q3 to 25,125 records in Q4, a 14% increase from quarter to quarter.
- The average number of records per breach increased 54% from Q3 to Q4 for Government entities (Q3: 6,078 vs. Q4: 9,362).
- Healthcare entities experienced a decline in the average number of records per breach from 11,195 records in Q3 to 5,850 records in Q4.
- "Other" entities registered no data for the average number of records per breach for Q3, but averaged 6,275 records in Q4.

6. WHAT ARE THE LEADING CAUSES OF DATA BREACHES?

The different causes of a data breach are summarized into seven major categories. These categories include Virus, Hacking, Loss, Theft, Public Access or Distribution, Unauthorized Access/Use, and Improper Disposal.[5] In Q4 (*See Figure 6*), the most common methods used to breach data were:

- Theft (40%)
- Hacking (23%)
- Public Access or Distribution (23%)
- Loss (8%)
- Unauthorized Access/Use (3%)
- Improper Disposal (3%)

FIGURE 6: Q4 2011 BREACHES BY TYPE OF METHOD

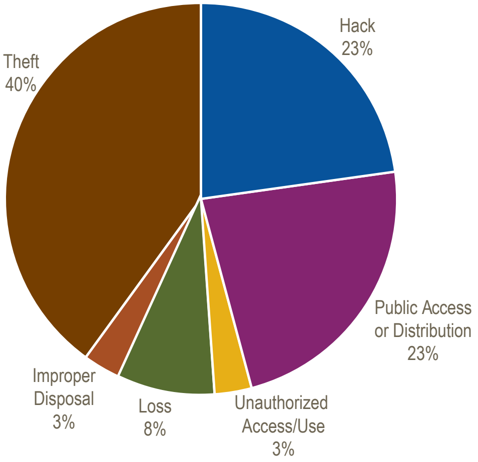
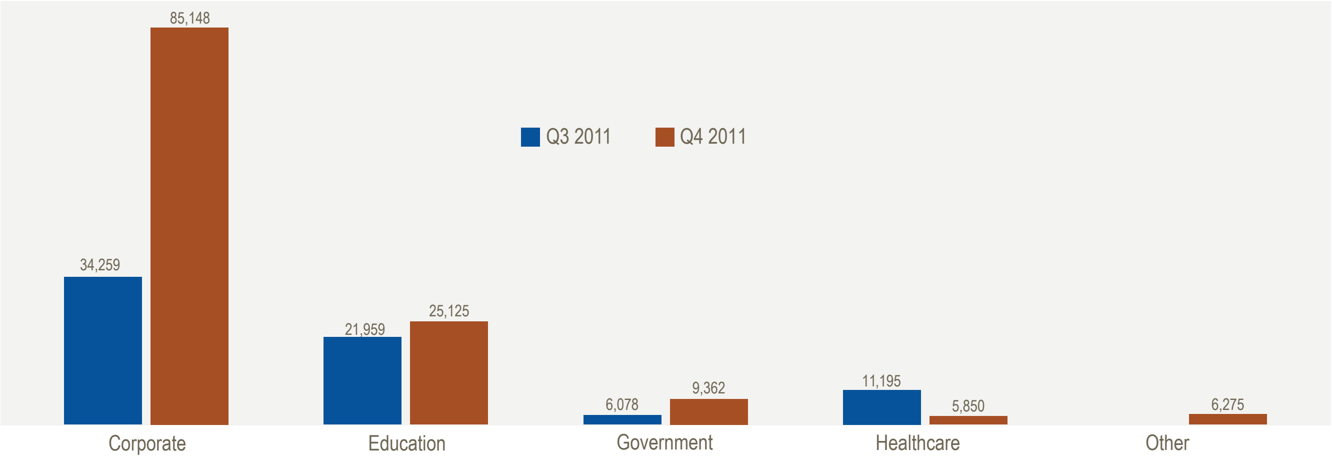
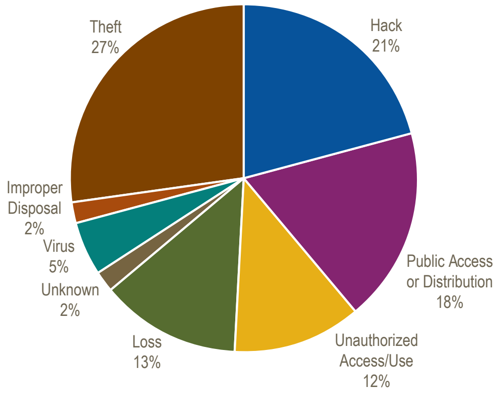


FIGURE 5: AVERAGE RECORDS PER BREACH BY TYPE OF ENTITY



Q3 (*See Figure 7*) had a similar break-out. Theft was again the most common type of breach (27%) followed by Hacking (21%), Public Access or Distribution (18%), Loss (13%), Unauthorized Access/Use (12%), Virus (5%), Improper Disposal (2%) and Unknown (2%).

FIGURE 7: Q3 2011 BREACHES BY TYPE OF METHOD



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

- Data breaches caused by Theft increased by largest percentage from quarter to quarter.
- 50% of Hacking incidents targeted Corporate entities in Q3, while 67% targeted Corporate entities in Q4.
- 55% of Healthcare breaches in Q3 and 68% in Q4 involved Theft.
- 67% of the breaches involving Government entities in either quarter were caused by Public Access or Distribution and Theft.
- The most common methods of the data breaches involving Education entities was Hacking and Public Access or Distribution.

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 Q4, 72% of the records compromised were electronic, while 24% were physical records. 2% of compromised records were classified as a combination of electronic and physical records. In Q3, 79% of the records compromised were electronic while 19% were physical records. Q3 and Q4 both had 2% of the records classified as unknown.

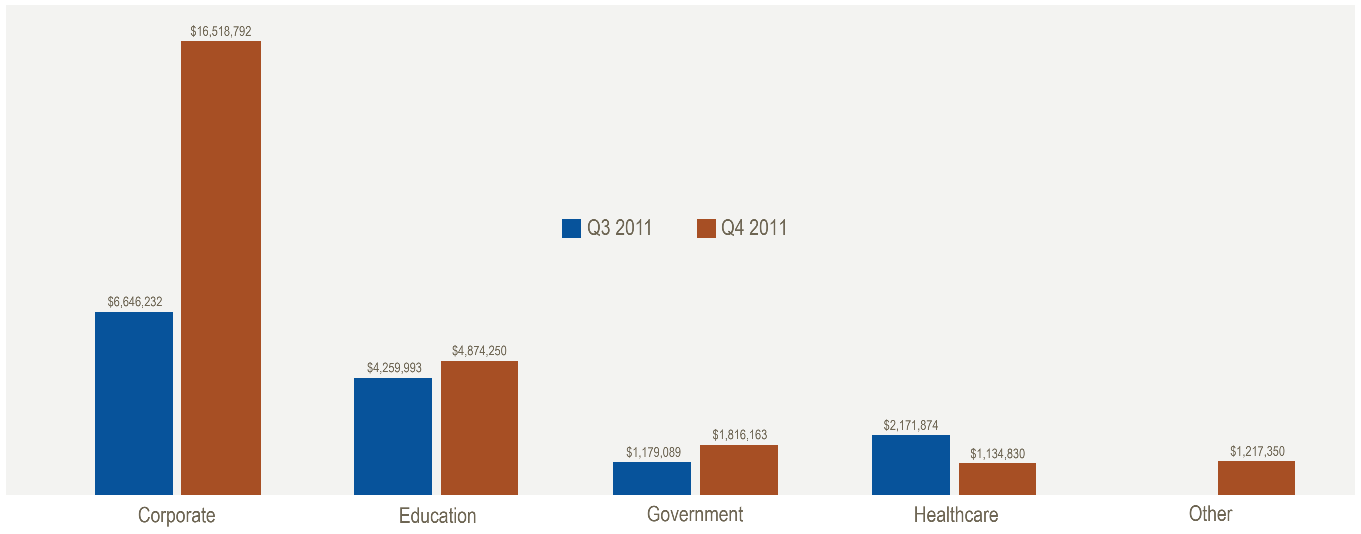
7. WHAT IS THE AVERAGE TOTAL COST OF A DATA BREACH?

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.[6] 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.

The average total cost of a data breach in Q3 was $3,541,075. The average total cost in Q4 was $6,027,405, a 70% increase. Some notable results from the average total cost of a data breach by entity were (*see Figure 8*):

A 529 college savings plan for a Midwestern state experienced a data breach when SSNs were printed on envelopes sent to participants in the plan. The SSNs were printed near the space designated for the recipient's name. The data breach was characterized as low risk because the envelopes were sorted by machine and only handled by mail carriers delivering them to individual residences. Once informed of the breach, the state attorney general contacted the bank who administers the plan to take immediate action. The bank reached out to those affected by the data breach offering free identity theft protection and credit monitoring.

FIGURE 8: AVERAGE TOTAL COST BY TYPE OF ENTITY



One of the largest restaurant wholesale outlets in the country had malware inserted into the company's credit and debit card processing system. The hack took place between September and November 2011, and resulted in over 300,000 customers having their credit card information exposed. Using the Ponemon Institute study estimates, the total cost of this data breach might be as high as $58.2 million. These costs include detection, discovery, notification, potential legal costs, ex-post costs, loss of customers, and/or brand damage. The hackers' use of malware allowed them to temporarily collect credit card information as it was processed and then send it to a computer server in Russia. The stolen credit card data included the names on the credit cards, credit or debit card numbers, expiration dates and the three digit verification code. Once the breach was identified, the wholesale outlet enhanced the company's security measures. The company is also reimbursing card holders for any reasonable costs incurred due to this breach as well as providing 12 months of credit monitoring.

- 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.
- In Q3, Corporate ($6,646,232) and Education ($4,259,993) entities were 88% and 20% above the average total cost of $3,541,075. Healthcare and Government entities were below the Q3 average total cost of a data breach by 39% and 67%, respectively. 'Other' entities did not have data available in Q3 to make an average total cost of a data breach comparison.

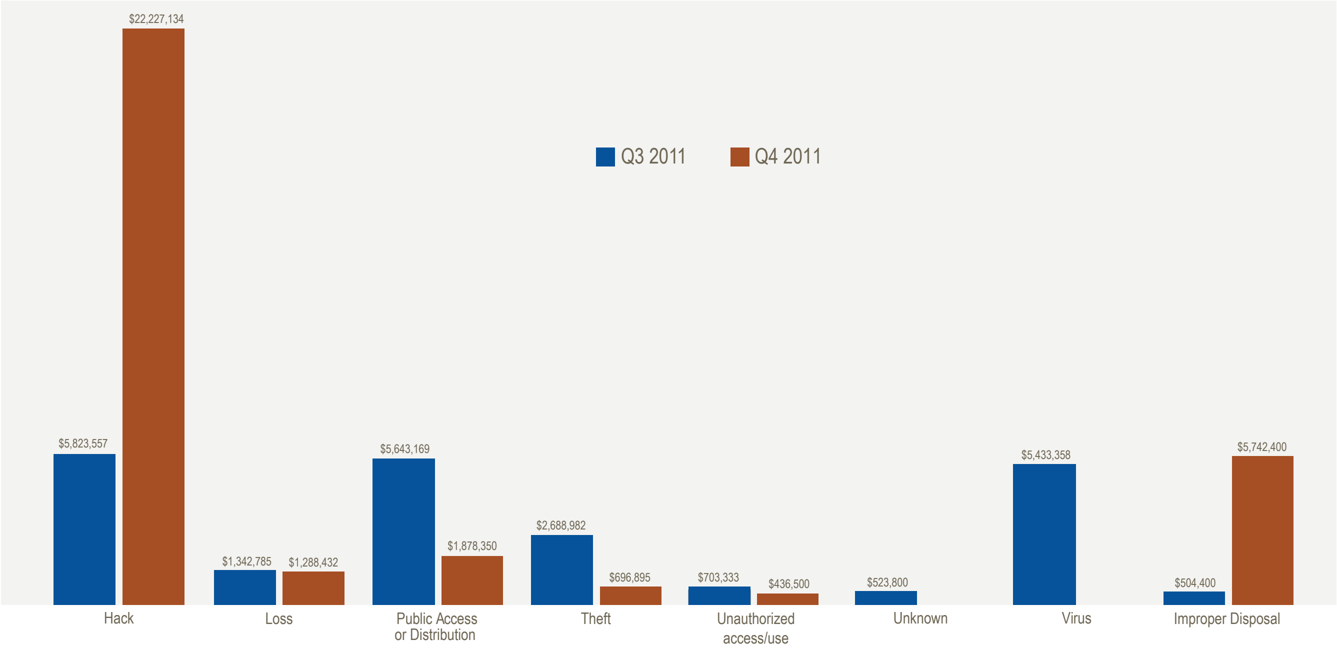
The average total cost of a data breach varied widely by type of entity between quarters.

- Corporate entities had the largest increase from Q3 to Q4. The average total cost of a data breach increased from $6,646,232 to $16,518,792 million, a 149% increase.
- Healthcare entities' average total cost of a data breach decreased 48% from quarter to quarter (Q3: $2,171,874 vs. Q4: $1,134,830).
- Education and Government entities also showed increases in the average total cost of a data breach from quarter to quarter. Government entities increased from $1,179,089 to $1,816,163. Education entities increased from $4,259,993 to $4,874,250. "Other" entities did not have Q3 2011 data to compare against.

We also calculated the average total cost of a data breach by method of breach (*See Figure 9*). Hacking (Q3: $5,823,557 vs. Q4: $22,227,134) and Improper Disposal (Q3: $504,400 vs. Q4: $5,742,400) both showed significant increases in the average total cost of a data breach. The other categories including Loss, Public Access or Distribution, Theft, and Unauthorized Access/Use decreased from quarter to quarter. The type of breach with the largest decrease from quarter to quarter was Theft, which saw a 74% reduction (Q3: $2,688,982 vs. Q4: $696,895). Theft was followed by Public Access or Distribution with a 67% decrease, then by Unauthorized Access/Use (38%) and Loss (4%).

The methods of breach that cost the most across both quarters were Hacking and Public Access or Distribution. 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). In Q3, Hacking ($5,823,557) was again the most expensive type of breach, followed by Public Access/ Distribution ($5,643,169) and Virus ($5,433,358).

FIGURE 9: AVERAGE TOTAL COST BY TYPE OF BREACH



SPOTLIGHT ON NOTABLE BREACHES

Company/Organization: Sutter Health

Industry: Hospital System

Record Type: Electronic Breach

Method: Theft

Type of Media: N.A.

Size of Breach: 4.24 million records

Type of Data Breached: Names, Dates of Birth, Financial Information, Medical

Sutter Health System, one of the largest not-for-profit health systems in California, had a desktop computer stolen with the personal data of over 4 million patients in October 2011. The theft occurred over the weekend of October 15, 2011, at one of the company's offices. It was immediately reported to the police and Sutter undertook an investigation to determine the extent of the breach. Sutter sent letters notifying patients of the breach in November and set up a toll free hotline to answer any questions. The data breach affects two groups of patients. The first group, comprising 3.3 million patients, had data compromised including names, addresses, dates of birth, phone numbers, e-mail addresses, medical record numbers and health insurance providers. The second group of patients, comprising 943,000 patients, had additional data compromised including dates of service, descriptions of medical diagnoses and procedures from January 2005 to January 2011. In response to this breach, Sutter has accelerated its efforts to encrypt desktop computers as well as provide additional training to its staff systemwide.

Company/Organization: Ultimate Bet Poker

Industry: Gaming

Record Type: Electronic Breach

Method: Hack

Type of Media: N.A.

Size of Breach: 3.5 Million Records

Type of Data Breached: Names, SSN, Financial

According to several news stories, a data breach took place at Ultimate Bet Poker involving 3.5 million accounts. The site has been in legal limbo since the Department of Justice seized the domain names and the assets of the company in April 2011.The site is still active and users can play poker for free online. The information breached from the popular poker site included the player's names, screen names, dates of birth, phone numbers, deposit methods, account status and e-mail addresses. The information was posted anonymously on a poker forum website. The data was organized by country, showing over 2 million users in the United States; 319,000 in Canada; 137,000 in the United Kingdom; and another 1 million accounts from all other countries. The site is entering liquidation and no action has been taken to notify users or remediate this issue.

[1] Jason Schreier, "Hackers Accessed Steam Users' Encrypted Passwords, Credit Cards," Wired 10 November 2011. For purposes of this study, Steam (Valve), Sutter Health, Ultimate Bet Poker, Trion Worlds, U.S. Chamber of Commerce, Care2.com and Nemours were considered outliers and thus not reported as part of the quarterly data. Sutter Health and Ultimate Bet Poker 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] 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. 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.

[6] "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

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
sstanton@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.

©2012 Navigant Consulting, Inc. All rights reserved.

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.