Even in news cycles dominated by the threat of global terrorism and the National Football League, large scale data privacy incidents continue to make headlines including P.F. Chang’s, eBay, the Montana Department of Public Health and Human Services, Butler University and Community Health Center, to name a few. The frequent news reports on data breaches have led to calls for increased regulation and notification at both the federal and state level. Kentucky became the 47th state to implement a data breach notification law and Florida just passed the Florida Information Protection Act of 2014 (SB 1524), an update to its existing rules and regulations. With Congress, the Federal Trade Commission, and State Attorney Generals now taking notice of data privacy events, it has become clear that companies need the proper risk management protocols in place to handle this increasingly complex environment.

Navigant is pleased to present our latest report, which is designed to provide you insights into notable breaches that took place in Q2 2014 and identify trends with the objective of answering the following principal questions:

1. What is the total number of breaches per quarter?
2. What types of entities experience breaches?
3. What is the average number of days between discovery and disclosure of a breach?
4. What types of data are compromised?
5. What is the average number of records per breach?
6. What are the most common methods of breach?
7. What is the average total cost of a breach?

METHODOLOGY USED FOR IDENTIFYING DATA BREACHES

Navigant reviewed United States breaches publicly disclosed during the second quarter of 2014 (April 1, 2014 – June 30, 2014). In this study, we compare Q2 2014 data against the prior four quarters referred to as the Four Quarter Average (“FQA”).1 The incidents identified in this report affected a minimum of 1,000 and maximum of 1,000,000 individuals through a breach of physical and/or electronic records.2 In the absence of a centralized notification repository, we have evaluated multiple sources to compile breach details, including news databases, online news sources, entity websites, blogs, and state and federal agency websites.

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

We identified 80 major data breaches in Q2 which was in line with the previous four quarter average of 81. Q2 breaches exposed 1,791,387 records, which is significantly lower than the FQA of 3,191,487 records.

Major breaches constituting over 1 million records have increased to the point where they are no longer considered outliers and going forward Navigant will report them as part of this study. We identified three major breaches in Q2 2014 totaling over 153 million records. Q1 saw the same number of major breaches but only 8 million records were identified as having been comprised. The number of records identified for the major breaches in Q2 was well above the FQA (FQA: 94,398,879 vs. Q2: 153,300,000).

2. WHAT TYPES OF ENTITIES EXPERIENCE BREACHES?

No industry or entity type is exempt from the threat of an information security breach, although incidence and magnitude vary among categories. Our report classifies the organizations that experienced a physical or electronic records data breach into five categories: Healthcare, Corporate, Education, Government and Other. Across Q2 and the FQA, Healthcare entities experienced the largest percentage of breaches identified. (See Figure 1).

LITIGATION SPOTLIGHT

One of the largest breaches identified in Q2 occurred at a technology company specializing in ticketing, digital marketing and access management at music festivals. The firm discovered its systems had been breached and as many as 50,000 records had been impacted. Upon learning of the breach in April 2014, the company contacted law enforcement to launch an investigation. The company also hired outside forensic investigators to determine the nature and scope of the breach. According to news reports and the company’s preliminary investigation, the hack took place between November 2013 and February 2014. The personal information breached included names, addresses, phone numbers, e-mail addresses, and payment card information as well as user names and passwords for the website. The company began to notify customers in early May 2014. It also implemented additional security measures to prevent a similar incident in the future.
Four of the top ten breaches in Q2 involved Corporate entities, followed by three breaches from Healthcare, and two from Education. The top ten breaches in Q2 represented 1.07 million records, or 60% of the total. During the prior four quarters, nine out of the top ten breaches involved either Corporate or Healthcare entities.

Among Corporate entities, several industry groups were affected by lapses in information security. The Services industry had a relatively steady number of breaches across each period. The greatest variation was found in the Insurance & Finance and the Retail & Wholesale Trade groups with both showing percentage increases from the FQA.

### 3. WHAT IS THE AVERAGE NUMBER OF DAYS BETWEEN DISCOVERY AND DISCLOSURE OF A 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. The vast majority of states have requirements regarding the reporting of a potential data breach to those affected. Some states allow entities to conduct a reasonable investigation of the incident before notification, while others have established specific timelines for notification. The only states without specific data breach notification laws are Alabama, New Mexico and South Dakota. However, New Mexico representative William “Bill” Rehm introduced House Bill (HB) 224 on January 28, 2014 following the highly publicized Target data breach. The legislation would mandate that organizations that experience a data breach must notify individuals within 10 days of a breach discovery, as well as the New Mexico Attorney General if more than 50 residents are affected. The bill would also require companies in New Mexico to implement and maintain reasonable security measures to ensure the protection of personal identifying information (PII). The bill was passed by the New Mexico House 60-0 and then referred to the state Senate, where it was referred to the Judiciary Committee and then postponed indefinitely.

Our study identifies the date on which a breach is first made public and the date of discovery. The average number of days between discovery and disclosure for all breaches decreased to 42 days in Q2 compared to 58 days in the FQA. The average number of days between discovery and disclosure is less consistent by entity type (See Figure 2). Education, and Healthcare entities experienced the most significant changes in this metric. The decrease in the time between discovery and disclosure for Education entities can be attributed to at least five incidents that were disclosed less than 15 days after the discovery of an incident. Education entities had the lowest number of days between data breach discovery and disclosure in Q2, compared to Healthcare, which had the highest (Education: 18 days vs. Healthcare: 48 days).

Both federal and state laws require entities with personal health information (PHI) to disclose a data breach within a specified time frame. For example, Federal rules require entities to provide notification within sixty days of discovery of a breach of protected health information involving a minimum of 500 records. Our analysis of breaches involving medical records shows the average time between discovery and disclosure in the most recent reporting period was below the sixty day limit (FQA: 67 vs. Q2: 52).

### LITIGATION SPOTLIGHT

A major credit card vendor suffered a breach in late March 2014, potentially involving 58,522 California residents. The names, credit card account numbers, expiration date and security code were breached according to a recent disclosure from the California Attorney General. This breach was linked to the hacking collective Anonymous who hacked several major credit card companies and then posted the information on Pastebin following a release of some data on Twitter. The breach of the credit card companies is still being investigated both in the U.S. and U.K., and is potentially linked to over six million credit cards. Following the disclosure of this specific breach for California card members in early June 2014, the company placed additional fraud monitoring on those affected and confirmed they would not be liable for any fraudulent charges.
4. WHAT TYPES OF DATA ARE COMPROMISED?

Personally Identifiable Information (PII) such as names, dates of birth (DOBs) and Social Security numbers (SSNs), and Personal Health Information (PHI) such as information related to medical conditions, the provision of healthcare, or payment for the provision of healthcare; and financial information or credit card numbers are among the most sensitive types of information that may be compromised by a breach. In this report, the data commonly at risk is categorized as Names, Contact Information, Passwords, SSNs, DOBs, Medical Information, Credit Cards, Emails, Financial Information, and Miscellaneous Information. Most of the incidents in this report involve multiple types of data. Figure 3 indicates that as the number of incidents increases between reporting periods, so does exposure of most data types, including sensitive data such as SSNs and Medical Information.

- SSNs were identified in 55% of breaches in Q2 up from 48% in the FQA.
- The exposure of Medical Information grew from 42% in the FQA to 51% of breaches in Q2.
- DOBs were part of 50% of the breaches reported in Q2, down from 54% in the FQA.
5. WHAT IS THE AVERAGE NUMBER OF RECORDS PER BREACH?

The average number of records can be affected by many factors within a reporting period, but a high average often indicates one or more extensive breaches. In this report, the Q2 average was 43% below the previous four quarter average (FQA: 39,401 vs. Q2: 22,392). All major breaches by entity type were below the FQA except Education which increased due, in large part, to two breaches over 100,000 records. (See Figure 4.)

- Corporate breach averages decreased by 64% between the FQA and Q2.
- Government entities saw the largest change, with a 91% decrease between reporting periods.

6. WHAT ARE THE MOST COMMON METHODS OF BREACH?

Breaches range from the accidental loss of a thumb drive to the willful hacking of a large corporate database. Our study classifies the methods of breach as Virus, Hacking, Unauthorized Access/Use, Improper Disposal, Theft, Loss, and Public Access/Distribution. Theft, Hacking and Unauthorized Access/Use ranked as the highest methods of breach across reporting periods. (See Figure 5.)

- Unauthorized Access / Use took the lead in Q2 with 26% of reported breaches versus 16% in the FQA.
- Public Access / Distribution also increased between reporting periods (Q2: 25% vs. FQA 20%).
- Public Access / Distribution was the most common method of breach affecting Healthcare entities in both reporting periods.
- Healthcare entities were evenly breached by several methods including Hacking, Public Access / Distribution, Theft and Unauthorized Access / Use.
- Hacking was the most common method of breach affecting Education entities with 33% in Q2 and 55% in the FQA.
7. WHAT IS THE AVERAGE TOTAL COST OF A DATA BREACH?

Response costs are a primary concern for entities faced with a data breach. One of the foremost studies on this issue is published by the Ponemon Institute and provides statistics regarding the costs associated with a data breach. Costs may include detection, discovery, notification, legal fees and fines, ex-post costs, loss of customers, and/or brand damage, and will vary with each incident. Navigant has used the Ponemon cost per record to estimate the average total cost of a data breach by type of entity and method of breach.

Education entities have the highest breach costs in Q2, although they were followed closely by Corporate entities in the same reporting period. Despite Healthcare entities accounting for the majority of breaches, they have one of the lowest average costs, indicating a lower number of records per incident. The average cost estimates regarding breach methods demonstrates that intentional data security breaches tend to affect more individuals and incur higher costs than other methods of breach. (See Figure 7).

- The highest cost associated with a method of breach in Q2 was $7,687,617 for breaches involving Hacking.
- The average total cost of a breach involving Loss dropped 80% (FQA: $3,642,329 vs. Q2: $741,590) across reporting periods.
- The average costs for Loss and Public Access/Distribution are comparatively lower than all other disclosed breach methods across the reporting periods.

LITIGATION SPOTLIGHT

A Midwestern university experienced a data breach involving 30,000 SSNs for current students and past graduates over the last 17 years. The data breach was discovered when internet traffic to the university slowed tremendously prompting a review of the university servers. It was discovered the servers had been hacked and malware called “minerd” was installed. The malware uses the computing power of infected servers to mine for bitcoins. The hack was discovered in late February and the servers were repaired and fixed in early March 2014. Several weeks later, the university sent letters to those affected informing them of the incident. The breach was also reported to law enforcement. In response to the breach, the university offered free credit monitoring to those affected. The university also rolled out additional security measures and destroyed the affected servers.
Company/Organization: Montana Department of Public Health and Human Services
Industry: Government
Record Type: Electronic
Method: Hacking
Size of Breach: 1.3 Million Records
Type of Data Compromised: Names, Addresses, DOBs, SSNs

The Montana Department of Public Health and Human Services was hacked in May 2014 exposing the personal information of 1.3 million people. Those affected included current and former Montana residents as well as employees of the agency. Once the hack was identified, the state immediately launched an investigation into the matter and alerted law enforcement. The hacked server was shut down and the state agency hired a forensic investigator to determine the extent of the hack. The investigation revealed the information compromised included names, addresses, DOBs and SSNs. Employees of the state agency also had their bank account information and dates of service breached. In response, the state is offering free credit monitoring and identity protection insurance to those affected by the incident and Montana also upgraded its security software following the hack.
NOTES


2 Breaches involving more than 1,000,000 records are considered outliers. Montana Department of Public Health are discussed in the Notable Breaches section of this report. eBay, and P.F. Chang’s, while considered outliers, are not discussed in the Notables Breaches section of this report. Quarterly data reported in prior studies may change when information regarding breaches is identified or amended.

3 Protected health information may be breached in incidents involving all types of entities. For example, insurance companies maintain health information but are classified as Corporate for the purposes of this study.

4 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. Theft involves physical records or electronic media that have been stolen or taken from an organization without permission from the responsible party. Loss is designated when either physical records or electronic media have been reported missing by an organization. Public Access/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. In prior editions of this study, Virus is a separate method of breach. In this and future editions, Virus is contained within the Hacking category.

5 2014 Cost of Data Breach Study – United States, Ponemon Institute LLC, May 2014. The total average cost per compromised record was $201. For purposes of this study, we estimated the total cost of each data breach using this figure calculated by the Ponemon Institute.

6 There is little value in reporting the cost of an incident in which the breach method is unknown, and we have not included these incidents in the costs data.

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.

CONTACTS

For questions related to the data presented herein:

Lead Data Breach Forensic Investigators
Steven Visser
303.383.7305
svisser@navigant.com

Bill Hardin
312.583.4119
bill.hardin@navigant.com

Cuyler Robinson
312.583.2188
crobinson1@navigant.com

Nicholas Barone
646.227.4453
nicholas.barone@navigant.com

Daren Hutchison
303.383.7322
dhutchison@navigant.com

Strategic Initiative Contacts
Scott Paczosa
312.583.2150
scott.paczosa@navigant.com

Darin Bielby
215.832.4485
dbielby@navigant.com

Marc Adams
312.583.3670
marc.adams@navigant.com

Research Lead
Bill Schoeffler
202.973.3140
bschoeffler@navigant.com

navigant.com

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