Are Large Scale Data Breaches Inevitable?

Cyber Infrastructure Protection '09
City College
The City University of New York
June 5, 2009

Douglas E. Salane
dsalane@jjay.cuny.edu

Center for Cybercrime Studies
John Jay College of Criminal Justice
Mathematics & Computer Science Dept.
445 West 59th Street
New York, NY 10019

Abstract – **Despite heightened awareness, large scale data breaches continue to occur and pose significant risks to both individuals and organizations. An examination of recent data breaches shows that fraudsters increasingly are targeting institutions that hold large collections of credit card and social security numbers. Particularly at risk are card payment processors and retailers who do not properly secure their systems. Frequently, breached data winds up in the hands of overseas organized crime rings that make financial data available to the underground Internet economy, which provides a ready market for the purchase and sale of large volumes of personal financial data. This study concludes that strong data breach notification legislation is essential for consumer protection, and that the direct and indirect costs of breach notification provide significant economic incentives to protect data. Also needed are standards for end-to-end encryption, enterprise level methods for quickly patching and updating information systems, and enhanced privacy standards to protect sensitive financial information.**

I. INTRODUCTION

A data breach occurs when an organization loses control over who has access to restricted information. The Privacy Rights Clearing House [1], a non profit privacy advocacy organization, maintains a partial list of the breaches reported since 2005. Losses of tens of thousands of records now occur almost on a weekly basis. Large scale breaches at data aggregators, credit card payment processors, and national retail chains have compromised the sensitive personal and financial data of millions individuals. Currently forty-four states have data breach notification laws that require organizations to notify the individuals affected by a breach. For organizations holding data on individuals, breaches are no longer an internal matter and can be quite costly, both in terms of breach notification costs and the loss of confidence of customers and business partners.

Data breaches exposing information that can be used to commit fraud are of particular concern. Such breaches typically involve sensitive financial information such as credit card and bank account numbers. Often causing even greater harm, however, is the loss of personally identifiable information (PII) such as drivers' license or social security numbers. Unlike compromised credit card and account numbers, it is difficult to know how thieves will use a social security number or other PII to commit fraud. A growing Web underground for the contraband now provides a ready market for both types of information, and data thieves have ample incentive to steal both.

The scale and scope of data breaches during this decade has been alarming. From 2003 to 2005, each of the three leading data aggregation companies, Acxiom [2], LexisNexis [3] and ChoicePoint [4], suffered serious data breaches by failing to control business partners who had access to their databases. (Reed Elsevier, the parent company of LexisNexis, purchased Choice Point in 2008.). In 2005, ChoicePoint inadvertently released the financial records of 163,000 persons by making the data available to identity thieves who posed as legitimate clients. In 2003 and 2004, in two separate incidents, Acxiom subcontractors extended their authorized authority and stole information in the company's databases. In one case, the subcontractor stole over one billion records. From 2003 to 2005, LexisNexis found that unauthorized persons used IDs of legitimate users to obtain social security numbers, drivers' license numbers, and the names and addresses of over 310,000 individuals in its databases. In a recent announcement (May 2009), the company notified over 40,000 individuals that credit card data it held may have been compromised in 2007.

During the past four years several major retailers and card payment processing companies have had extremely large data breaches. In June 2005, Master Card disclosed that a card processor, CardSystems Solutions, suffered a data breach that compromised the credit card information of over 40 million card holders [5]. In the widely publicized TJX Companies breach that occurred from 2005 to 2007, thieves stole over 45 million credit card numbers [6]. According to the Massachusetts Bankers Association, the breach affected the credit records of over 20% of New Englanders. In March 2008, Hannaford Brothers Co. disclosed that malicious software in its payment systems compromised at least 4.2 million credit and debit card accounts [7]. In December of 2008, payment processor RBS Wordplay said a breach of its payment systems affected more than 1.5 million people [8]. Security and law enforcement experts are still trying to determine the extent of the Heartland Payment System Breach discovered in Dec. 2008. Heartland processes over 100 million credit/debit transactions per month and is one of the top ten payment processors. For over 18 months, malicious software on a Heartland server intercepted unencrypted Track 2 (information on the magnetic strip of a credit or debit card). The company became aware of the breach when Visa reported excess fraudulent activity in credit card transactions processed by Heartland [9].

Although large scale breaches attract the most attention, smaller targeted breaches can result in significant losses since they often provide thieves all the information needed to commit fraud. Recently thieves installed skimmers on ATM machines in New York City and positioned concealed cameras near the machines to record PIN numbers. After fabricating credit cards with the stolen information, the thieves were able to steal over $500,000 from about 200 victims [10]. Thieves then attempted to withdraw the maximum allowable amount from each account for as many days as possible. Skimmers for capturing the card's Track 2 data and devices for fabricating cards are available on the Web. This type of crime no longer requires exceptional technical skills, and ATM frauds that use this equipment are becoming increasingly common.

Due to the potential impact of breaches on consumers, organizations, and commerce, data breach research is an active area. Two organizations that provide breach information are the Open Security Foundation through its DataLoss DB project [11], and the previously mentioned Privacy Rights Clearing House. The DataLossDB project maintains a downloadable data base of incidents and provides aggregate statistics on breaches since 2005. The primary sources of information on data breaches are breach notification letters sent to state attorney generals, which typically are required under state breach notification laws, and copies of breach notification letters sent to individuals whose information has been compromised. Press reports, SEC filings, and company statements are other important sources. Despite California's landmark breach notification legislation in 2003 and the adoption of breach notification legislation in 44 states, detailed information on a data breach is seldom made public or shared with the larger security community at the time of a breach.

Data breaches, particularly large scale breaches involving PII, raise many questions. Unfortunately, the secrecy that typically surrounds a data breach makes answers hard to find. Detailed information, which may be essential for threat detection throughout a particular industry, is seldom made available at the time a breach occurs. In fact, the details surrounding a breach may not be available for years since large scale breaches usually result in various legal actions. The parties involved typically have no interest in releasing any more information than the law requires. Ironically, detailed breach information often becomes available in the course of a legal action when it becomes part of the public record. Thus the exact means by which a breach occurred often is not known until long afterward, if ever. Moreover, information on perpetrators and what exactly they do with the information is difficult to obtain. Such information may only come to light years later, if at all, in the course of criminal prosecutions. In addition, it is often not clear how to quantify the harm that may be caused by a breach − if 40 million records are compromised, what portion of them is likely to be used to commit fraud? What information should be made available to affected individuals, and how should they be instructed to protect themselves? Who bears the costs? In industries where multiple parties process data, who are the responsible parties?

The remainder of this paper examines notable large scale breaches in the data aggregation, card payment processing, and retail industries. The paper explores remedies and practices that have been suggested to mitigate breaches, particularly in the card payment industry. The paper discusses the costs of notable large breaches both to individuals and the companies involved. The paper describes research and developments needed to improve data breach detection, deterrence and response.

II NOTABLE BREACHES: INSTITUTIONS, CAUSES AND COSTS

By 2005, largely through acquisitions of smaller data management companies, Acxiom, ChoicePoint and LexisNexis had grown to be the world's three largest aggregators and providers of data on individuals, each with revenues of over $1 billion annually. These organizations leveraged their significant analysis and processing capabilities, gleaned over many years of managing data for large corporate clients, to provide detailed information on and profiles of individuals to insurers, collection agencies, direct marketers, employment screeners, government agencies, including state and local law enforcement agencies. The web site of Accurint [12], the information subsidiary of LexisNexis, indicates the detailed information held and made available. For example, one product provided by the company, People at Work, holds information on 132 million individuals including addresses, phone numbers and possible dates of employment. The site advertises the ability to find people, their relatives, associates, and assets. Large scale breaches at each of theses data aggregators earlier in this decade raised a great deal of attention among privacy advocates and prompted calls for regulation of the activities of the data aggregation industry [13].

During 2002 and 2003, Acxiom suffered two separate serious data breaches that involved Acxiom business partners who had legitimate password access to the company's databases [14],[15]. The first involved the system administrator of a small company who provided services to

Acxiom and who routinely downloaded files from an Acxiom FTP server. The administrator exceeded his authority on the server and was able to download and decrypt a file containing passwords. He obtained a master password that allowed him to then download files belonging to other companies. The administrator sealed his fate when he told a hacker friend in a chat room that he had been able to obtain access to a local telephone company data base. A subsequent investigation of the hacker friend led to the administrator. As part of the same investigation, Acxiom technicians came upon a second more serious breach that involved theft by a subcontractor to an Acxiom contractor. From January 2001 to June 2003, the subcontractor, who owned a firm that provided e-mail advertising services, accessed over one billion records in Acxiom's databases by extended his authorized access. The individual was later arrested and convicted on various federal charges that included 120 counts of unauthorized access of a protected computer [16]. Prosecutors claim he used the data in his own e-mail advertising business and eventually planned to sell his company and its newly expanded database to a credit rating company.

The Choice Point breach occurred in Fall 2004 and involved the theft of 145,000 consumer records – the number was later updated to 163,000 records [17]. Under California's breach notification law, ChoicePoint had to disclose the breach to California residents. Shortly afterward, attorney generals in 38 states demanded that ChoicePoint disclose the breach to victims in all states [18]. The breach led to numerous calls for an investigation of how information held by aggregators might be used to harm individuals [19]. The breach cost Choice Point $2 million just in notification fees and over $10 million in legal fees. In Feb. 2005, the Company said about 750 individuals had been victims of identity theft. The company stated at the time that the breach did not involve a compromise of its networks or hacking, but was carried out by a few individuals who posed as legitimate business customers and were given access to the data, which included personal financial information. The company stated that financial fraud conducted by seemingly legitimate businesses is a pervasive problem. The Federal Trade Commission (FTC) later determined that Choice Point was in violation of the Fair Credit Reporting Act. The company settled with the FTC by paying $10 million in fines and $5 million for consumer redress. One of the perpetrators, a Nigerian national living in California, later was arrested and tried under California law on charges of identity theft and fraud. He was sentenced to 10 years in prison and ordered to make restitution of $6 million. The incident led to dramatic changes in the way ChoicePoint safeguards sensitive personal information and screens potential business customers.

LexisNexis, another leading data aggregator, announced a major breach in 2005 that exposed the personal information of 310,000 individuals [20]. LexisNexis found after analyzing data over a two year period that unauthorized people used IDs and passwords of legitimate customers to obtain consumers' social security numbers, drivers' license numbers, names and addresses. The company stated that the breach involved 59 incidents of improper access to data. The company added that various techniques were used to gain access to the data, including, collecting IDs and passwords from machines infected with viruses, using computer programs to generate passwords and IDs that matched those of legitimate customers, and unauthorized access by ex-employees of companies with legitimate access to LexisNexis data. The incident appeared to be not one breach but a series of breaches that occurred over a multiyear period and involved several different groups.

Recently (May 2009), LexisNexis disclosed a breach that exposed the personal information of 40,000 individuals and compromised names, birthdates and social security numbers [21]. The breach appears to have taken place from June 2004 to Oct. 2007. The company breach letter [22] said the thieves, who were once legitimate LexisNexis customers, used mailboxes at commercial mail services and PII taken from LexisNexis to set up about 300 fraudulent credit cards. The breach letter indicated that LexisNexis learned of the breach from the United States Postal Inspection Service, which was investigating the fraudulent credit cards.

In congressional testimony in 2005, Acxiom's chief privacy officer discussed the company's data breaches [23]. She claimed that most information obtained was of a non sensitive nature and none of it was used to commit identity fraud. She noted that the company would henceforth require stronger passwords and keep data on servers only for the period for which it is needed. She mentioned that Acxiom had decided to appoint a chief security officer, a position now common in most large organizations. From her testimony, it was obvious that this breach was an embarrassment for a company that obtains over 80% of its revenues from managing data for large corporations and large public agencies. She indicated that Acxiom was in the process of participating in dozens of audits by clients, whose trust in the company had certainly been diminished. The privacy officer reflecting the words of the then FTC commissioner said there is no such thing as perfect security and breaches will happen even when all precautions are taken. The privacy officer's testimony underscored the importance of removing data when it was no longer needed and effectively monitoring contractors and vendors with access to company data. At a recent presentation at John Jay College [24], the chief security officer of Time Inc. indicated that vendor management now was one of his major responsibilities.

The retail and card payment processing industries have suffered a number of large scale breaches during the past five years. Unlike the data aggregation industry, breaches in these industries appear to have involved malware on servers that collected data and transmitted it outside the company. These breaches, however, also involved individuals with detailed insider knowledge of the systems that were compromised. Although the credit card industry and retail industries have not reported significant rises in the rates of credit card fraud [25], the scope of recent payment card breaches, the rapidity with which stolen credit information was used, and the geographical scope of the fraud, raise concerns that data thieves are now taking advantage of the capabilities afforded by world wide crime organizations to monetize vast collections of breached financial information.

One of largest breaches of a payment processor occurred at CardSystems Solutions, a company that processed both credit and debit credit card transactions. According to the FTC [26], in 2005 the company handled over 210 million card purchases worth $15 billion for more than 119,000 small and mid-size merchants. The company's CEO admitted in congressional testimony [27] that the data thieves captured Track 2 information belonging to 263,000 individuals. Security experts later determined that credit and debit information of over 40 million customers may have been compromised. Despite the incredible volume of transactions processed by the company, at the time the company had only 115 employees. The breach and was discovered not by CardSystems, but by Mastercard security while tracking fraudulent card activity [28].

The FTC charged CardSystems Solution with violation of Section 5 of the FTC Act, which prohibits unfair or deceptive business practices [29]. The FTC claimed that the company violated the Act by failing to adopt widely accepted, easily deployed security standards that would have prevented the exposure of the sensitive financial data of tens of millions of individuals. The FTC further charged that the company neglected industry security polices with respect to the type of data it collected and the amount of time it held the data.

A forensic investigation of the breach found numerous security lapses both in the company's systems and procedures. The company violated it own industry security polices by storing data in unencrypted format on a server accessible from a public network. Data thieves were able to execute an SQL injection attack that allowed an unauthorized script to be placed on a web facing server. The script exported data to an external FTP site every four days. In addition, data was retained for purposes other than payment processing, another violation of industry policy. Furthermore, the company did not adequately assess its systems' vulnerabilities to commonly known attacks, did not use strong passwords, and did not implement simple, widely used defenses to thwart SQL attacks. The CEO also added in congressional testimony [30] that the company stored Track 2 data for later analysis, another violation of industry security standards.

The breach raised new levels of security awareness within the card payment processing industry and provided significant impetus for compliance with the industry's newly developed Payment Card Industry Data Security Standard (PCI DSS or simply PCI) [31]. Today, loss of PCI certification can put a payment processor out of business as it undermines the confidence of customers and partners. Shortly after the CardSystems breach, Visa and American Express stopped processing with the company. After revising security policies, upgrading systems, and implementing end-to-end encryption on its backend systems and networks, the company eventually gained PCI certification. PayByTouch, another payment processor, then purchased the company at a steep discount [32].

The largest breach of a retailer's payment processing systems occurred at TJX Companies from 2005 to 2007 [33]. Intruders had access to the systems for over 18 months. In filings with the SEC, the company said 45.6 million card numbers may have been taken. Card issuing banks later raised the total to 94 million. In addition, thieves captured personal information such as drivers' license numbers, which was used to track merchandise returns [34]. According to industry estimates, a card replacement can cost between $5 and $15 dollars, and a breach notification may cost up to $35 per notification. Shortly after the compromise, thieves used the card numbers to make purchases in Georgia, Florida, and Louisiana in the United States as well as in Hong Kong and Sweden. By Sept. 2007, the breach had cost the company over $150 million, and the company still faced numerous class action law suits.

TJX believes a flaw in its wireless networks may have allowed malware to be placed on one of its Retail Transaction Switch Servers (RTS) that processes and stores information on customer purchases and charge backs for its stores throughout North America. At the time TJX was in the process of upgrading its wireless security from the weaker Wired Equivalent Protection (WEP) standard to the stronger WiFi Protected Access (WPA) standard [35]. TJX admits that intruders had accessed the system at times from July 2005 to January 2007.

A report by the Office of the Privacy Commissioner of Canada [36] provides a summary of TJX Companies' security lapses that led to the breach. The privacy commission found that the TJX intruders gained access to the names, addresses, drivers' license numbers and Provincial Identification Numbers of over 330 persons with addresses in Canada. According to Canadian privacy law, TJX should not have collected this information in card transactions. Citing analyses of the incident, the commission found that the company did not have in place adequate logging procedures to do a proper forensic analysis of the incident. The data thieves actually deleted information so it was difficult to tell what information was compromised. The commission also faulted the company for not being fully compliant with industry standards and practices such as PCI. The commission noted that as far back as 2003 IEEE standards committees had recommended migration from the WEP security standard to the stronger WPA standard, yet the company had at the time of the breach failed to complete the migration. Even though the commission found that TJX had an adequate organizational security structure in place, it faulted the company for collecting too much data, holding it too long, using a weak security protocol, and not having adequate monitoring in place to detect a breach in progress or determine the extent of the breach after the fact.

Another payment processor, RBS World Pay of Scotland suffered a serious breach in Dec. 2008 that involved over 1.5 financial million records [37]. According to the FBI, thieves stole Track 2 data from debit cards that were used to pay employees. They also may have accessed the social security numbers of one million customers. The FBI said the thieves worked with cashiers in 49 cities including Atlanta, Chicago, New York, Montreal, Moscow, and Hong Kong to withdraw over $9 million from accounts. The cashiers fabricated cards locally and made withdrawals from local ATMs. Timing is critical in these frauds. If good fraud monitoring is deployed, the information has to be monetized quickly before cards are cancelled.

In Jan. 2009, Heartland Payment Systems Inc. announced the largest data breaches to-date of a payment processor, over 100 million cards compromised. Heartland is among the top ten card payment processors and handles over 100 million credit and debit card transactions per month. The breach was detected not by Heartland, but by VISA's security organization, which noticed an increase in fraudulent activity on cards processed by Heartland. The source of the breach was malware on a Heartland system, which intercepted payment information sent to Heartland from thousands of retail merchants. At the time of the breach announcement, Heartland claimed no social security numbers, unencrypted PIN numbers, addresses or telephone numbers were revealed [39]. Thieves, however, were able to intercept the Track 2 information, which is sufficient to fabricate a duplicate credit card. At the time the company said it did not know how long the malware was in place, how it got there, or how many accounts were compromised. A security analyst at Gartner Inc. noted that the company was probably not doing file integrity monitoring to detect unauthorized changes in files and directories [40].

The losses in this breach are significant. Thus far the breach has cost the company $12 million including a $7 million fine imposed by Mastercard. Given the number of compromised cards, banks would be unlikely to cancel and reissue all of them since the costs could be between $600 million to $1 billion, which is bigger than any anticipated fraud. Heartland, however, faces a class action lawsuit filed on behalf of financial institutions that have reissued credit and debit cards and now are attempting to recover these and other expenses associated with the breach. The loss of confidence on the part of customers and partners also is a major issue the company is attempting to address [41].

Thus far this report has focused on breaches in companies in the data aggregation and payment processing industries. Large scale breaches, of course, can occur in any organization that maintains large data repositories or does high volume transaction processing. The Open Security Foundation DATALOSSdb web site [42] shows a dramatic increase in the number of breach incidents since 2000, which probably is due mainly to the widespread adoption by states of breach notification laws beginning in 2005. Statistics available on that site show that educational institutions and government agencies account for 42% of reported incidents, while non medical business account for about 46%. Rather than malicious attempts to steal data, many breaches, about 29% of those reported, are simply the result of lost or stolen storage media (tapes, jump drives and laptops). The site also shows that breaches that involve third parties, common in the payment processing industry, often result in a greater numbers of records lost than those that do not involve third parties

III. MONETIZING THE CRIME

What makes large scale data breaches so dangerous is that modern organized crime has developed efficient mechanisms for the sale and wide spread distribution of large quantities of identities and personal financial information [43]. So-called carding forum web sites provide repositories for credit information for cyber thieves around the world. These sites often make available both Track 1 and 2 data for a card. In addition, there are sites that include full information about a victim, so-called "fulls", which include name, address, phone, numbers, SSN, credit or debit card numbers, PINs and a possible a credit history report. This information is of course more costly than just credit card or account numbers. Thieves know that there is a ready market for the proceeds of a large scale breach of financial information or PII that can be used to commit fraud.

Carders (those who run carding sites) typically buy information from hackers responsible for the breach. Carders can break the data into smaller packages and distribute it to lower level carders who may assume the more risky task of making cards information available to end users. End users, sometimes known as cashers, ultimately monetize the stolen information, which involves the most risk and difficulty (fabricating a card, changing an address, etc.). In some card account heists, a world-wide network of cashers fabricates cards and makes withdrawals at ATMs around the world shortly after the breach. The shadow crew site, for example, which was dismantled by the United States Secret Service in 2004, had over 4000 members throughout the world, trafficked in at least 1.7 million credit cards, and caused losses estimated at $4.3 million [44]. Many considered the Shadow Crew to be a loose configuration of cyber criminals, not a highly organized crime group.

A ready market for a large collection of account information creates serious response issues for financial institutions. In a small scale breach that involves 200 accounts, banks can simply reissue cards with new account numbers. The cost to reissue 45 million compromised cards, however, is probably going to be more than any credit fraud so banks won't reissue cards in such a large breach. Thus compromised cards may stay active and available at carding sites long after the breach. Losses to individuals, merchants and banks may continue for some time. ID Analytics [45], a firm that investigates credit fraud, found in one breach they studied that breached information was used sparingly at first, probably to avoid fraud detection. Soon after the breach was discovered, however, there was an immediate increase in activity in the use of breached identities, followed by a sharp drop off in use after the breach was publicly announced.

Recently, a site known as DarkMarket was closed down by its alleged operator. Besides credit card information, the site offered ATM skimmers and other hardware needed for fraud operations. The site's operator said he was closing it because too many law enforcement agents and reporters had gained access to the site, and it was proving difficult to be sure that their accounts had been eliminated. Dark Market even provided review mechanisms that allowed users to evaluate merchandise and weed out so-called "rippers," or those who rip off other fraudsters. In recent congressional testimony [45], Rita Glavin, Acting Assistant Attorney General, expressed concern that international carding forums provided a ready market for large scale data breach contraband. She noted that at its height Dark Market had 2500 members world wide. Late in 2008 in connection with the DarkMarket site, the FBI announced the arrests of 60 people from six different countries including the United States, Estonia, and the Peoples Republic of China. Investigators found more than 40 million credit cards, including some from the TJX breach. An FBI undercover agent who penetrated the site provided further details of the DarkMarket operation at the April RSA security conference [47].

IV. CHALLENGES AND REMEDIES

Each industry presents its own data security challenges. Notable large scale breaches in the data aggregation industry indicate the need to prevent insiders from exceeding authorized access, a challenge in an industry where revenue comes from making data available to partners and clients. In the card payment processing industry, the complexity of the data flows and systems in use make securing data a vexing task. In this section, we focus primarily on remedies proposed and existing challenges in the payment processing industry, which has experience the largest breaches of sensitive financial information.

In 2006, the payment processing industry adopted the Payment Card Industry Data Security Standard [48]. The standard addresses the following areas: network security, protection of card holder data, management of vulnerabilities in system and application software, access control measures, monitoring and testing of network resources, and organizational information security policies. The goal is that all organizations involved in processing payment transactions, i.e., card-issuing banks, merchants, acquiring banks and card brand associations, eventually will comply with the PCI standard. An industry supported council oversees continued development of the standard, certifies organizations as complaint, and certifies PCI auditors who monitor compliance.

Recent congressional testimony on PCI standards [49] by representatives of the card associations, a major retailer, and the National Retailers Association indicate the difficulty of establishing, implementing and monitoring compliance of security standards in an industry as complex as the payment processing industry. For example, the head of fraud control at Visa pointed out that the company serves as the connection point between 1.6 billion payment cards, 16,600 financial institutions, and 29 million merchants in 170 countries. He could have also added that this system includes hundreds of payment processors such as Heartland and RBS who provide the electronic delivery path that connects merchants, card organizations like Visa and Mastercard, and the financial institutions who provide the funds. In addition, these payment processors also handle ATM card and debit transactions for financial institutions. In these transactions, they hand data over to organizations such as NYCE [50], which acts as a clearing house for ATM transactions. The card payment system includes larger retailers such as Wal-Mart, with adequate budgets for data security, as well as small corner stores that have very limited resources. It is not surprising that rates of PCI compliance vary considerably throughout the industry [51]

One frequent criticism of the PCI standard is the requirement that data need be encrypted only on public networks or if stored on devices accessible from public networks. Data on private networks does not need to be encrypted. In fact, typically Track 2 data delivered by retailers to payment processors is not encrypted. In recent congressional testimony, the head of the National Retailers Association and the CEO of a major retail chain both stated that their organizations would prefer to deliver data in encrypted format. Currently, this is not feasible since there is no industry wide encryption standard. After the CardSystems breach and the more recent Heartland breach, both organizations proposed either encryption in back end systems or end-to-end encryption as solutions. The Accredited Standards Committee X9 (ASC X9) of the American National Standards Institute (ANSI) is currently working with payment processing industry to develop the end-to-end standard [52]. The cost would be considerable since merchants would have to upgrade all point of sale equipment to comply with the standard. Some large retailers, however, believe the cost of large scale breaches may make a significant return on investment case for the required equipment upgrades [53].

Retailers criticize the card payment system because it requires them to retain too much data on their systems. Charge-backs present a difficult challenge for the industry since retailers must retain PII in addition to credit card data to uniquely identify transactions and prevent charge-back fraud. Frequently, retailers retain a card number and an address, which might provide credentials for a purchase. Rather than maintain data to track the transaction, retailers would like the payment processor and card association to have systems that can provide them with records of the transaction so they only have to store a signature and a number that identifies the transaction. The Canadian Privacy Commission examination of the TJX Companies breach [54] faulted the company for storing drivers' license numbers and Provincial Identification Numbers, which were taken from about 300 people in Alberta, Canada during the breach and used to commit fraud.

In order to prevent and respond to data breaches on an industry-wide level, the security community in an industry must have detailed knowledge of incidents and vulnerabilities as soon as possible. For most commercial and open source software, information sharing and collaboration regarding software vulnerabilities and available patches have been the norm for some time [55]. In the payment processing industry, where a vulnerable software component could be in use throughout the industry, such information sharing and response capabilities are only beginning to be considered. In March 2009, The Financial Services Information Sharing and Analysis Center (FS-ISAC) formed the Payments Processing Information Sharing Council (PPISC), a forum for sharing information about fraud, threats, vulnerabilities and risk mitigation practices [56]. At the councils first meeting in May 2009, the CEO of Heartland handed out USBs with the malware found on Heartland's systems so other payment processors could try to determine if it was on their systems [57]. Effective deterrence and response require that knowledge of software vulnerabilities and malware be made available, at least to the security community, as soon as it is available.

Card companies increasingly are promoting optional passwords to use with cards [58]. Only a few participating merchants now accept password protected cards, but the number of merchants is increasing. Password protected cards may be particularly attractive to merchants who accept on-line purchases and international transactions. Unlike card present transactions where fraud rates have dropped during the past ten years, credit card fraud associated with on-line and international purchases is a continuing problem for the industry.

The card associations MasterCard and Visa long have used fraud detection systems based on usage patterns to detect anomalous transactions. Their systems store examples of valid transactions and constantly update cardholder data to create a current usage profile. Each new transaction is evaluated against the individual's transaction history. For example, card present purchases of certain types of items outside of an individual's geographic region trigger an alert. These anomalous detection systems have to be consistently updated as thieves consistently find ways to circumvent them. A recent trend is the use of a botnet computer to make an on-line purchase from an IP address that is within the card holder's geographical region [59].

Breach prevention, detection, and response present challenges to law enforcement agencies, the IT industry, and those charged with formulating information security policy. Based on the breaches examined here, the following is a brief summary of the challenges:

> Law Enforcement: 1) Immediate notification in the event of a breach. 2) Enhanced knowledge of carding sites and the role organized criminal activity plays in monetizing large scale breaches. 3) Cooperation among law enforcement agencies and governments throughout the world to facilitate breach investigations.
>
> IT industry: 1) Tracking data in large complex systems. 2) Capabilities for rapid system wide updating and patching. 3) Automated fraud detection tools. 4) Maintaining the integrity of software and systems. 5) Standards for end-to-end encryption in complex distributed systems. 6) Industry wide clearing houses to share breach information and coordinate an industry wide response to a breach.
>
> Information Security Polices: 1) Limiting data collection and retention versus maintaining data for marketing and other activities. 2) Protecting data when there is commingling of proprietary systems and networks with those attached to the Internet. 3) Authorization and auditing polices that address the ease with which large data repositories can be copied.

National breach notification legislation is now before congress [60]. In addition to notification, the bill would force companies holding PII to follow data privacy policies established by the Federal Trade Commission. Proponents claim several advantages of the proposed law: 1) Simplify breach notification requirements for organizations. 2) Establish standards for protecting data. 3) Provide uniform standards by which individuals could check data held for accuracy. Previous attempts at national breach notification legislation raised concerns among privacy advocates because the proposed federal legislation had a lower threshold for breach notification than most state laws, which the bill would have preempted.

The Federal Stimulus bill passed in Feb. 2009 [61] requires notification of health care data breaches. The bill requires all medical providers, health plan administrators, and medical clearing houses covered by HIPPA, and even organizations not covered by HIPPA, e.g., the on-line health record services proposed both by Google and Microsoft, to provide information on breached medical data. Moreover, the law requires the Health and Human Services Dept. to issue guidelines for protection of sensitive medical data. Given the rash of large scale data breaches during the past decade, it is not surprising that recent national breach notification legislation includes provisions for increased government oversight of the use of PII.

V. CONCLUDING REMARKS

Data breaches must be understood within the industries and organizations within which they occur. Notable breaches in the data aggregation industry involved insiders such as contractors who extended their authorized access. Breaches in the payment processing industry made use of malware that relayed sensitive personal financial information to data thieves. Regardless of the industry, however, basic privacy policies that 1) limit the amount of data collected, 2) limit where data is stored and the time for which it is stored, and 3) restrict the use of data to the task for which it was collected, play a critical role in preventing breaches. Large scale breaches are expensive, especially if the information lost involves sensitive personal financial data. Breaches in the payment industry can exact extremely high costs, particularly to organizations such as card processors whose businesses depend on the trust of partners and customers. Breach notification laws, which keep both consumers and business partners aware of what is happening with their data, are changing the way all industries and organizations view information security.

ACKNOWLEDGMENT

This work was supported in part by the Center for Cybercrime Studies at John Jay College and NSF Grant 0619226.

REFERENCES

1. Privacy Rights ClearingHouse, http://www.privacyrights.org/. (Last visited May 31, 2009)
2. Acxiom - About Acxiom, http://www.acxiom.com/about_us/Pages/AboutAcxiom.aspx.(Last visited May 1, 2009)
3. LexisNexis – About Us, http://www.lexisnexis.com/about-us/. (Last visited May 31, 2009)
4. ChoicePoint, http://www.choicepoint.com/. (Last visited June 1 2009)
5. T. Zeller, "MasterCard say security breach affects over 40 million cards," New York Times, June 5, 2005.
6. J. Vijayan, "TJX data breach at 45.6 million card numbers, it's the biggest ever," Computer World, March 29, 2007.
7. J. Vijayan, "Hannaford says malware planted on its store servers stole card data," ComputerWorld, March 28, 2008.
8. B. Krebs, "Data breach led to multimillion dollar ATM heists, Security Fix, The Washington Post, Feb. 5, 2009.
9. B. Krebs, "Payment processor breach may be largest ever," Security Fix, The Washington Post, Jan. 20, 2009.
10. A. Gendar, "ATMs on Staten Island rigged for identity theft; bandit steal $500G," The Daily News, May 11, 2009.
11. Open Security Foundation, DatalossDB Project, **http://datalossdb.org/**. (Last visited June 1, 2009)
12. Accurint, **http://www.accurint.com/**. (Last visited May 5, 2009)
13. D. Solove and C.J. Hoofnagle, "A model regime of privacy protection," University of Illinois Law Review, Feb. 2006, pages 375-404.
14. K. Poulsen, "Chats led to Acxiom hacker bust," SecurityFocus, Dec. 19, 2003. Available at http://www.securityfocus.com/news/7697. (Last visited April 10, 2009)
15. B.J. Gillette, "Data thief exposes flimsy security, nets 8 years," Email Battles, Feb. 24, 2006. Available at http://www.emailbattles.com/. (Last visited April 4, 2009)
16. United States Code, Section 1030 (a) (2) (c). Availalble at **http://www.law.cornell.edu/uscode/18/1030.html**. (Last visited 5/1/09)
17. L. Rosencarnce, "ChoicePoint says data theft cost is $6 Million," Computerworld, July 21, 2005.
18. T.R Weiss, "State officials push choice point on ID theft notifications," Computerworld, Feb. 18, 2005.
19. G. Gross, "Lawmakers call for ChoicePoint investigation," Computerworld, Mach 3, 2005.
20. J. Krim, "LexisNexis data breach bigger than estimated," The Washington Post, April 13, 2005.
21. A. Westfeldt, "LexisNexis warns 32,000 people about data breach," SanFrancisco Chronicle, May 1, 2009.
22. LexisNexis Breach Notification Letter. Available at http://privacy.wi.gov/databreaches/pdf/LexisNexisLetter050509.pdf. (Last visited May 1, 2009)
23. J. Barret, Acxiom Corporation, Testimony before House Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, May 11, 2005. Available at http://archives.energycommerce.house.gov (Last visited May 10, 2009)
24. R. Duran and F. Garcia, "Information security and privacy: challenges in a bad economy and difficult legislative environment," presentation at the Center for Cybercrime Studies, John Jay College of Criminal Justice, March 10, 2009.
25. CyberSource Corporation, "Online Fraud Report: Online payment fraud trends, merchant practices and benchmarks," Available at http://www.cybersource.com. (Last visited May 1, 2009)
26. Federal Trade Commision, "CardSystems Solutions settles FTC charges," Feb. 23, 2006. Available at http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm. (Last visited May 1, 2009)
27. 27 J. Perry, CardSystems Solutions, Testimony before House Subcommittee on Oversight and Investigations of the Committee on Financial Services, July 21, 2005. Available at http://www.house.gov. (Last visited May 1, 2009)
28. T. Krazit, "MasterCard blamed a third party processing firm," Computerwold, June 17, 2005)
29. Federal Trade Commission, "Enforcing Privacy Promises: Section 5 of the FTC Act." Available at http://www.ftc.gov/privacy/privacyinitiatives/promises.html. (Last visited May 1, 2009)
30. See *supra* note 27.
31. PCI Security Standards Council, "About the PCI Data Security Standard (PCI DSS)." Available at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. (Last visited May 4, 2009)
32. M. Mimoso, "Cleaning up after a data attack," Information Security, April 14, 2006.
33. J. Vijayan, "TJX Data Breach at 45.6M card numbers, it's the biggest ever," Computerworld, March 29, 2007.
34. J. Vijayan, "Breach at TJX puts card info at risk," Computerworld, January 22, 2007.
35. Sans Institute, "The evolution of wireless security standard in 802.11 networks: WEP, WPA and 802.11 standards," 2003. Available at www.sans.org. (Last visited March 10, 2009)
36. Office of the Privacy Commissioner of Canada, "Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies," Sept. 25, 2007. Available at http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm. (Last visited May 5, 2009)
37. See *supra* note 8.
38. See *supra* note 9.
39. E. Mills, "Payment processor Heartland reports breach," CNET News, Jan. 20, 2009. Available at http://news.cnet.com/8301-1009_3-10146275-83.html. (Last visited May 1, 2009)
40. J. Vijayan, "Heartland data breach sparks security concerns in payment industry," Computerworld, Jan.22, 2009.
41. Heartland Payment Systems, "Heartland payment systems returns to Visa's list of PCI-DSS validated service providers," May 1, 2009. Available at http://www.2008breach.com/. (Last visited May 5, 2009)
42. Open Security Foundation DATALOSSdb Project, Data Loss Statistics. Available at http://datalossdb.org/statistics. (Last visited June 1, 2009)
43. K. Perreti, "Data Breaches: what the underground world of carding reveals," Santa Clara Computer and High Tech Law Journal, Vol. 25, No. 2, pages 375-413 (2009).
44. D. Gage, "Head of Shadowcrew identity theft ring gets prison time," Security Baseline, June 30, 2006. Available at http://www.baselinemag.com. (Last visited April 10, 2009)
45. ID Analytics, Inc., http://www.idanalytics.com/. (Last visited May10, 2009)
46. U.S. House of Representatives, "Do Payment Card Industry Data Standards Reduce Cybercrime?", Hearing of the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, March 31, 2009. Available at http://www.usdoj.gov (Last visited at May 15, 2009)
47. S. Nicholas, "FBI Agent discusses big cybercrime bust," iTnews, April 23, 2009. Available at http://www.itnews.com.au. (Last visited May 30, 2009)
48. See *supra* note 31.
49. See *supra* note 46.
50. NYCE Payments Network, LLC, http://www.nyce.net/about.jsp. (Last visited May 5 20, 2009)
51. A.Conry-Murray, "PCI and The Circle of Blame," Information Week, pages 31-36, Feb. 25, 2008.
52. Heartland Payment Systems, "Accredited Standards Committee X9 Developing New Merchant Data Security Technology Standards," April 29, 2009. Available at http://www.heartlandpaymentsystems.com. (Last visited May 21, 2009)
53. L. McGlasson, "Heartland databreack: Is end-to-end encryption the answer?," BankInfo Security, May 11, 2009. Available at

http://www.bankinfosecurity.com/articles.php?art_id=1455&pg=1, (Last visited May 30, 2009)

54. Office of the Privacy Commissioner of Canada, "Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies, Inc.," Sept. 25, 2007. Available at http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm. (Last visited May 1, 2009)
55. Financial Services Information Sharing and Analysis Center, "Payments processing information sharing council forms to foster information sharing among payment processors." Available at http://www.ppisc.com/InTheNews.asp. (Last visited May 10, 2009)
56. U.S. Cert, Technical Cybersecurity Alerts, http://www.us-cert.gov/cas/techalerts/index.html. (Last visited June 1, 2009)
57. R. Vamosi, "Heartland comes out swinging after databreah," Computerworld, May 12, 2009.
58. Visa Security and Protection, http://usa.visa.com/personal/security/index.html. (Last visited May 21, 2009)
59. Brett Stone-Gross, et al., "Your botnet is my botnet: Analysis of a botnet takeover," Technical Report, Department of Computer Science, University of California, Santa Barbara. Available at http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf, (Last visited May 30, 2009)
60. Data Accountability and Trust Act, H.R.2221, 111th Congress (2009).
61. 61.B. Bain, "Law requires health data breach notifications," Federal Computer Week, Feb. 27, 2009. Available at http://www.fcw.com/Articles/2009/02/27/Health-Data-Breach-Notification.aspx. (Last visited May 30, 2009)