Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Srinivasan, S. (2015). Privacy protection and data breaches. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* 429-444. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p429-444Srini1984.pdf

Privacy Protection and Data Breaches

S. Srinivasan
Information Systems, Texas Southern University,
Houston, TX, USA

srinis@tsu.edu

Abstract

Data breach is the act of accessing a central data repository without the consent of the data owner. Data breaches are occurring frequently and involve millions of records. Major breaches have been reported since 2005. Often data breaches occur due to someone with malicious intent accessing the stored data. In this paper we look at the types of data breaches and how they impact people's privacy, we introduce a data protection model with the goal of protecting people's privacy. Given today's mobile information needs it is essential to have access to personal data. Social networks are making it difficult to keep personal information private. We provide several different summaries to show the effect of data breaches and data losses on people. We conclude this paper with a set of recommendations to protect people's privacy.

Keywords: Data breach, identity theft, global, security, privacy, social network, protection model

Introduction

Technology growth has enabled more people to use the internet and share information globally. The main drivers of such sharing involve SMS messages and photos. This is also closely related to the widespread use of social media to communicate. Unlike the prior technologies, social media users place much of their personal information online and share it with a small circle of friends. The intent is clear but the consequences are disastrous when such information is stolen from the service provider. This is exactly what has happened over the past several years due to data breaches. Most data breaches exploit some type of system vulnerability. Some data breaches have occurred due to financial greed of a trusted insider and others have occurred due to someone with access to data exceeding their need for data. We will discuss these events as part of the learning process to develop steps to protect customer data.

Hackers want to have greater impact for their exploits. So, they tend to attack central repositories of data available with various retail stores, financial institutions and health care organizations. These organizations take data protection seriously and institute sound policies for implementation. However, these organizations are also growing through acquisition of other smaller entities and incorporating them into their information system. In this process they lose sight of some server that belongs to the network that does not have the same level of protection as the other servers on the system. The hacker gains this knowledge through an employee or through a phish-

Editor: Eli Cohen
Accepted by Executive Review

ing attack. Once the vulnerable access point into the network is identified the hacker enters the network and keeps looking for other vulnerabilities to implant malware. An analysis of several data breaches shows that attackers carried out their exploits over several months after gaining entry into one of the servers. The hackers were usually abroad and kept looking to gain entry into the root server from one of the non-critical servers that were not monitored closely by the organization. In the first major hack of 2007 the intruders spent over a year on the internal systems of TJ Maxx before they started exporting sensitive data out of the system. This observation shows that data breaches are perpetrated over a period of time, not just in one single scoop. The take away from this is that all servers on the network should be monitored for activities, especially activities that originate from outside the system and continue to persist on the system.

Data breaches are not innocuous. Often sensitive data about people's address, date of birth, phone number, email address, userid, passwords, etc. are stolen. This type of data is generally classified as Personally Identifiable Information (PII). The hackers stealing the data often make the sensitive data available over the internet for others to access. Many hacks have resulted in significant financial loss to the organization that was breached. These breaches have also resulted in increased identity theft whereby the effect of the data breach is felt much beyond the initial place where the breach occurred. In United States, many state governments have passed laws requiring the organizations to disclose to their clients the data breach and offer remediation methods. These state laws require notification be sent within a period ranging from 5 to 45 days after the breach is detected. All the states that have enacted data breach notification laws have provided exemption from notification if the breached data pertains to encrypted data. At present there is no US federal law requiring any form of data breach notification. However, US Congress is considering multiple such legislations at this time as this matter has gained greater significance in the wake of some major data breaches such as the 2014 Sony data breach attributed to a foreign government. In the federal system of governance in US, many states have enacted legislation requiring notification of affected parties whenever there is a data breach. All but three states – Alabama, New Mexico and South Dakota – have enacted such legislation. These legislations have varying periods before a notification becomes mandatory. From the time of discovery of breach the organization may have from 7 to 45 days before it needs to notify the affected individuals and offer protection services such as credit monitoring for free up to one year. All these laws have a notification waiver clause built-in if the stored data is encrypted.

As mentioned earlier, there is no federal law on data breach notification requirements. The discussion in this regard revolves around the trigger to be used for notification. One trigger being debated is "harm caused". This is difficult to quantify in all cases. It is evident from the many state laws in place now that they are providing several exemptions from notification. Another issue being debated is the time duration during which notification must be sent. The duration allowed for notification takes into account the fact that it might take a while for an organization to even know that there was a data breach. Prior to sending out notification the organization must be prepared to handle the media publicity and customer enquiries that would be generated. For these reasons, the federal law enactment in this regard is not close at hand. However, there is a new Executive Order on the creation of Cyber Threat Intelligence Integration Center aimed to coordinate sharing of cyber threat information between industry and federal government.

The scope of the data breach problem is drawing the attention of the businesses and consumers. However, the frequency and the magnitude of the data breaches have made the issue significant for the government and the industry but the average consumer has become indifferent thinking that the responsible parties will provide the protection such as credit monitoring and reissue of new credit cards. To get a better picture of this problem we provide two tables below – one pertaining to data at the national level and the other pertaining to California.

The national picture is revealed from an analysis of the annual Verizon Data Breach Investigations Report. This Study has been conducted in collaboration with the US Secret Service and the Dutch High Tech Crime Unit. An analysis of this Study shows that organizational detection of data breach is very low. Table 1 shows the rate of detection for 2010, 2011, 2012 and 2013. The data comes from Verizon Data Breach Investigations Report dated the following year. Table 2 highlights the breach related information from the California Attorney General Reports for 2012 and 2013.

Table 1. Organizational Detection of Data Breach (DB)

	2010		**2011**		**2012**		**2013***	
Overall DB detection	Internal	External	Internal	External	Internal	External	Internal	External
	11%	86%	6%	92%	82%	13%	6%	92%

*Data corresponds to POS and Web App attacks only

Table 2. California Attorney General Data Breach Report

Item	**2012**	**2013**
Loss of PCI data	41%	38%
Loss of PHI data	17%	19%
Loss of SSN	56%	48%
Data breach in Retail	26%	26%
Data breach in Financial	23%	20%
Data breach in Health Care	15%	15%

Brief Analysis of Major Data Breaches

In this section we will examine the cause for data breaches that happened over the last 10 years and the lessons learned to prevent such data breaches in the future. In this discussion we include data loss that occurred without someone with malicious intent hacking into a network. The details presented below show that in many cases the data breach was actually a data loss due to poor data handling practices. Often the data loss occurred due to theft or loss of a portable device with sensitive data kept in unencrypted form. Table 3 summarizes the major data breaches that we address below in this section.

Table 3. Major Data Breaches for the decade 2005 to 2015

Year	**Organization**	**Number of Records Breached**	**Remark**
2005	AOL	92,000,000	Former employee stole data for financial gain
	CardSystems	40,000,000	Policy violation at a third-party card processor exposed data
2006	US Dept. of Veterans Affairs	26,500,000	Laptop and external hard drive with sensitive data stolen from employee home. Data was not encrypted.

Year	Organization	Number of Records Breached	Remark
2007	TJ Maxx	94,000,000	Earliest known large data breach. Hackers stayed within the network for 18 months without being detected.
2008	UK Dept. of Defence	1,700,000	Hard disk with a variety of data lost or stolen
2009	US Dept. of Defense	76,000,000	Defective hardware containing unencrypted data was returned to contractor
	Heartland Payment Systems	130,000,000	Largest involving credit cards
2011	Sony PlayStation Network	77,000,000	Network was down for over a month to fix
2012	Utah Medicaid	780,000	Default password not reset before server went online with health data
	Zappos	24,000,000	Hacker attack on servers
2013	Target	70,000,000	Unauthorized access through Point of Sale systems
2014	Ebay	145,000,000	Hacker attack
	Home Depot	56,000,000	Attack originated at self-service POS terminals
	JP Morgan Chase Bank	83,000,000	Stolen login credentials used to gain access
	Sony	50,000	Fewer in number but highly sensitive data
2015	Anthem Blue Cross	80,000,000	Unencrypted data stolen, but none related to financial data

In the 2005 AOL data breach in which nearly 92,000,000 records were stolen, it was due to an internal employee seeking to gain financial advantage by selling customer data. Encrypting such data alone would not prevent theft by internal employees. Protecting such data requires policy aspects backed up by technological constraints. It is clear from the Edward Snowden data leak on NSA surveillance data that even highly classified data could be stolen by a determined employee. Clearly better policies must be developed and enforced with technological constraints so that internal employees could not steal data. In 2005, MasterCard, Visa, American Express and Discover cards were victimized when the third party credit card data processor CardSystems failed to protect the credit card data that they handled. This data breach resulted in an estimated 40,000,000 credit card data being exposed. The incident report shows that the hacker installed malware on CardSystems' network that extracted the necessary data. Moreover, CardSystems kept a file stored with data on rejected transactions for research, in violation of policy against storing any customer data after the transaction processing. Even though this was revealed through the post-incident security audit, this alone did not cause the massive data breach.

In 2006, the US Department of Veterans Affairs had one of their laptops and external hard drives stolen from the home of an employee. The employee was authorized to take home the laptop and external hard drive with sensitive data for over three years when the theft occurred. The data was unencrypted. This data breach resulted in sensitive personal information of 26,500,000 veterans stolen. The response of Veterans Administration department that the employee violated organizational policy by moving equipment from premises turned out to be erroneous. This incident shows the lack of coordination and knowledge within organizations about security policies. In spite of known benefits of encryption, data was kept unencrypted and allowed to leave premises. This incident shows how security best practices are not widely followed by organizations.

In 2007 TJ Maxx Company revealed that its computer systems were compromised by hackers starting as early as 2005 and they noticed the breach only after 18 months. During this period the amount of credit card information stolen was nearly 94,000,000. The hackers had the decryption key for the encrypted data stored by TJ Maxx and so the encryption did not protect the stored data. This incident also showed the violation of storing credit card information beyond the transaction processing time, a violation that was noted with CardSystems earlier. In this incident the hackers had access to the systems for a very long time without being detected. This shows the need for better policy and monitoring guidelines to be followed.

The data breaches occurred in other countries as well. In 2008, there were numerous data losses in United Kingdom’s Ministry of Defence. Majority of the losses occurred when either a laptop or flash drive was lost or stolen outside the offices. Much of the lost data was unencrypted. These incidents show that data breaches and losses are preventable if sensitive data was kept encrypted and required to be kept on premises.

In US, some of the major data losses occurred in 2009. Two of the major data losses each involved several million records. The Department of Defense which stored information on veterans in a RAID disk realized that the hardware was defective and so returned the hardware to the contractor who sold it to them without first removing the data stored in the drive. This RAID drive contained data for 76,000,000 veterans in unencrypted format. When the contractor realized that the device could not be repaired, it was sent for recycle. Even though there was no specific harm caused by this poor practice, it is still considered a data breach because there was the potential for harm for millions of veterans. Another major data breach occurred when Heartland Payment Systems was hacked and 130,000,000 data records were possibly stolen. The data involved in this case related to credit card data processed for over 250,000 businesses. The hackers installed malware and siphoned off data from this credit card data handler. This hack went undetected for nearly 7 months. Heartland was responsible not only handling credit card data between the retailer and the merchant banks but also for transfer of funds between these institutions. One of the lessons learned from this data breach is the creation of new processes whereby data encryption occurs at the POS terminals. This new approach is still not mature but has the potential to provide better security as the data moves through multiple networks from POS terminals to payments to merchants through banks.

Even though every data breach appears to have had disastrous consequences for the merchants and financial institutions, the Sony hack had a different level of impact on the public. The 2011 hack involved nearly 77,000,000 customers worldwide who belonged to Sony PlayStation Network (PSN). In the course of settling some issues with the public Sony thought that it had resolved the contentious issues. However, the group Anonymous mounted a well-publicized attack on PSN which resulted in Sony having to pull their systems offline for six weeks, causing significant disruption to its base of gamers spread around the globe. This attack on Sony PlayStation Network revealed that Sony was collecting plenty of data about the devices and users on its network that several users were unaware of. Attackers used the power of Amazon EC2 cloud computing service to acquire the necessary computing power to crack the encryption used by Sony for the stored financial data. Other personal information about users were stored in unencrypted format. In the section on cost of data breaches we will discuss the cost to Sony due to this data breach.

An overview of data breaches shows that health care data is often breached. A case in point is the 2012 data breach that occurred in Utah. A new server was placed online with health care data of nearly 780,000 people. This server still had the default password settings for access which a hacker found out and stole data about people that included Social Security Numbers (SSNs). It is important to note that large financial institutions still use SSNs to authenticate the customers and so perpetrating Identity Theft becomes much easier once the thief has the SSN of an individual. Once again this breach shows the prevalence of human errors that contribute to the data breaches. Another major breach that occurred in 2012 was with Zappos.com, an online retailer of shoes. Hackers broke into the company servers and stole customer data for 24,000,000 customers. Even though the passwords were encrypted as per PCI guidelines, much of other customer data was in plaintext. There are plenty of tools available to decrypt simple passwords quickly. Thus, the encrypted passwords that were not strong would be easy to decrypt. Moreover, customers use the same email and password combination with multiple accounts. This gives the hackers an easy target to defraud customers who used simple passwords. This incident shows that encrypting passwords alone is not sufficient but use of strong passwords is critical. As we saw from the many state laws enacted to address data breach, there is a notification waiver if the data was encrypted. This incident shows that encryption alone does not offer protection and notification of breach might still be needed. Zappos is currently part of Amazon but maintains its identity on the web. Amazon’s SEC filings identify as a separate item thereby we can find revenue figures for Zappos.

The Target store data breach of 2013 turned out to be a game changer. It was a sophisticated hack performed from abroad that pilfered credit card data from POS terminals. The hack occurred during the peak of the Christmas holiday season and lasted nearly three weeks. This data breach impacted 70,000,000 customers who shopped at Target stores during the Christmas holiday period in 2013. In addition to being a costly matter for Target to deal with this data breach, the CEO of Target was forced to resign along with the CIO. Financial institutions that issued those credit cards had to reissue new credit cards to customers. This also showed the need to treat purchases online with greater care since the new EMV cards have a chip implanted with greater security possible.

In 2014, there were four major data breaches reported. The first one mentioned here was at eBay. Attackers entered the eBay network in February 2014 and were detected by eBay only in May 2014. Even though PayPal is a subsidiary of eBay, none of the information from PayPal was stolen in this attack. eBay reported that personal information on 145,000 customers were affected. In many cases the encrypted passwords and userids were stolen. There was an online posting purporting to sell the stolen data but it was considered fake data. The good thing to note in this incident is that the encryption used by eBay was strong irrespective of the strength of user passwords. eBay added additional digits to the user password known as salt before encrypting the password. This process makes decrypting the password lot more difficult. One policy issue that came into light from this incident is that eBay attached greater security protection to the payment data in PayPal than the customer data of eBay customers consisting of addresses, phone numbers, email addresses and passwords. The hackers who broke into the eBay network stole login credentials for eBay employees and so they were able to access the data they wanted. This shows the need to elevate the security protection level for employees’ login credentials. Most organizations do not have any specific policies to this effect.

The second major data breach of 2014 occurred at Home Depot. This data breach resulted in data loss of 56,000,000 customers. Home Depot reported that the breach occurred at the Self-checkout

Lane terminals where the hackers had installed their malware to steal credit/debit card data. Hackers were able to enter the Home Depot network using a stolen third party vendor credentials. Once inside the network with limited access they were able to exploit a vulnerability and elevate their privileges to install the malware. The data breach occurred in US and Canadian stores of Home Depot. The malware identified is a variant of BlackPOS. The infected POS terminals all were running Windows OS. Often the breach is detected by third parties such as banks or government agencies. They monitor the activities of Rescator.cc, an organization known for selling stolen credit/debit card data in batches. This breach was first publicized by others one week prior to Home Depot announcing the breach. An analysis of the data breaches at Target and Home Depot shows that the companies do not take security seriously.

The third major data breach of 2014 occurred at JP Morgan Chase Bank during summer. It affected 76,000,000 million households and 7,000,000 small businesses. Non-financial data was stolen in this attack. It took two months for Chase Bank to detect that data has been stolen. Like the other data breaches this data breach was also detected by third parties first. Attackers gained entry into the corporate network after stealing login credentials of an employee. Since the security system used in a server did not have two-factor authentication the hackers were able to gain entry. Information stolen related to customers' address, phone number and email address but not passwords or any financial data. The lesson learned from this breach is that all servers on the network should be protected.

The fourth data breach occurred at Sony Pictures Studios in California. In this leak, Guardians of Peace (GOP) were the attackers and they claimed to have acquired several terabytes of data, somewhere from 12 to 100 terabytes of data, on Sony's current and former employees, numerous emails, other celebrities and several Sony movies in development. The number of records involved in this breach is far fewer than previous breaches but this had sensitive data of different kind. It is estimated that the breach involved data about approximately 50,000 individuals. Prior breaches involved financial or health care data about individuals. In the Sony breach, the attackers demanded financial payoff and other actions from Sony in order to not release the stolen data. The attackers provided their contact information briefly but law enforcement was not able to precisely identify them. The attackers appear to have gained access to Sony network through stolen credentials or with help from some internal employees. Unlike all the prior data breaches, this breach appears to have involved not only stolen data but also several systems that were completely erased.

We conclude this section with some information on the latest mega data breach at Anthem Blue Cross. This data breach was detected in late January 2015 by Anthem and steps were taken immediately to notify the customers affected in multiple ways. The breach affected 80,000,000 current and former customers as well as employees of Anthem. The data stolen related to names, addresses, dates of birth, social security numbers, email addresses, employer information and income data. The stolen data was not encrypted. No health care data was stolen but yet identity theft for several people are a real possibility because the social security numbers and dates of birth were stolen, two key pieces of data needed to establish a new identity for someone.

Data Protection Model

In this section we develop a Data Protection Model for protecting people's privacy. The goal is to build safeguards into protecting PII and deal with a data breach. Adherence to the model will help with risk mitigation. Analysis of the data breaches shows that attackers gain entry into a network using legitimate credentials. This fact leads us to focus on policy based authentication and persistent monitoring of user activities on the network. The respective policies for these types of users are enunciated below:

Employee Access Control

Employees have an onboarding process. In developing this policy based approach we have taken into account that some employees may not have a physical organizational location nor organization-supplied equipment. Hence, all employees must set up additional credentials for later use during remote access. Implementing this policy gives the organization an ability to authenticate a legitimate user. Employees with an organizational location and hardware should be allowed access to the network if the access request originates from a known location and hardware. Traditional userid and password combination combined with organizational location and hardware ID should facilitate this process. For non-organizational location or hardware, use the additional credentials established during onboarding process.

Partner Access Control

Partner access monitoring has becoming critical because in several of the recent data breaches the attackers gained access to the network using stolen partner credentials because many partners lack the resources to protect such information. The policies in this regard are described next.

a. Pre-register partner hardware ID
b. Have a secondary channel validation code distribution to partner. The secondary channel could be either a mobile phone or a non-organizational email. In either case the code should be sent to a predetermined number or email address.
c. At periodic intervals require revalidation of user
d. Limit access to sensitive data using two-factor authentication

Guest Access Control

If guest access is required to organizational network, have minimal privileges associated with such accounts. Log guest credentials. Limit guest access to preset time intervals such as 30 minutes.

In order to protect the network and data, all users must be validated at periodic intervals using external channels of communication such as mobile phone. Hackers exfiltrating data often hide it in other documents. Thus, movement of data out of the central repository should be monitored. Advanced Persistent Threats (APTs) are difficult to control. Analysis of the data breaches shows that attackers linger in organizational network for an average of 220 days before they are detected. Typically the attackers accumulate the data of interest for them inside the network and exfiltrate the data in a span of 15 minutes. Such exfiltrations occur during times of heavy use of the system since the organization might not be monitoring all traffic due to response time considerations. The policy based methods discussed in this section provide some level of control for the organization against data theft. However, it will be extremely difficult to prevent all data theft when much of the activity on a network happens in an automated manner. We have summarized these steps in Figure 1.

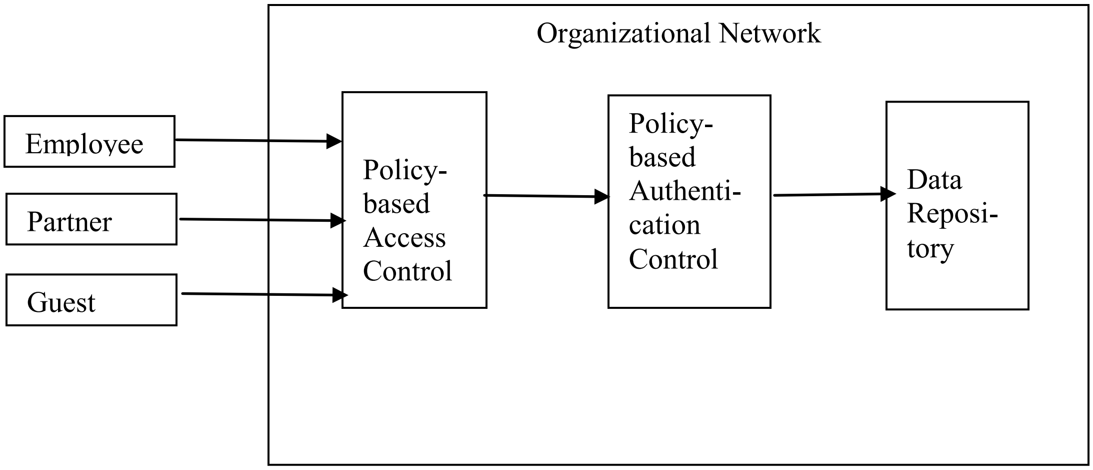
Organizational Network
Employee
Partner
Guest
Policy-based Access Control
Policy-based Authentication Control
Data Repository

Figure 1. Data Protection Model

Anatomy of the Target and Sony PlayStation Data Breaches

Target, like most retailers, has a Security Operations Center (SOC) but does not monitor that as closely as a big bank, defense contractor or a government agency would do. In the case of Target they had installed the malware detection software FireEye in their systems. CIA also uses FireEye. This system was being monitored by Target from its Bangalore, India location. When FireEye detected the malware in late November when the hackers installed data exfiltration software to move the stolen credit card information out of Target servers to their computers in Russia, it notified the Corporate Head Quarters. No one at Target SOC acted on the information. Later, when the Department of Justice notified Target of the hack around December 15, 2013 then Target started looking into it and realized the data breach. This points to human failure for action. US Secret Service which monitors financial fraud of all types noted that the malware used in the Target breach has been used in several other attacks as well.

The hackers gained access to Target network using credentials that they stole from a Target vendor, in this case a HVAC contractor. This contractor was not providing HVAC services to Target stores but had other business with Target for which he was accessing Target network to submit electronic invoices. This allowed access into Target network for the hackers but they could not do much immediately because of the limited permissions this account had. However, since they were inside the network, they were able to probe the network for vulnerabilities and exploit one of them to gain elevated privileges, which eventually led them to install the malware. As mentioned above, Target did not heed its own security monitoring warnings about malware. Further, it became clear that Target did not isolate its sensitive and non-sensitive data and provide adequate defenses to protect the sensitive data. Target is PCI compliant. PCI standard requires two-factor authentication for remote access to sensitive financial data. However, Target did not require all third party vendors with access to Target network to have two-factor authentication. The classification of vendors by the nature of their association with Target dictated the level of credentials verification. As a policy this might be acceptable but combined with other internal failures in monitoring this turned out to be highly disastrous.

Analysis of the Target attack shows that the stolen credit card data was accumulated in Target servers for several days and then moved to external servers located in Russia and elsewhere over several days. Typical security policies require monitoring external movement of sensitive data. This was apparently lacking in Target's security practices. One thing that stands out from Target's post hack analysis is that heeding to security alerts is critical and that using simple tools such as FTP (File Transfer Protocol) to move sensitive data should be prevented.

Next, we analyze the Sony PlayStation hack to see what lessons could be learned. This particular hack clearly shows that even a highly visible global brand company is no match when it comes to defend itself from determined hackers. Sony PS3 (PlayStation 3) had a successful launch in 2006 and had a feature called 'Other OS' that users could use to run other operating systems on PS3. When PS3 Slim was introduced in 2009 without the 'Other OS' feature and the automatic firmware update for all PS3s on the market to remove the 'Other OS' feature, several users felt that Sony had breached the contract. This group of approximately 10 volunteers known as 'failOverflow' led the attack on the PS3 security system and succeeded in exposing the system vulnerabilities. The 'failOverflow' attack exposed that the PS3 controller did not enforce separation of code and data spaces as well as it did not have 'Run Time Integrity Check'. Moreover, the security flaws enabled the attackers to gain access to root signing key. These three vulnerabilities were exploited by 'failOverflow'. They made available a USB device with 'jaibreak' capability to run other OS on PS3. Ultimately Sony decided to install firmware update that would block the 'jailbreak' but at the same time allow 'jailbreak' to run outside the PlayStation Network. Even though Sony came to this compromise after having to pull down the PSN for over a month to fix the flaws, the lessons learned show that the designers should test the systems for security flaws in all its components, keep executables in separate space from data and do run time integrity check in order to verify that systems do not run unauthorized software beyond initial authentication of system.

The Sony hack affected nearly 100 million gaming customers worldwide besides exposing personal information about thousands of customers. The attackers also accessed user IDs and passwords that were stored in unencrypted format. As mentioned above, the hackers found the root signing key and made it public. The root signing key would enable the users to play pirated video games. This possibility led Sony to file a lawsuit against one of the hackers. The lawsuit's premise was that the root signing key publication violated the Digital Millennium Copyright Act's protection for Sony PS3. Sony settled the case with the hacker in exchange for the ban on hacker launching any future attacks on Sony. The determined attack by a group of hackers exposed Sony system's vulnerabilities. The main lessons learned from this attack experience is that internal users could facilitate significant attacks, systems should be tested for strong authentication for all critical components and implementing run time integrity check could prevent unauthorized systems running on the network. Apparently the significance of the threat that current or former employees could pose was not noted by Sony and it came to haunt them in the 2014 hack as well.

General Observations on Data Breaches

Typically data breaches occur when the hacker has a financial motive. Often the stolen data pertains to credit card or health information. Stolen data are sold through underground platforms that tout such information. Law enforcement is aware of such websites and monitor them for activities or disclosures of stolen data. This is one source of information that is used by law enforcement to alert the organizations that have been hacked. In over 90% of the cases the organizations that were hacked were unaware of the hack until brought to their attention by a third party. Among the organizations, financial institutions are better prepared to handle an attack and prevent data breaches often. They have better monitoring of their systems to detect any unusual activity. The stolen data is often used for identity theft, which is a very serious matter for individuals concerned. Health Care organizations are often the target of attacks for data breaches. Penalties for loss of health care information is significant through HIPAA implementation. In health care field the breaches occur due to poor controls and insufficient risk analysis. Attackers are focusing on all endpoints to see which endpoints are vulnerable. It is often the case that many third party vendors who may have simple access to a major organizations often lack the resources to protect their systems. Since third parties often have limited access many organizations do not monitor them carefully. This assumption is being reevaluated in light of the Target hack of 2013.

Hackers of financial systems often target the POS terminals. POS terminals are often at risk of being hacked because they are deployed in large numbers and are located at many small merchants' premises. These small merchants lack the resources to monitor for hack or take any action if one is detected. Often confusion prevails as to who is responsible for taking action to fend off the data hack. Small merchants assume that it is the responsibility of the vendor who sold them the POS terminal or software. These merchants expect the vendor to be responsible for the management of the system. The credit card industry in US is in transition by moving to the new EMV cards with chips embedded. PCI has laid out a timetable of October 2015 (for non-gas stations) and October 2017 (for gas stations) to transition responsibility to merchants for any loss for non-compliance with the EMV cards processing. However, many merchants have not made the transition to process EMV cards with the chips present. They are still being processed as magstripe cards. It remains to be seen if merchants would embrace the EMV cards with chips for the added security. Even this enhanced security feature is not expected to put a dent on credit card data theft because the US adoption plan does not require a PIN to be used with the use of credit card as in a debit card transaction. The reason for this approach is the customer convenience.

Hacks with a financial motive were the principal causes in all data breaches until the Sony PlayStation hack of 2011 and the Sony hack of 2014. Analysis of the information available on these two hacks showed that insider help made it feasible for the hackers to cause significant damage quickly. The 2011 hack was due to ideological differences with the Sony approach and the 2014 hack was due to lax enforcement of good security practices. These two attacks throw open the possibility for new types of data breaches with severe consequences. The current approach to data breaches centers around detecting data breach attempts early and thwarting them quickly. The new threats may not attempt to exfiltrate data for financial gain, identity theft or espionage. The threat may involve simply affecting data integrity by modifying data pertaining to individuals. In this context we consider changes to someone's health information or financial information. The change in health information could indicate to treating physicians wrong picture of a person's health, warranting more costly or dangerous diagnosis or treatment. On the financial side, it could either tremendously boost someone's financial health or affect it adversely. Thus, the focus of data breach should be to detect changes in stored information which in itself would trigger multiple actions such as notifications sent to the affected parties who would then be able to know if the change was warranted or not. This approach would help the organizations more in monitoring access to data.

In this context of data breaches we test two hypotheses:

H1: A data breach event at an organization would adversely impact the organizational finance

H2: A data breach event at an organization would adversely impact the organizational reputation

To test the first hypothesis, we looked at the financial situation of the organization pre and post breach. Of the 9 publicly traded organizations that we looked at, only CardSystems as a business closed. However, the business was sold to Pay by Touch, which eventually closed as well. Zappos was acquired by Amazon and so it is difficult to get the financial situation pertaining to Zappos only. Hence, we give below the financial data for the remaining 7 businesses. To test the hypothesis H1 we looked at the organizational finance of these 7 publicly traded companies immediately preceding the breach and for three years post breach through their Securities and Exchange Commission (SEC) filings. This data is summarized in Table 4.

Table 4. Summary of Finances Pre- and Post- Breach

Company	Breach year - 1	Breach year + 1	Breach year + 2	Breach year + 3
TJ Maxx	$15,955,943	$18,336,726	$18,999,505	$20,288,444
Heartland Payment Systems	$1,544,902,000	$1,855,839,000	$1,985,577,000	$2,013,436,000
Sony	¥7.2 trillion	¥6.5 trillion	¥6.8 trillion	¥7.77
Target	$69.87 billion	$71.28 billion	$72.62 billion (projected)	N/A
Ebay	$16,047 million	$17,902 million	$4.5 million in Q1	N/A
Home Depot	$5.385 billion profit	$6.345 billion profit	$7.179 billion profit projected	N/A
Chase Bank	$96.606 billion	$94.205 billion	$24,8 billion in Q1	N/A

Note: Since the data breach occurred late in the year for Home Depot and Chase Bank, we used the data from the year of breach for the column Breach year + 1.

The analysis of the data clearly shows that none of these businesses were affected by the breach in terms of their net sales or profit margins. In fact, there is information in the public media that indicates that some of the organizations were breach occurred, pulled back their marketing expense because of the free publicity from the breach, albeit in a bad light. Hence we conclude that our hypothesis H1 is validated and H2 is shown false.

Cost of Data Breaches

Data breaches cost the organizations both in direct costs to recover from the breach and indirect costs that result in loss of customer confidence in the organization’s ability to provide online access to their products and services. The direct costs include the cost of providing credit monitoring for affected customers, notification cost, phone support for customer concerns, penalties levied by groups such as PCI, penalties levied by government agencies under HIPAA, SOX, GLBA, FERPA, and forensic examination to understand the cause and depth of data breach. The indirect costs are more of an estimate based on loss of customer confidence and patronage, impact on the stock price of the organization, and the new steps taken to secure the network systems and access points to the network. It costs anywhere between 10 to 100 times the cost of securing the system prior to the attack. In order to compare the cost of data breaches we should only look at direct costs. Companies are trying to protect themselves against data breaches and its consequences by taking separate insurance. Later in this section we will closely look at the insurance angle of data breaches.

A quick look at the cost of the major data breaches discussed above shows that it has run into several million dollars. The Target data breach cost the company $246 million. It recovered $90 million of that from its insurance. The Target stock price dropped by 46% after the disclosure of data breach. Home Depot data breach cost the company $62 million. It recovered $27 million from its insurance. There was no impact on its stock price due to the data breach. Sony PlayStation Network breach cost Sony $171 million. So far Sony has been unable to collect any of the costs incurred from its insurer because the courts ruled in favor of the insurer. This particular breach has shown that organizations need to take specific cyber insurance to cover costs associated with a data breach. Some organizations are taking the “self-insurance” aspect to save the cost of insurance.

The Ponemon Institute and IBM have been studying the cost of data breaches annually over a nine year period. This study shows that the cost of data breaches per record has increased from $188 to $201 over the last two years (Ponemon Institute, 2014). As noted earlier, the direct costs associated with a breach involve many aspects. We have not included in the cost the impact of data breaches on the stock price of the business after the breach. Most businesses have realized the importance of additional insurance to cover data breaches. An analysis of 117 insurance claims due to data breaches by NetDiligence shows that the average cost per record jumped from $307 in 2012 to $956 in 2013 (NetDiligence, 2014). This study breaks down the payouts by the type of information lost such as PII, PHI or PCI. The PII includes all personally identifiable information including email addresses and passwords. The maximum claim payout by insurance companies for 2014 in each of these categories is as follows:

Payout for PII data loss	$7.3 million
Payout for PHI data loss	$13.7 million
Payout for PCI data loss	$11.75 million

These numbers show that many businesses are hoping to recover some of the data breach costs through their cyber insurance policies. Thus cyber insurance policies are becoming more common among businesses now and the corporate boards are paying greater attention to cybersecurity.

Data breaches are not confined to any one country. It is a global phenomenon. In 2013, Ponemon Institute studied the impact of data breaches by calculating the cost per record across multiple countries. Based on the data available for both 2011 and 2012 we are able to compare the cost per record for data breaches in eight countries. Table 5 shows that the average per record cost due to data breaches decreased in three countries, increased in four countries and remained the same in one country.

Table 5. Average per record cost of data breach

Country	2011	2012
Australia	$145	$133
England	$124	$132
France	$159	$168
Germany	$191	$199
Japan	$132	$125
India	$42	$42
Italy	$102	$124
USA	$194	$188

The cost analysis due to data breaches also shows that many businesses are focusing on forensic examination of evidence to understand the root causes for the breach and corrective action. Also, companies are seeking legal coaching to defend against customer lawsuits. The significant portion of the cost in dealing with data breaches still goes to notification of affected customers and regulatory bodies, credit and identity theft monitoring for a period ranging from 12 to 24 months, managing a hotline to address customer concerns and penalties levied by regulatory bodies and government entities monitoring the businesses.

Privacy Protection

People expect the organizations that collect their personal data to protect such data from abuse. Often data breaches result in loss of customer data which could include address, phone number, social security number, date of birth, credit card number, email address and password. The hacker could then sell this data online and the purchaser of such data could steal the customer identity. The notification laws in 47 of the 50 states require the businesses that experienced a data breach to notify the customers in a timely manner so that the affected party could take the necessary steps to protect their identity. In the protection model discussed in section 3 we outline policy-based access control mechanisms to such data. Enforcing these policy-based access controls will enable a business to know that people gaining access to their systems have a legitimate function to fulfill. Organizations that collect and store customer data should place high emphasis in protecting that data because loss of such data could result in a privacy violation. For example, someone performing his/her duty in their official capacity might disappoint a customer. In such situations the customer should not be in a position to get hold of the official's home address, phone number in order to harass them or even physically harm them or their dependents. Thus, privacy protection is of paramount importance to the people who share their data out of necessity.

One of the common tools available to protect customer data is encryption. Standard encryption techniques afford a high level of reliability. Sometimes external systems that the organization permits might need to access customer data. In such cases the format in which the data is stored becomes a problem. Typically, systems process social security numbers as 9 numeric digits. When encrypted data is accessed, the encrypted social security number may be larger than 9 characters and all characters may not be numeric. To avoid this type of problem the organization may have to choose the more expensive option of choosing a format preserving encryption scheme. This might make it difficult for some businesses to automate some of the processing in order to protect customer privacy.

Businesses have the option of implementing multi-factor authentication in lieu of encryption to enforce access control. Even though multi-factor authentication would involve something more than the userid and password, implementing such a system properly is expensive. Often businesses use a variation on the multi-factor authentication by asking the users to set up answers to challenge questions. In many instances this approach to access control may be adequate. However, for more sensitive personal data such as social security number and date of birth, a differentiated access control system must be established. Also, partners who seek access to organizational customer data must be vetted properly so that the data does not fall into the wrong hands.

Summary

This paper describes the major data breaches that occurred since 2005. Usually loss of data results in identity theft. In order to protect customer privacy many states have enacted breach notification laws. We identify the 47 states that have enacted such laws. There is no single federal data breach notification law in place. Because of that businesses dealing with a data breach will have to follow the various requirements of states such as the time allowed for notification and the waiver requirement for notification if the data is encrypted. Even though encryption might protect passwords, when a hacker steals passwords and uses a password cracker algorithm they would succeed in cracking very simple passwords. Most organizations that take the precaution of encrypting passwords do not require the customers to use a strong password such as the ones requiring the use of non-dictionary words, use of upper and lower case letters, numbers and special characters. For this reason, it might be necessary for organizations that use encryption to seed all passwords before encrypting. This would provide a higher level of protection for stored data. Another requirement that we have identified for protection against data breaches is access control. The model developed in this paper uses a policy-based approach to data access. Overall, the organizations that have experienced a data breach have been successful in maintaining a growth, without any harm caused to its brand.

References

Baker. (2014). *Data breach notification laws by state*. Accessed 5/27/15 from http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf

California DBR. (2014). *California data breach report*. Accessed 5/29/15 form https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf

Cavoukian, A. M. (2012). Privacy by design: Origins, meaning, and prospects for assuring privacy and trust in the information era. In G. O. M. Yee (Ed.), *Privacy protection measures and technologies in business organizations: Aspects and standards* (Ch. 7). Hershey, PA: IGI Global.

ITU. (2012). *Privacy in cloud computing.* ITU-T Technology Report. Accessed 5/22/15 from http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

Net Diligence. (2015). *The real cost of a data breach*. Accessed 5/28/15 from http://www.allclearid.com/business

Ponemon Institute. (2013). *Cost of data breach report*. Accessed 5/23/15 from https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Ponemon Institute. (2014). *2014 cost of a data breach study: United States*. Accessed 5/29/15 from http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf

Ponemon Institute. (2014). *Is your company ready for a big data breach?* Accessed 5/29/15 from http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

Privacy Rights Clearinghouse. (2015). *Data breaches.* Accessed 5/26/15 from http://www.privacyrights.org/data-breach/new

Verizon. (2011). *Data breach investigations report*. Accessed 5/29/15 from http://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf

Verizon. (2012). *Data breach investigations report*. Accessed 5/29/15 from http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

Verizon. (2013). *Data breach investigations report*. Accessed 5/29/15 from http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf

Verizon. (2014). *Data breach investigations report*. Accessed 5/29/15 from https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf

Biography

S. Srinivasan (nickname Srini) joined TSU on August 1, 2013 as Associate Dean for Academic Affairs and Research as well as a Distinguished Professor of Business Administration. Prior to coming to TSU, he was the Chairman of the Division of International Business and Technology Studies at Texas A & M International University's A.R. Sanchez School of Business in Laredo, TX. He was there from 2010 to 2013. Before coming to Laredo, he spent 23 years at the University of Louisville (UofL) in Louisville, Kentucky. At UofL he held joint appointments in the Computer Information Systems Department in the College of Business and the Computer Science Department in the Speed School of Engineering. During his time there he started the Information Security Program as a collaborative effort of multiple colleges. He was Director of the InfoSec program until 2010 when he left for Laredo. The program was designated a National Center of Academic Excellence in Information Education by the National Security Agency (NSA) and the Department of Homeland Security (DHS). He successfully wrote several grant proposals in support of the InfoSec Program. His first book on Cloud Computing titled “Security, Trust, and Regulatory Aspects of Cloud Computing in Business Environments” was published in March 2014 by IGI Global, Hershey, PA. The second book on Cloud Computing titled “Cloud Computing Basics” was published in May 2014 by Springer, NY. His area of research is Information Security. He is now working on a new project on Big Data Analytics. He has taught the Management of Information Systems course at the MBA level in US as well as in international programs in El Salvador and Greece. He has spent his sabbatical leaves from UofL in Siemens at their R & D facility in Munich, Germany; UPS Air Group in Louisville, KY; and GE Appliance Park in Louisville, KY. Besides these industry experiences, He has done consulting work with US Army, IBM and a major hospital company in Louisville, KY.