Introduction to PCI and PII:
Securing Your Organization's Data

SHERPA SOFTWARE

Executive Summary

Just about every day, the national headlines include stories about data breaches that have compromised the security of thousands or even millions of confidential electronic records, often containing credit card or social security numbers. Usually, this occurs at organizations found to be in violation of various regulations or industry standards designed to prevent such incursions. These notable hacks and thefts have prompted organizations to look to their own policies to avoid becoming the next front-page story.

Enter the Payment Card Industry (PCI) & Personally Identifiable Information (PII) standards. This white paper will cover:

- **Types of PCI and PII found in most organizations**
- **Notable breaches**
- **Costs associated with data loss**
- **Identifying PCI and PII & Establishing Policy**
- **Using redaction to secure data**
- **Recommended software for mitigating risk**

Common Types of PCI

Two key areas of data compliance revolve around PCI and PII. Payment Card Industry (PCI) data falls under the aegis of the *Data Security Standards*, currently in version 3.0, promulgated by a council of global payment brands (Visa, American Express, etc.). The standards apply to all retailers that accept credit/debit cards for payment, with these merchants falling into one of four tiers, based on their volume of card transactions.

In short, the objectives of the standards are to:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Personally Identifiable Information (PII) includes items such as social security numbers, date of birth, personal health information, and other data that can be linked to an individual. In fact, a *Stanford study* found that ***63% of the US population can be identified only by the combination of the person's gender, zip code and birthdate, making the stakes of protecting PII incredibly high for any organization.***

Common Types of PII

- Government issued identification – Social security numbers, driver's license information and the like can be linked with personal information (date of birth, mother's maiden name, etc.) to uniquely identify individuals making them prime targets identify theft.

- Healthcare data – An individual's health record contains extremely private patient details and is protected by HIPAA (named for the Health Insurance Portability & Accountability Act of 1996) and other regulations.

- Mobile & App Data - Many companies have mobile apps that collect location and behavioral data that is very specific and could identify users. *Apple suffered a data breach of their iCloud service in 2014 where many users' personal files and photos were available for all to see.*

- The Internet of Things: As web connected devices, such as wearable health trackers, are growing in popularity, so will the amount of collected data. *FitBit* and other tracking devices can be open to hacking and misuse of information.

- Website registrations - Most websites collect customer data including email or home addresses via forms or downloads for lead generation. These companies are responsible for keeping this data secure.
- Biometric data – Fingerprints, retinal scans and other biological markers that aid in identification usually used to control access or prevent crime must be protected.

Various privacy laws and industry regulations are responsible for detailing how PCI and PII records should be handled. Recommended protections range from maintaining secure networks to managing the flow of private information. For data stored at rest (e.g. on file shares or email servers), the details generally boil down to:

Don't transmit or store PCI and PII in plain text

Audit your systems

Enforce policies to ensure your organization remains in compliance

Understanding the effect PCI and PII have on businesses is no longer solely the responsibility of records management or the IT department.; Data breaches will affect an entire organization. Departments and key stakeholders must come together to establish policies and procedures to protect sensitive information.

Notable Breaches

The costliness of PCI and PII data breaches have certainly grown over the years. Settlements don't cover the true cost of theft or leak, but are often the yardstick by which such events are measured. Some examples include:

- Target - 2015 - $39 million settlement paid to several banks after the loss of *40 million customer's financial data.*

- Sony – 2015 - A *$5 million settlement* with employees after embarrassing emails were not secured.

- In 2016, Wendy's *was named in a class-action lawsuit* alleging they did not secure customer PCI adequately.

- Home Depot is embroiled in a suit regarding a *cyber-hack* that exposed PCI data in 2014.

- The IRS *lost nearly half a million* E-File PIN numbers during a data breach in early 2016.

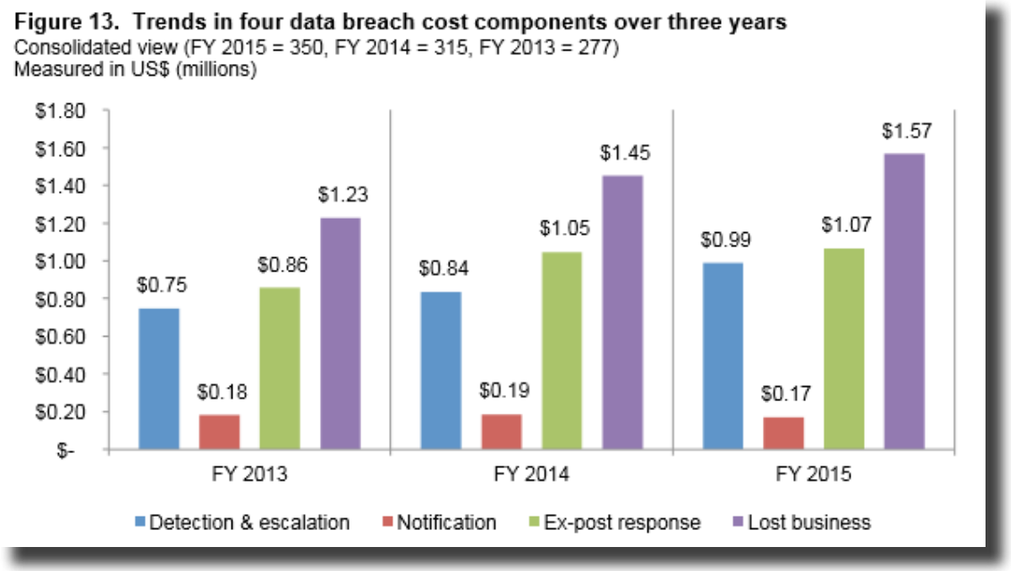
- *Hackers stole over 21 million* records from U.S. Government databases, including biometric data and security clearance background information.

The Cost of Data Loss

Giant settlement amounts from household names will always stand out. However, IBM has studied the origins and costs associated with these types of data loss and published findings in *2015 Cost of Data Breach*: Global Analysis comparing 350 companies in 11 countries.

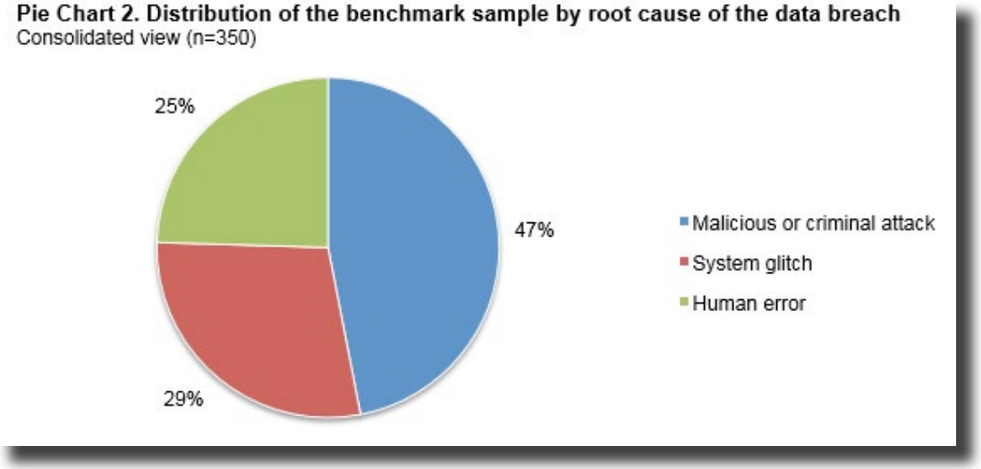
"The study found the average consolidated total cost of a data breach is $3.8 million... The study also reports that the cost incurred for each lost or stolen record containing sensitive and confidential information [is]... $154."

Lensed in those very real terms, organizations can see what is at stake with protecting sensitive PCI and PII. Investigating IBM's breakdown of associated costs, lost business (defined by IBM as abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished good will) is by far the costliest factor in a data breach event. In addition to the legal costs and response phase, the trust component with vendors and customers is destabilized when a breach occurs. Implementing proper data policy and security is a terrific way to mitigate these events.



Source: "2015 Cost of Data Breach: Global Analysis" *http://www-03.ibm.com/security/data-breach/*

The IBM report also shows that recent breaches are not always the fault of the dreaded cyber hacker. Of the 350 events studied, more than half were due to human error or system failure. Criminal hacking isn't the only way PCI and PII can escape a network, but it is the most costly with an associated cost of $170/record compared with $142 for human error and $134 per system glitch.



Source: "2015 Cost of Data Breach: Global Analysis" *http://www-03.ibm.com/security/data-breach/*

Identifying PCI and PII & Establishing Policy

If your organization deals with any sensitive datasets (personal information, health data, credit card account numbers, etc.), you will need to establish an internal policy on handling that data. Consider the following questions and steps to begin the data collection policy process:

Identify your data sets. What PCI or PII does your organization deal with? Sherpa's director of product services, Marta Farensbach, *provides tips on scanning your system and using regular search expressions to locate PII in your data.*

Do you need to store it? In the data collection age, organizations may accrue high-liability *dark data*, information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes. This is a huge problem as the data may contain secure information, but has no value. Maintaining this information increases risk with little to no benefit. Store only what is essential.

What industry, state & federal laws (HIPAA, FRCP, FOIA, SOX, Gramm-Leach-Bliley Act) do you need to follow? Some industries are more regulated than others. Understanding which laws apply to your organization will help you understand what security measures are expected and which compliance laws apply to your data sets.

Ensure network and database security. Assess your network to have a complete system diagram and identify points of weakness. Use automated software to scan your file shares and email systems for visible or actionable PCI or PII. Encrypt, eliminate or redact files containing PCI or PII so that they are not stored in plain text or accidentally transmitted outside your organization. As part of this process, don't forget to secure paper records containing sensitive data, as well.

Implement an internal policy that will dictate the retention, backup and deletion of your data records. Policies should be agreed upon and followed across the organization. For preventative compliance maintenance, implementing software like *Altitude IG* will assist in establishing and enforcing these policy choices across your records. Read more about *establishing or automating policy.*

Educate and Respond. Ensuring that your employees are educated on policy and procedure for data protection is essential in preventing human error. Creating an Incident Response Team for general computer security will enable your organization to react to threats and breaches in a timely manner as well as help monitor suspected incursions.

Audit your policy. Periodically and consistently test your systems to ensure that no PCI or PII is insecure. Repair any weakness or vulnerabilities that are revealed. It may help to engage an outside firm to conduct the audits, ensure impartiality and strengthen defensibility.

In the event of a breach: Contain the problematic system so no further damage can occur. Follow state and federal laws by reporting to the proper agencies. Conduct investigations to assess the tactics of the breach and the impact, then implement secure fixes to prevent repeat breaches and remediate the issue. It is essential that affected customers or individuals are notified as soon as possible.

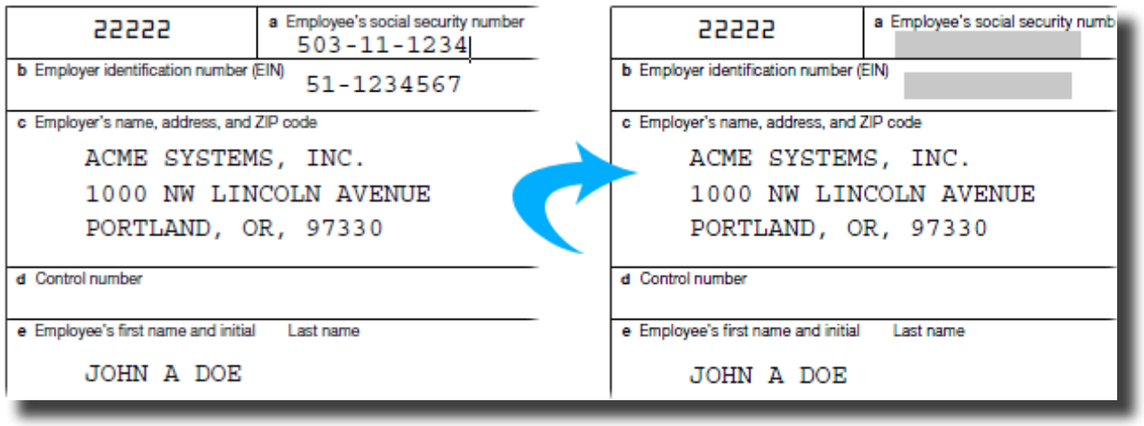
Address distribution of data. In the event that you face litigation or other types of required data sharing, reactive measures will be necessary to protect sensitive information.

Organizations are vulnerable to revealing PCI or PII during eDiscovery or other productions of data (investigations, regulatory requests, FOIA, etc.). Extra vigilance is required to identify and redact data when sharing documents to prevent the inadvertent distribution of medical records, social security numbers, etc., which could expose your organization to further legal liability.

Redaction

Commonly used to mask sensitive data, redaction is a critical step that is deployed before distributing documents containing PCI or PII to outside parties. According to *TechTarget*, "To redact is to edit, or prepare for publishing. Frequently, a redacted document, such as a memo or e-mail message, has simply had personal (or possibly actionable) information deleted or blacked out; as a consequence, redacted is often used to describe documents from which sensitive information has been expunged."

Documents, emails, and data such as tax returns, credit card statements, etc. are especially vulnerable to hackers. Illustrated below is the difference between a W2 form in its original state versus the redacted version. By using specialized software, organizations are able to run specific searches for keywords, social security numbers, and more to identify items which need to be redacted. Redacted images replace the originals for distribution to prevent the data loss.



During the redaction process, the specified keywords/phrases were replaced with the redaction value. This simulates someone using a black or gray marker to obscure text on a printed page.

Keep in mind that the *Federal Rules of Civil Procedure (FRCP)* also list metadata (the unseen information about a document, including document creator, text revisions, notes and comments, bookmarks and access date and time stamps) as discoverable. Counsel will agree to its relevance at the "meet and confer" conferences prior to trial, but must also ensure that this hidden data is guarded against inadvertent production of sensitive information.

Workshare released a *report* that succinctly lists the metadata obligations related to specific FRCP guidelines:

Table 2. Key Ammendments Affecting Metadata

Rule	Key Point	Impact Summary	Implications for Your Organization
34(A)	Creates new category of Electronically Stored Information (ESI)	Removes any doubt whether electronic data (including metadata) are potentially discoverable	• Must be able to preserve and produce ESI • Can no longer argue that electronic documents are not discoverable "documents" under the FRCP • Electronic data must be part of litigation holds and other litigation procedures
34(B)	Gives requesting party the right to specify format in which ESI is produced	Encourages requiring production in native file format (i.e. Word, email, Excel)	• Native file format will include metadata • Forces a move away from scanning and printing electronic documents only • Requires development of systems and policies for preserving, producing and handling ESI in native file formats
26(b)(2)	Introduces categories of "accessible" and "inaccessible" ESI	Implies that metadata will NOT be considered "inaccessible"	• Eliminates argument that hidden data is not "accessible" • Strongly encourages development of policies, procedures and systems for preserving and handling metadata in ESI • Production of ESI will involve consideration of metadata in every case
37(f)	Creates a "safe harbor" protection from sanctions for deletion of ESI in course of routine, good faith operations of computer systems	Reduces the chances of severe penalties in many cases and recognizes the practical difficulty of controlling everything today's computers do while operating	• Places a premium on creating policies and procedures that can be automated to create routine metadata operations • Requires all business decision-makers to participate in development of policies and procedures • Offers a "safe harbor" for rules-based, automated deletion and management of metadata in electronic documents
16(b) and 26(f)	"Meet and confer" rules require early discussion of ESI issues	Forces discussion of ESI early in discovery process and requires understanding of ESI issues for both you and your opponent	• Requires legal team to understand fully how ESI, including metadata, is handled in your organization • Requires that reasonable and defensible plans and procedures be in place for dealing with ESI that a judge will be likely to approve • Requires preparation for dealing with metadata in every case

Source: FRCP & Metdata, Dennis Kennedy, Workshare *https://d3liiczouvobl1.cloudfront.net/uploads/file/667/original/1449665804.pdf*

Conclusion

Organizations must take ownership of PCI and PII challenges. Costs of breaches are incredibly high and storage costs are at all-time lows, ensuring that many organizations are sitting on mountains of data that increase risk and liability.

Experts recommend using an IT-centric approach to identify potential privacy issues that will:

- Reduce the collection and processing of private information that is not relevant to business needs
- Better identify the sensitive information already existing in datasets and apply policy to secure it.
- Conduct frequent audits to ensure policy is effective in safeguarding PCI or PII data
- Review data transmitted outside the organization (including eDiscovery productions) to ensure any PCI or PII data is protected.

We recommend minimizing the use, collection and retention of PCI and PII where applicable. Narrow the use sensitive information to only what is absolutely necessary to conduct business. Finally, implement a handling process for electronically stored information company-wide that provides responsive, adaptable policy for this quickly-changing data landscape.

Resources / Orgs:

A. https://www.pcisecuritystandards.org/index.php
B. http://www.shrm.org/templatestools/samples/policies/pages/personalidentityinformation(pii).aspx
C. https://support.office.com/en-us/article/Use-Office-365-to-help-comply-with-legal-regulatory-and-organizational-compliance-requirements-ce773cec-2151-4d06-9a4e-2818613bd7e0
D. http://apps.americanbar.org/litigation/committees/businesstorts/articles/fall2014-1214-between-a-rock-and-a-hard-place-intersection-of-data-privacy-and-e-discovery.html
E. http://www.sherpasoftware.com/blog/introduction-to-the-payment-card-industry-data-security-standard/

Sherpa Software, a leading provider of technology-driven information governance solutions, has helped more than 4,000 companies worldwide. Sherpa's award-winning software, services and support address information management, regulatory compliance, electronic discovery, policy enforcement, PST management and more. Sherpa Altitude IG, Sherpa Software's signature information governance platform, connects to more data sources than traditional platforms, leaves your data in-place and offers robust analytics and metrics, while addressing core business issues.

www.SherpaSoftware.com | information@sherpasoftware.com | 1.800.255.5155