

Protecting personally identifiable information: What data is at risk and what you can do about it

Virtually every organization acquires, uses and stores personally identifiable information about its customers, employees, patients, students and other individuals. These organizations are expected to manage this private data appropriately and take every precaution to protect it from loss, unauthorized access or theft. Misusing, losing or otherwise compromising this data can carry a steep financial cost, damage a business's reputation, and even lead to criminal prosecution, because of complex and frequently changing regulations. This white paper examines the challenges organizations face and the steps they can take to protect themselves and their customers against data breaches and ensure the safety of this sensitive information.

By John Stringer, Product Manager, Sophos

Protecting personally identifiable information: What data is at risk and what you can do about it

Not so long ago, the most common way people protected their personally identifiable information (PII) was to pay for an unlisted telephone number. Today, there are many types of PII that we need to protect, with credit card information one of the most common (see Table 1). Customer records are processed and stored electronically in databases. And it's not just businesses that use and must protect PII. Universities, healthcare facilities, retailers, government offices and many other organizations also acquire, process and store highly sensitive records. This use of technology has resulted in much greater flexibility and speed when it comes to making purchases, processing payments and managing data records. However, it also has led to a growing data leakage prevention (DLP) problem that puts people's PII at risk.

In 2008, 285 million data records were breached, according to the 2009 Data Breach Investigations Report. There are two types of data loss: accidental and malicious. Human error or carelessness as well as a lack of data security in an organization can lead to accidental loss, including something as simple as sending an e-mail attachment containing PII to the wrong recipient.

Malicious data breaches, on the other hand, are deliberate internal or external attacks on an organization's data systems. Regardless of how the data is lost, the cost of a data breach can be huge. The average cost to companies per lost or stolen record is \$204, according to the Ponemon Institute (Fifth Annual U.S. Cost of a Data Breach Study, January 2010). The average organizational cost of a data breach reached more than \$6.6 million in 2008, up 46% since 2005, according to Ponemon. These costs include fixing the cause of the breach, replacing lost or stolen laptops and storage devices, legal defense costs, disclosure costs for informing consumers about the breach via letters and press releases, loss of business, and expensive fines (e.g., up to \$1.5 million per year in the case of a breach of healthcare records in violation of the Health Insurance Portability and Accountability Act [HIPAA] regulation).

Table 1: Examples of PII

Unique identifiers	When combined with other data
<ul style="list-style-type: none"> » Full name (if not common) » National identification number » IP address (in some cases) » Vehicle registration plate number » Driver's license number » Face, fingerprints or handwriting » Credit card numbers » Digital identity 	<ul style="list-style-type: none"> » First or last name (if common) » Country, state or city of residence » Age, especially if non-specific range » Gender or race » Name of school attended or workplace » Grades, salary or job position » Criminal record

What is PII?

PII, according to the U.S. Office of Management and Budget, is any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person.

It consists of a broad range of information that can identify individuals, including Social Security numbers, driver's license numbers, credit card numbers, bank account numbers, health and insurance records, and much more. Unless your company only accepts cash payments and keeps no payroll-related data about its employees, it has PII it needs to protect.

Most consumers are careful about disclosing their personal information. But once the information is given to an outside organization, it becomes incumbent on the holder of that PII to be vigilant about its use and access.

According to the U.S. General Accounting Office, 87% of the U.S. population can be uniquely identified using only gender, date of birth and ZIP code. So it's not just the most obvious types of PII—Social Security numbers or credit/debit card information—that require protection.

Consequences of not protecting PII

The cost of losing PII to carelessness or theft goes beyond dollars or euros. For organizations that misuse or allow PII data to leak out of their systems, the negative publicity, loss of customer trust, lost business, and legal costs can be severe:

- » Retailer TJX lost an estimated 94 million customer records in a breach that continued for more than a year. The company set aside \$170 million to cover costs, including multiple lawsuits.
- » In 2009, Heartland Payment Systems suffered the largest data breach to date, which compromised about 130 million credit and debit cards. Heartland has committed up to \$8 million to settle lawsuits.

- » The U.S. Veterans Administration lost more than 26 million records when an employee's unencrypted laptop—carrying PII—was stolen.
- » A major UK cellular provider lost tens of thousands of customer records when a rogue employee stole and sold them to a competitor.
- » Health Net of the Northeast Inc. lost a hard drive containing 7 years' worth of unencrypted personal, financial and medical information on about 1.5 million members and network physicians. It agreed to pay for two years of credit-monitoring services for those affected.

The media rarely miss an opportunity to report on such incidents—the dreaded “CNN moment” for affected organizations. Employee morale also takes a hit from the work involved in fixing and recovering from a serious data breach incident.

Questions for developing PII acceptable use policies (AUPs)

- » Who need access to PII to do their jobs?
- » What regulatory mandates must your company comply with?
- » What are your current vulnerabilities?
- » What data can be transferred within the organization? Sent outside to third-parties?
- » What rules and permissions for data transfer does your organization have or need?
- » Is encryption required before data can be transmitted or stored on portable devices?
- » Who is authorized to change or update the AUP?

The three states of data

Data in use is data on endpoints being used by employees to do their jobs.

Data at rest is information stored on endpoints.

Data in motion is data sent over networks.

Table 2: Five rating criteria to determine what data needs to be protected most

Distinguishability	Look for data that by itself can identify a unique individual.
Aggregation	Look for two or more pieces of data that when combined can identify a unique individual.
How PII is used	<ul style="list-style-type: none"> » Frequently transmitted over networks » Stored redundantly on servers or portable devices » Used by many people in the organization
Compliance	<p>Your organization must comply with one or more regulations and standards for protecting PII, such as:</p> <ul style="list-style-type: none"> » U.S. state data breach notification and data protection regulations » PCI DSS for credit card processors » HIPAA for healthcare organizations » FERPA for colleges and universities » Canadian personal information protection regulations (PIPEDA) » European Union Data Protection Directive
Ease of use	<p>Decide if the PII:</p> <ul style="list-style-type: none"> » Is easily accessed by any employee » Can be copied, sent and saved without restriction » Is available for use by HR for employee management or by customer service when assisting a customer » Is not protected by PINs or passwords before being accessible by staff

Creating acceptable use policies

IT managers must balance the desire to tightly control and protect PII with the needs of employees to use the data to perform their jobs. Think of it in terms of CIA: confidentiality, integrity and availability of PII. The goal is to create and enforce AUPs that clearly define which data is most sensitive and which employees are allowed to access and use it in their work. Form a team to help identify and prioritize all the PII your business possesses.

The team typically would include IT operations, the security team and data controllers—who know what data is available and where it's located—and representatives of the HR and legal departments, who have expertise in compliance regulation and legal obligations. This team can help you define your organization's acceptable use policies for handling and storing PII.

5 steps to acceptable use policy

There are five key steps every organization must take to begin the process of preventing data loss:

- » Identify PII your organization must protect.
- » Prioritize PII.
- » Find where PII is located.
- » Create an AUP.
- » Educate your employees about your AUP.

How do you find the PII in your organization? It may be in multiple places, redundant on servers, laptops, PCs and removable media. Thinking about the data in each of its three states (see page 2) will help you identify where it's located.

Once you've found the PII, you need to define what your organization's AUPs are for accessing and using it. AUPs will vary from company to company, but in any organization, they should accomplish three goals:

- 1) Protect PII data.
- 2) Define who can access PII.
- 3) Establish rules for how authorized employees can use PII.

The AUPs you develop will only be effective if your employees feel they have a part to play in protecting your PII. Comprehensively educating employees is a critical and often overlooked step. Deliver copies of AUPs to employees, offer training sessions and have them sign a statement acknowledging they will abide by the policies. This will make every employee an active participant in the enforcement of AUPs, and the organization-wide effort to prevent data leakage and the loss of PII.

Choosing the right solution to protect PII

After you've identified your organization's PII and adopted AUPs for its safe use, it's time to look at how to secure your network, endpoints, other devices and applications. Strong, system-level security can prevent accidental data loss and stop malicious threats before they harm your business, while ensuring the right employees have access to the data they need to do their jobs, within established AUPs. There is no silver bullet to accomplish these goals (see Table 3). Rather, it requires a combination of technologies for defense-in-depth or a multilayer security strategy.

Encryption

Encryption is an integral technology to protect your organization's sensitive data. If a threat gets by your anti-virus, firewall and other controls, PII is vulnerable. But if data that is encrypted before it's placed on removable media or sent by email falls into the wrong hands, it is unreadable. You can provide the password or exchange keys to the encrypted data on a case-by-case basis among groups or individuals who require access to perform their jobs. Adding SPX encryption converts an email into a PDF for safe sending.

Another key benefit of encryption is it enables organizations to comply with regulatory mandates for protecting PII. If an organization that encrypts all of its portable devices, email, and media used by employees experiences the loss or theft of those devices or communications, the organization could avoid having to disclose the data breach, thus avoiding the business-damaging notoriety of a CNN moment. Properly deployed encryption provides a "safe harbor" from data breach disclosure regulations.

Table 3: Essential technologies to protect PII

Encryption	<ul style="list-style-type: none"> » Full disk encryption » USB, CD and removable media encryption » Policy-based email encryption » File share encryption » Central key management and backup » Ability to audit encryption status
Threat protection	<ul style="list-style-type: none"> » Protect endpoint, email and web vectors with proven security. » Detect known and unknown malware proactively without the need for an update, including viruses, worms, Trojans, spyware, adware, suspicious files, suspicious behavior, potentially unwanted applications (PUAs) and more. » Get anti-virus, firewall, application and device control in a single agent. » Defend all of your platforms (Windows, Mac, Linux, UNIX).
Data loss prevention	<ul style="list-style-type: none"> » Stop accidental data loss by scanning content for sensitive information sent by email or IM, and saved on storage devices with automatic rules, such as: <ul style="list-style-type: none"> • File matching rule: Specified action is taken based on name or type of file a user is attempting to access or transfer • Content rule: Contains one or more data definitions and specifies the action taken if a user attempts to transfer data that matches those definitions
Policy compliance	<ul style="list-style-type: none"> » Develop a list of applications that need to be controlled under all or certain circumstances to prevent the accidental transmission of sensitive data, by email, IM, P2P, online storage, smartphone synchronization and other frequently used communications apps. » Introduce and enforce methods of web control, as the internet is the source of most malware. » Enable control of three types of devices that are commonly used in the accidental storage or sending of sensitive data: <ul style="list-style-type: none"> • Storage: Removable storage devices (USB flash drives, PC card readers, and external hard drives); optical media drives (CD-ROM/DVD/Blu-ray); floppy disk drives • Network: Modems, wireless (Wi-Fi interfaces, 802.11 standard) • Short range: Bluetooth interfaces, infrared (IrDA infrared interfaces)

Threat protection

Effective protection from malware and other threats is crucial to keep your network up and stop the ubiquitous viruses that can infect an organization's computers and steal data. This requires more than anti-virus software alone. A solid defense reduces your threat exposure by protecting all vectors using preventive techniques. A comprehensive anti-malware solution delivers a quick, thorough scan to detect malware, adware, suspicious files, unusual user behaviors, phishing attacks, and unauthorized software deployment. The solution you choose should:

- » Update frequently with the latest signatures to automatically guard against new and targeted threats.
- » Stop zero-day threats with a built-in host intrusion prevention system (HIPS) and web-based script attack detection.
- » Automatically assess managed and guest computers for out-of-date security and patch status before they join your network.
- » Deliver instant visibility of security status for all Windows computers from the same console used to manage Mac, Linux and UNIX machines, which would enable a fast, accurate assessment of the banker's PC in Table 4.

Data loss prevention

It's imperative that you scan the files and content leaving your organization to identify any that contain PII. As in the example in Table 4 below, the objective is to warn users before they send sensitive data to ensure they are aware of the organization's AUP, or prevent the data from being emailed, transferred to a memory stick or otherwise put in motion. Deploying a standalone DLP solution to protect against the accidental loss of sensitive data can be time consuming and costly, and adding another scanning agent can slow down your endpoints and the people who use them.

A top-notch content control solution identifies sensitive data such as PII, financial information and any other records you have flagged as private. Once the scan is complete, you have several options:

- » Allow the file transfer to proceed, and log the event.
- » Warn users that they are about to send data with PII and what the consequences are, remind them about the organization's AUP, and log the event.
- » Block the transfer of the data because it violates the AUP, and log the event.

Table 4: Protecting PII

A loan officer at a mid-size bank needs to e-mail important papers to a loan applicant. The bank's network security solution must provide:

- » **Encryption** that will keep the data safe if the loan officer's laptop is lost or stolen.
- » **Threat protection** to keep his PC safe from viruses, phishing and other threats.
- » **Data loss prevention** that will warn him he is about to send a file with Social Security numbers and other PII.
- » **Policy compliance** that will block him from using a browser with a known security vulnerability or stop him from saving the file to an unencrypted USB stick.
- » **Blocking of anonymous proxies** for Web searches, because they allow personal information to be accessed by administrators of the proxy server.

An integrated security solution enables you to monitor and control the transfer of files to specified storage devices or by specified internet-enabled applications (e.g., email client, web browser or instant messaging) without having to deploy a separate solution for each application, which minimizes administrative costs and improves performance. Email encryption and DLP content control are vital components of any data protection solution, but to be effective, the solution must be simple and non-disruptive to users. In the case of email, for instance, content monitoring and control is needed on both the endpoint and the mail gateway to ensure PII is protected. A content control list feature used by the banker company in Table 4 would scan for sensitive data in email messages and attachments, and then warn the banker before he hits the send button, blocking him from sending the information, and/or logging the event, depending on the bank's preferences.

Policy compliance

Policy compliance comprises three key elements—application control, device control and web control—that need to work together to ensure users comply with applicable policies.

Application control: Another potential source of DLP is employees accidentally—or intentionally—sending information using unauthorized applications such as IM, P2P file sharing, online storage, or smartphone synchronization. These applications use significant amounts of network bandwidth and are increasingly the cause of security, legal and productivity issues in business. Consequently, IT departments are charged with controlling the unauthorized installation and usage of these apps. A layered security solution integrates the detection of such controlled applications alongside malware and potentially unwanted application detection—as in Table 4, where the banker was prevented from using a web browser with a known vulnerability—enabling control without the requirement of purchasing,

installing and managing a separate point product.

You can support your AUPs by leveraging granular application control technology to prevent use of these applications if it's determined they create a vulnerability for data leakage. You also can configure policies for groups of endpoint computers to reflect the security requirements for specific locations or departments. For example, VoIP can be switched off for office-based desktop computers, yet authorized for remote computers. Administrators can easily manage application control by employing whitelists (permitted applications) and blacklists (prohibited applications). These further take the guesswork—and risk—out of managing these potential sources of lost or stolen PII, without impeding the normal course of business.

Device control: In conjunction with application control, device control can significantly reduce your company's exposure to accidental data loss and restrict the ability of users to introduce software and malware from outside your network environment. You can establish policies that control the use of network devices and removable storage media, down to specific models and by work group or individual, which will block the ability to place PII on USB memory sticks, or burn it to CDs, or provide read-only access. In Table 4, the banker was blocked from placing data containing PII on an unencrypted memory stick.

Having the ability to exert appropriate control over both device instance and model exceptions means the use of a USB key belonging to the marketing department, for example, can be prohibited by the removable storage block policy, but an encrypted USB stick used by the legal department to store PII would be permitted.

Web control: Another important aspect of an overall policy compliance program is to introduce and enforce methods for controlling the web, which is the primary source of malware, infecting users who visit compromised sites. Web control can prevent infection by blocking access to known malicious and infected sites. Controlling access to the internet and Web 2.0 applications is critically important for an effective data-protection strategy:

- » Webmail, blogs, forums, and social networking sites present a significant risk for accidental data loss or leakage.
- » An effective policy compliance solution must address the risks associated with data leakage through Web 2.0 by:
 - Controlling access to malicious and high-risk sites
 - Controlling data that leaves the organization through web applications
 - Blocking the use of insecure, anonymous proxy servers, which can capture and compromise sensitive information.

Recommendations

- » Choose a layered security approach that delivers all the following capabilities:
 - Encryption
 - Threat protection
 - Data loss prevention
 - Policy compliance
- » Prioritize the solutions based on your risk profile (determined after a risk assessment). Prioritizing the security deployment ensures that budgets and resources are not strained. An integrated solution offers many advantages:
 - Simple to install and easy to manage
 - One place to call for support
 - Best, most comprehensive protection
 - Saves time and money

Sophos solution

To learn more about how Sophos can help you protect your data in one simple-to-manage solution, please visit: <http://www.sophos.com>.

Boston, USA | Oxford, UK

© Copyright 2010. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM