SOPHOS

simple + secure

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 (PII). Most have it for their employees and, depending on their area of business, may also have it for a wider group including customers, patients, residents and students.

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 and damage an organization's reputation. This white paper examines the challenges companies face and the steps they can take to protect themselves against data breaches and ensure the safety of this sensitive information.

by John Stringer, Product Manager, Sophos

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—and it's not just businesses that use and must protect PII. Schools, universities, healthcare facilities, retailers, government offices and many other organizations also acquire, process and store highly sensitive records.

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 has also led to a growing data loss prevention (DLP) problem that puts people's PII at risk.

There are two types of data loss: accidental and malicious. Human error or carelessness as well as a lack of data security processes in an organization can lead to accidental loss, including something as simple as sending an email 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.

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 dates of birth, addresses, driver's license numbers, credit card numbers, bank account numbers, health and insurance records, and much more. Unless your organization keeps no payroll-related data about its employees, it has PII it needs to protect.

While most adults are careful about disclosing their personal information, this issue is particularly sensitive for organizations that have information on minors, such as schools, councils and medical services. 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, like credit card numbers, that require protection.

"87% of the U.S. population can be uniquely identified using only gender, date of birth and ZIP code."

Table 1: Examples of PII

- First or last name (if common)
- Date of birth
- Country, state or city of residence
- Credit card numbers
- Immunization history/medical records
- Age
- Telephone numbers
- Email addresses
- Gender
- Race
- Criminal record

Consequences of not protecting PII

Regardless of how the data is lost, the cost of a data breach can be huge. Fines are one of the most widely-known consequences of losing personal data, and they can be very expensive (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 or up to £500,000 from the UK Information Commissioner).

However, the consequences extend much further and include reputation damage, loss of customer trust, employee dissatisfaction and attrition, and clean-up costs following the breach. Examples include:

- Hartland Payment Systems committed $8 million to settle lawsuits following a data breach which compromised 130 million credit and debit cards
- Health Net of the Northeast Inc. agreed to pay for two years of credit-monitoring for 1.5 million members whose details were on a lost hard drive
- Sony provided free services to customers affected by their 2011 data breaches to help them protect against identify theft

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, file servers and information repositories like Exchange servers, Sharepoint and web servers.
Data in motion is data sent over networks.

Organizations must ensure they they consider data in all three states when protecting their PII.

Questions for developing PII acceptable use policies (AUPs)

- Who needs access to PII to do their jobs?
- What regulatory mandates must your organization comply with?
- What are your data security 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?

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 organization 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.

"Regardless of how the data is lost, the cost of a data breach can be huge."

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 Table 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 organization to organization, but should accomplish three goals:

- Protect PII data
- Define who can access PII
- 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 loss and the loss of PII.

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 stored, transmitted, used	• Frequently transmitted over networks • Stored redundantly on servers or portable devices • Used by many people in the organization
Compliance	Your organization must comply with regulations and standards for protecting PII. Which ones will depend where you are based and scope of work. However these may include: • **Payment Card Industry Data Security Standards** (PCI DSS) (International) – setting out requirements for data security when handling card payments • **Data Directive** (EU) – requiring the safe storage using data loss prevention technology of data generated in connection with public electronic communication • **HIPAA and HITECH ACT** (U.S.) – enabling fines of up to $1.5 million per year for a breach of healthcare records • **Criminal Justice and Immigration Act** (UK) – giving the Information Commissioner power to levy fines of up to £500,000 for data breaches There are also a large number of data security regulations applicable at regional or state level. If you work in a geography covered by such legislation you should understand the implications for your organization.
Ease of access	Decide if the PII: • 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 staff • Is not protected by PINs or passwords before being accessible by staff

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 organization, 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.

Table 4: Protecting PII

Example scenario: A HR manager needs to provide important papers to a pension company. The company's network security solution must provide:

- **Encryption** that will keep the data safe if the manager'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 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

Table 3: PII solutions

Encryption	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	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 antivirus, firewall, application and device control in a single agent • Defend all of your platforms (Windows, Mac, Linux, UNIX)
Data loss prevention	Stop accidental data loss by scanning content for sensitive information uploaded to websites, sent by email or IM, and saved on storage devices with automatic rules, such as: • 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	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: • 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)

Recommendations

Protecting PII requires organizations to work through a number of steps. Exactly what you do under each step will vary depending on your industry, the type of data you hold, the geographies you work in, your attitude to risk, your resources, and other factors.

However all organizations should follow the same broad steps:

- Identify what PII you hold
- Create policies around handling the data
- Educate your users (for resources to help educate users about data security download the free Sophos Data Security Toolkit)
- Implement a layered technology approach that puts in place practical data security controls, including:
  - Encryption
  - Threat protection
  - Data loss prevention
  - Policy compliance (devices, applications and web access)

To learn more about Sophos and to evaluate any of our products free for 30 days, please visit us at www.sophos.com

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Boston, USA | Oxford, UK

SOPHOS