MOORE

AUGUST 2024

MOORE NEWSLETTER

The Importance of Data Privacy: Safeguarding Sensitive Information in the Digital Age

The digital age has ushered in an era of unprecedented data collection, storage, and processing, transforming how businesses operate and interact with customers. While this data revolution has brought immense benefits, it has also raised critical concerns about data privacy and cybersecurity. For instance, the recent partnership between Kroger, a major US grocery chain, and Microsoft to implement "smart shelves" in their stores. This initiative, which involves integrating digital technology into shelves to track inventory and analyse customer behaviour, has raised concerns about the potential for "exploiting sensitive consumer data" through facial recognition tools. This recent controversy serves as a stark reminder of the potential risks associated with unchecked data collection and the importance of safeguarding sensitive information. As businesses navigate this complex landscape, it becomes increasingly imperative to prioritise data privacy and cybersecurity, ensuring that organisations are maintaining robust data privacy practices to protect the confidentiality, integrity, and availability of Personally Identifiable Information (PII) and other sensitive personal data.

Sensitive PII and non-sensitive PII

PII refers to information associated with a specific individual and can be utilised to determine their identity. Disclosing personal data can offer advantages, as it enables organisations to customise offerings to the desires and needs of customers. Yet, the burgeoning stockpiles of PII collected by organisations concurrently draw the attention of cybercriminals and potential insiders to commit identity theft.

There are two types of PII: Sensitive PII and Non-sensitive PII. Sensitive PII is sensitive information that directly identifies an individual and could cause significant harm if leaked or stolen. Examples of sensitive PII include:

- Social security number (SSN)
- Biometric data (E.g. Fingerprints)
- Financial information (E.g. Bank account numbers and credit card numbers)

Non-sensitive PII is personal data that in isolation would not cause significant harm to a person if leaked or stolen. Examples of non-sensitive PII include:

- Full name of a person
- Email address
- Place of birth
- Telephone number

Common attacks on PII

Cybersecurity threat	Definition	Example
Data breach	Security incidents in which unauthorised parties obtain access to secure, protected data.	Cybercriminals infiltrate a firm's database or system and steal PII such as credit card numbers, medical records, and passport numbers.
Phishing attack	Involves the use of deceptive electronic communications, text messages, fraudulent emails or fake websites to manipulate individuals into revealing sensitive information.	Attackers send fraudulent emails disguised as communications from trusted organisations and request the recipients to click on malicious links, tricking them into providing personal information like login credentials or bank account details.
Malware	Malicious software that infects devices and networks, enabling attackers to steal or compromise sensitive PII stored on the systems.	Cybercriminals can infect devices with malware to collect a trove of an individual's personal information, including social security numbers, home addresses, and financial data. This enables them to commit identity theft and financial fraud.
Insider threat	Cybersecurity threats originate with authorised users, like employees and business partners, who intentionally or accidentally misuse their legitimate access.	A fierce employee who works in accounting at a bank stole customer information after getting a bad performance review. She used her access to copy private information including names, addresses and bank details to a hidden USB drive. Then, she used the stolen data to open fake accounts in customers' names, maxing them out and causing big financial losses.

Data privacy best practices for individuals

1. Adopt strong passwords

Create complex and unique passwords for your online accounts and avoid using the same password for different accounts. Utilise a combination of uppercase and lowercase letters, and special characters to make your password more difficult to crack.

2. Use VPN

Using a VPN allows your device to connect to the internet through a secure, third-party server rather than directly. This provides a significant boost to your online privacy and security in several ways such as encryption of all data transmitted between your device and VPN server.

3. Optimise privacy settings in your online accounts

Enable privacy features such as two-factor authentication and private browsing modes. These add an extra layer of security and minimise the digital footprint when accessing sensitive information.

4. Keep software and devices up to date

Ensure that systems and applications like operating systems, web browsers and anti-virus are at the most up-to-date version. Software updates often include security patches that address newly discovered vulnerabilities.

Data security controls to safeguard PII

Protecting PII is a crucial element of data security and privacy. Organisations that handle PII data must implement a comprehensive set of security controls to safeguard sensitive information. The following security controls serve as essential safeguards to protect PII data from unauthorised access, disclosure, modification, or destruction, thereby preserving its confidentiality, integrity, and availability.

1. **Encryption**

Encryption is a powerful tool for safeguarding sensitive information and protecting data confidentiality. By transforming intelligible data into an unreadable format, encryption ensures that even if unauthorised parties gain access to the information, they will be unable to make sense of it.

For example, when transmitting data over a network or transferring files, encryption plays a crucial role in preventing eavesdropping and unauthorised access. By encrypting the information during transit, the original data is obscured and rendered incomprehensible to anyone without the proper decryption keys. This protects the confidentiality of PII and other sensitive data.

2. **Identity and access management (IAM)**

IAM systems are responsible for defining, implementing, and enforcing access policies that determine who can access specific data or resources. By implementing the principle of least privilege and role-based access controls, IAM helps ensure that users can only access the minimum amount of data necessary to perform their duties, limiting the potential exposure of sensitive information.

3. **Security awareness training**

Training should be conducted to help employees understand the importance of data privacy and the consequences of data breaches. Also, it is crucial for employees to understand their individual roles in protecting sensitive data. This includes following established data handling procedures, reporting suspicious activity and maintaining best practices for password management.

4. **Cybersecurity tools**

Data leak prevention solutions facilitate three key objectives, including data at rest (capable of identifying and logging where specific types of information are stored across the company), data in motion (capturing and analysing network traffic) and data in use (monitoring data movement stemming from actions taken by end users on workstations).

5. **Incident Response**

An incident response plan should be in place while encountering data leakage and data breach. The organisation should establish clear criteria for identifying PII breaches, designate an incident response team to assess the scope and severity, and gather all relevant information about the incident, including the type of PII, number of individuals affected, and potential impact.

Summary

In conclusion, maintaining robust data privacy practices is crucial to protect the confidentiality, integrity, and availability of Personally Identifiable Information (PII) and other sensitive personal data. This includes securing sensitive PII such as social security numbers, biometric data, and financial information, as well as non-sensitive PII including names and contact details.

Common cybersecurity threats including data breaches, phishing attacks, malware, and insider threats pose serious risks to personal data, potentially enabling identity theft, financial fraud, and other harms. Organisations must prioritise data privacy by adopting rigorous security measures, implementing strong access controls, and educating employees on data protection best practices.

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SMEs to listed companies from a wide variety of industry, and public sectors including government bureaus and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

To find out more, please contact one of our experts below:

PATRICK ROZARIO
Managing Director
T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal
T +852 2738 4631
E kevinlau@moore.hk