Adopting Technical Controls for Data Privacy in the Digital Age

These days, people tend to share seemingly related or unrelated personal information online, such as birthdays, addresses, contact details, relationships and holiday plans. People are also inclined to share pictures of their lives and provide opinions on sensitive issues on various social media platforms. On the other hand, new and exciting technologies are emerging on an almost daily basis, which lead to people sharing their information in the form of playing games online, attending virtual meetings and events, and shopping online. Similarly, organizations collect and store relevant personal information for business purposes. Consequently, privacy risk increases ubiquitously with every share, and the shared data, individually or collectively, can be used for malicious activities. Organizations can implement basic technical controls to mitigate this risk and achieve privacy.

What Is Privacy?

Privacy is an individual's fundamental right to have control over the collection, usage and dissemination of individuals' personally identifiable information (PII). PII is the information that directly or indirectly identifies an individual. This can include a person's name, address, date and place of birth, national identity number, and biometrics (e.g., fingerprints, irises).

Data privacy, also known as information privacy, deals with the ability of an organization to handle PII, or an individual's right to determine what kind of data can be collected/stored in a computer system and shared with third parties. Data security is about ensuring that technical controls (related to confidentiality, integrity and availability) are implemented to protect PII from malicious cyberattacks.

Organizations can sometimes be confused by the difference between data privacy and data security. Both of them pertain to PII, but they are distinct concepts. Data privacy is about the control over PII, such as policies and procedures being established to ensure that PII is collected, stored, used and shared appropriately. Data security is about securing and protecting PII. In other words, data security is a more technical aspect of PII, whereas data privacy is a more legal aspect. In layman's terms, privacy is the fundamental right to be left alone without any intervention.

Muhammad Tariq Ahmed Khan, CISA, CRISC, CSIM, CDPSE, CISSP, CEH, CDFE, ISO 22301 BCM LA, ISO 27001:2013 ISMS LA, PMP
Is the head of cybersecurity audit in the internal audit division at Arab National Bank, Riyadh, Saudi Arabia. He is a subject matter expert in technology and cybersecurity audits. He has more than 21 years of experience in the banking industry in areas such as IT, cybersecurity and IT audit. He has a solid understanding and application of risk-based audit methodology, International Organization for Standardization (ISO) ISO 27001, ISO 22301, US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), COBIT®, and IT and information security regulatory compliance. Khan also has technical knowledge in various IT platforms and IT project management, with experience in disaster recovery and business continuity management. He has published articles on different cybersecurity topics and has spoken at seminars and conferences.

Enjoying this article?

- Read *Achieving Data Security and Compliance: How to Safeguard Identity, Protect Information, Reduce Risk and Create Value. www.isaca.org/data-security-and-compliance-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Privacy Risk

One of the biggest challenges faced by any organization is managing privacy risk. Privacy awareness has increased over time and, therefore, people are becoming more concerned with how organizations are handling their personal information.

Moreover, with the inception of privacy regulatory laws such as the Asia Pacific Economic Cooperation (APEC) Privacy Framework, the EU General Data Protection Regulation (GDPR) and the US State of California Consumer Privacy Act (CCPA) and their associated penalties, it has become mandatory for organizations to take necessary steps to establish and implement strong privacy risk management frameworks. Inadequate or a lack of risk management frameworks may present risk to organizations, such as:

- Damage to the organization's public image and reputation
- Financial or operational losses
- Regulatory sanctions and penalties/fines
- Loss of customers' trust and failure to attract customers
- Damaged business relationships

Recommended Privacy Technical Controls

Digital records of PII demand unique forms of protection at each part of their life cycle. It is paramount for an organization to implement an effective privacy program that includes the following privacy technical controls to address privacy risk.

Privacy Framework

Organizations should have a formal corporate governing structure to determine the level of privacy risk appetite acceptable for senior management. Based on the determined risk appetite, a privacy risk management framework can be developed to identify, analyze, evaluate and mitigate privacy risk. The framework should contain policies and procedures relating to the privacy of personal information, including data classification, record management, data retention and data destruction. It should also state the detailed roles, responsibilities and accountability related to the privacy program through its life cycle.

Data Collection

Organizations should document the business purposes for collecting personal information to ensure that PII that is not required is not collected and retained. Organizations must identify what types of PII the organization is required to collect, who will collect it, how it will be collected and who will define what is personal or private.

Permissions

A technical solution to set different permission levels for employees based on what PII they need to access such as public, private and restricted access (depending on the type of organization) should be implemented. Stakeholders must be well aware of where all personal information is stored and who has access to it, and it is essential to maintain audit trails and logs.

Data Confidentiality Assurance

Stakeholders must ensure that PII is encrypted at rest and in motion throughout the data life cycle (i.e., collect, store, secure, use, dispose). For instance, PII should be encrypted at various levels, including when in databases, networks, system platforms, application layers and business process/functional levels. In addition to encryption, the disclosure rules of PII should be identified and shared with relevant third parties and not disclosed to unauthorized entities (i.e., people and systems).

> "DIGITAL RECORDS OF PII DEMAND UNIQUE FORMS OF PROTECTION AT EACH PART OF THEIR LIFE CYCLE."

Education and Awareness

Employees who handle or have access to personal information must complete privacy awareness training to ensure that they are aware of their specific responsibilities depending on their assigned roles in handling privacy requirements, issues and concerns. Organizations must ensure that resources are available to help employees

develop, implement, maintain and execute an effective privacy program.

Privacy Compliance Monitoring Framework
A compliance monitoring framework must be established to periodically verify the compliance level to ensure that privacy policies and procedures are being followed and are detailed enough to meet new or current requirements, such as the CCPA, GDPR, and the US Health Insurance Portability and Accountability Act (HIPAA). Organizations must assess the privacy laws and regulations that are currently applicable for the organization or that will be applicable in the future.

Privacy Incident Response Plan
A privacy incident response plan should be developed in the event of a breach or attempted breach of personal information to report such breaches to authorized individuals or regulators or anyone who has been affected by a data breach. This also includes breaches that occur on the part of third parties.

Data Flow Map
Stakeholders should establish a data flow map that covers what kind of information is subject to transfer from one location to another, such as between departments, between individuals, to and from third parties, and through geographical borders.

Technological Solutions
Any software or system or technology to be used for privacy should be fully evaluated to ensure that the solution is meeting the privacy requirements. Organizations should also consider deploying hyperautomation by using technologies such as robotic process automation (RPA), artificial intelligence (AI), machine learning (ML) and process mining to automatically redact PII from both static files and audio and video recordings.

Key Benefits of Good Technical Controls

There are a number of key benefits of having good technical privacy controls, including:

> "ORGANIZATIONS MUST ENSURE THAT RESOURCES ARE AVAILABLE TO HELP EMPLOYEES DEVELOP, IMPLEMENT, MAINTAIN AND EXECUTE AN EFFECTIVE PRIVACY PROGRAM."

- Protecting the organization's image and reputation
- Protecting the valuable data of the organization and its customers, employees and business partners
- Achieving a competitive advantage in the marketplace
- Complying with applicable privacy laws and regulations and avoiding regulatory penalties
- Enhancing an organization's credibility and promoting confidence
- Promoting good practice and culture within the organization
- Protecting the organization from potential financial and operational losses

Conclusion

Protecting individuals' privacy cannot be separated from technological development, and these days, organizations are inclined to invest in security technology to reduce the risk of exposing individuals' PII. However, there is no technology that will completely prevent and eliminate the risk of a data privacy breach. Therefore, organizations should fully understand the nature of risk and take a layered approach to improve their security postures by taking the time to understand PII and re-evaluate how data privacy can be managed and protected.

Author's Note

This article does not cover data privacy with respect to the collection, usage, storage and dissemination of PII in physical form.