Cost of an individual's data – An overview

The enterprise business data is a heart for any enterprise to run their business. Similarly the PII – the Personally Identifiable information of an individual is very sensitive in nature and it is very expensive if the data is being lost and that is the reason every enterprise classify these data as confidential and invest more to protect the data. If the PII is available to an unauthorized user, it would become dangerous and result in identity theft causing major damages to an individual as well as to an enterprise. This document describes how companies evolved to safeguard their customer data.

Overview of Data Privacy Act

The PII helps to identify an individual and the PII can be Name, Address, telephone #, SSN, Passport number, driving license number, biometric information etc. Today, every countries developing their own data privacy acts to protect their citizen's nonpublic data from an adverse exposure. With increase in threats in different dimensions, many countries constantly amending their data privacy acts. Several countries have started adopting data privacy acts from UK, Australia and Canada and amending further to meet their culture into the privacy laws. Technology advancement helps people to perform everything faster, on the other hand presence of vulnerabilities in the IT systems and the way the data is being processed or stored or transmitted pose big threat to an enterprise as well as to an individual.

The data privacy laws applicable to both private and public organizations. The countries like USA does not have specific data privacy laws; however, their compliance act broadly covers data privacy and they are HIPAA (Health Insurance Portability and Accountability Act), SOX (The Sarbanes–Oxley Act), GLBA (The Gramm-Leach-Bliley Act), FTC (The Federal Trade Practice Act), and COPPA (Children's Online Privacy Protection Act).

The United States has mandatory state laws to report security incidents in stipulated timeframe and however there is a delay in identification and reporting of security incidents. Some enterprise does not want to reveal their security incidents to hide its weakness in their existing systems and to avoid its business repercussions. In the Europe, it is not mandatory for an enterprise to report the data breaches to regulatory authorities. With new Europe Union's General Data Protection Regulations (GDPR), it is mandatory for an enterprise to report the data breaches within 72 hours after detection of a security breach.

Impacts of inadequate data privacy acts

An inadequate customer data protection results loss of market due to customer migration to better service providers, penalties from regulators, customers may sue an enterprise for inadequate protection of their private data.

How can an enterprise can protect customer data?

An enterprise must collect the data with consent from an individual and collect only limited data that is required for the processing, used data for a specific purpose that was collected and destroy it once its objectives are met. An enterprise shall perform the followings to protect the customer data;

- Define data governance policy
- Provide restricted data access on need basis
- Define and implement adequate security controls to protect the data and keep monitoring the effectiveness of controls
- Encrypt the data during transmission using strong encryption algorithm as recommended by the regulation authorities and also based best practices
- Conduct period awareness training that includes social engineering
- Classify the data based on its value
- Destroy the data once the data collection and data processing objectives are satisfied
- Periodic backup of data as recommended
- Perform periodic privacy data impact analysis and implement the recommendations based on findings derived from privacy data impact analysis

How can an individual protect their private data?

The natural person should aware pf phishing attack which may collect their sensitive information in a fake website pages. Cookies play an important role and some cookies collect user information and generate a natural person's profile. The natural person has option to provide his/her consent to store the data in cookies in the form of temporary files. Periodically scan the laptop and update antivirus patch in the personal laptop.

Data privacy laws in various countries

Country Name	Data Privacy Act
USA	HIPAA (Health Insurance Portability and Accountability Act) GLBA (The Gramm-Leach-Bliley Act) FTC (The Federal Trade Practice Act) COPPA (Children's Online Privacy Protection Act)
UK	Data Protection Act 1998 (DPA)
Europe Union	General Data Protection Regulation (GDPR)
Australia	Privacy Act 1988
India	Information Technology Act 2000 (several sections cover different aspects)
Canada	The Personal Information Protection and Electronic Documents Act (PIPEDA)
Hong Kong	Personal Data (Privacy) Ordinance (Cap. 486)
New Zealand	Privacy Act 1993
Japan	The Act on the Protection of Personal Information (APPI) The Act on the Protection of Personal Information Held by Administrative Organs The Act on the Protection of Personal Information Held by Independent Administrative Agencies
Singapore	Personal Data Protection Act (PDPA)
South Africa	The Protection of Personal Information Act (POPIA)
Malaysia	Personal Data Protection Act 2010 (PDPA)
Dubai	The Dubai International Financial Centre (DIFC) - Data Protection Law No.1 of 2007 (Law)

Conclusion

Every enterprise should perform data privacy impact assessment and audit periodically to ensure that they meet the local regulations and compliance. Data value changes as it being used by the primary systems and then subsequently used by secondary systems. Based on the value of the data, appropriate controls must be implement to safeguard data of a natural person. The value of an individual data is very high and that is the reason every enterprise implement appropriate controls to protect their data.

Authored by Ananda Narayanan G
TCS - Enterprise Security and Risk Management