Appendix M

Data Privacy, Data Protection and Cybercrime

Introduction

This appendix is closely related to the central theme of the book. The challenge of protecting valuable/sensitive/confidential information is becoming tough as organizations push the envelop of what technology and globalization enable in terms of business and operational models. The risks associated with the mismanagement of sensitive information are increasing, as regulators and other constituencies around the world seek to place the burden of such losses or breaches on anyone in the supply chain who handles such data, including service providers. Chapters 9 and 11 (Chapter 11 in CD) should be referred to for case illustrations that bring out this point. The issue of "data breach" is closely related to "identity theft" (discussed in Chapter 5). Organizations need data protection measures to prevent data breaches.

The objective of this appendix is to provide a commentary on the three terms mentioned in the title and to put the concepts in perspective in the context of current scenario. We know that cybercrimes are on the rise – refer to the data presented in Chapter 1. The sophistication and publicized number of attacks and breaches of IT systems have increased remarkably and show no signs of abating. Data protection and cybersecurity is top-of-mind these days for everyone. Data protection is indeed the need of the hour. Appendix V describes the Data Privacy Framework that has emerged from India [developed by the Data Security Council of India (DSCI)]. In simple terms, data privacy is a person's right to control personal information about themselves. Toward the end of this appendix we have presented the gist of "The Indian Personal Data Protection Bill" regarding this topic.

"Personal data" is any data element relating to identified or identifiable individuals. "Processing of personal data" includes collection, storage, disclosure, transmission access to and use of personal data. "Privacy" as a general concept is a very broad term. "Privacy" is usually defined as "the claim of individuals to decide for themselves when, how and to what degree information about them is conveyed/communicated to others or used by others." In other words, "privacy" is an individual's freedom to decide how the information about him/her can and should be used. "Privacy" and "Security" are related (see Fig. M.1).

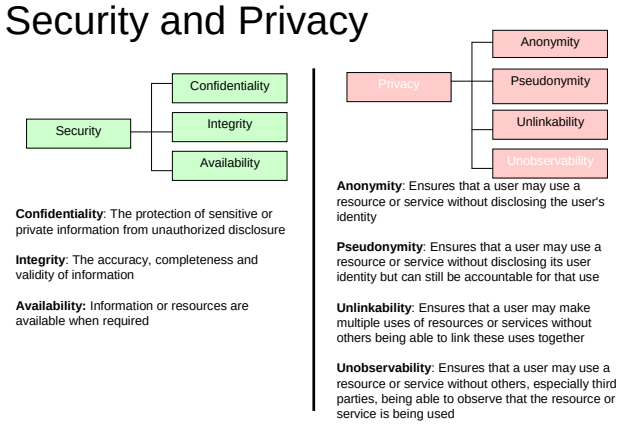

Figure M.1 Privacy and security.

Data is stolen when it is not protected and "data theft" is one type of cybercrime. For example, in insider attacks by copying confidential digital data from their employers and selling it to competitors, some insiders can cost their parent companies millions of dollars (detailed discussion is available in Chapter 9). Credit card frauds are so common and to know more about it visit Section 11.4 in Chapter 11; in particular Illustration 1: Stolen Credit Card Information. A criminal with your 16-digit credit card number, the three-digit CVC (Card Verification Code) number available behind the card and using your name, could buy anything using your money. Data protection is thus essential. Security and privacy both are required for data protection (see Fig. M.2).

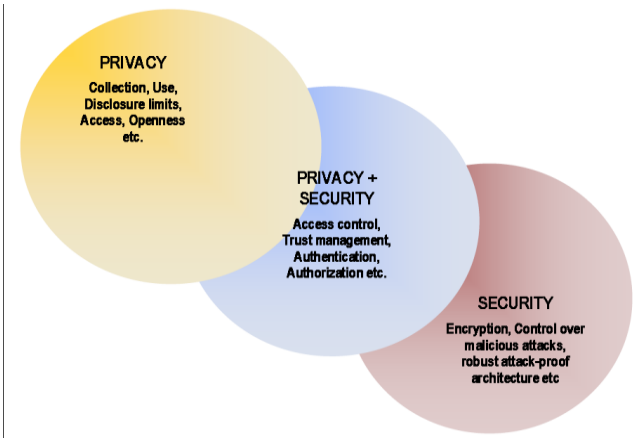

Figure M.2 Security and privacy.

Data protection is about the collection, maintenance, use and dissemination of personal information. Over the years data protection has gained prominence on account of technological advances and its effect on safeguarding personal information. It is significant to note that the use made of personal data, the interests of the individual and the interests of society may conflict and therefore they need to be resolved in the same way as in the context of individual liberty. By way of another definition, "Data Privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them."

Data Protection and Privacy in Global Business Context

For modern businesses that are driven globally, information assets are crucial and most information assets today exist in soft form residing on corporate networks. Information now changes hands like never before and much more easily given that digital information is so easy to copy and transfer! Although cross-border transfer of information takes place for legitimate business purposes, however, there are criminals lurking to illegally access that information or to steal it to satisfy their ulterior motives. Loose security measures lead to weakening of data protection and criminals take advantage of that weak position. Protection of information assets needs to be addressed not only at the technical security level but also at the legal compliance and policy framework level to ensure a well-rounded approach toward information asset security. Recall the discussion in Chapter 6 about the legal framework for cybersecurity arena. Data theft, unauthorized copying, alteration or deletion of data, hacking, identity thefts, Intellectual Property Right (IPR) violation and unauthorized access are just a few issues that are causing serious concern in corporations and need to be handled effectively to ensure a clean, safe and secure work environment. Data protection constitutes two key aspects:

1. Prevention of misuse of personal data through legal safeguards to prevent misuse of information about individual people on a medium including computers.
2. Installation of safeguards of personal data – the adoption of administrative, technical or physical deterrents to safeguard personal data.

"Breach of privacy" means unjustified disclosure of private and non-trivial information about an individual (including images), which causes distress to the individual. Under the IT Act, however, there is no such concept of "personal data." As mentioned in Table 1.7 of Chapter 1, CHAPTER IX (Penalties and Adjudication) and CHAPTER XI (Offences) only define *cyber contraventions* related to unauthorized access to computer, computer system, computer network or resources, unauthorized alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, computer database, etc. According to some people sections of those chapters can be considered as the "backbone" of the data protection regime in India.

It takes tremendous amount of efforts for corporation to develop their business crucial data and yet loosing it easily if due control postures is not adopted. There have been several instances where the employees walk away with critical information and data of the company. Recall "Heartland Payment System Fraud" mentioned in Chapter 9. Although enterprises take pride in authoring and painstakingly developing confidential data over several years, there can be outsiders as well as insiders who harbor an intention to misuse it by either sharing it with the competitor or by starting his own competing business or just make it available in the public domain thus reducing its value to nil! This also may result in a tarnished brand name, loss of customer confidence, impact on the company's profit margin and loss of funds in the form of penalties and fines from regulators and loss of business and assets! In Chapter 9, the impact on organizations due to insider threats was discussed. Outsourcing of IT services support to India is on the rise and in such a scenario it becomes nation's responsibility to make good faith of our customers place in us. Without adequate measures for data protection, this would not be possible.

India, Data Privacy and Data Protection

In the last few years, there has been significant growth in India's business, data and knowledge process outsourcing industries. However, various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. The Information Technology Act is often presented, in India, as the "text regulating data protection under Indian Law." However, unlike the US or the European Union, India does not have a data protection law. Some however argue that although so far, no specific legislation pertaining to data protection has been enacted in India, the Indian Contract Act offers an alternative solution to protection data under Article 366(10). Nevertheless, no general right, relating to personal data protection, has been developed so far.

The Indian conception of "data privacy" tends to be unlike that in the European one. Although the ITA 2000 is based on the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on the International Trade Law (UNCITRAL), it is often quoted in India as an Act containing provisions pertaining to data protection. However, the concept of "personal data" is not defined. The need for a law on data protection is vital if India is to uphold investor confidence, in particular among foreign entities that send large amounts of data to India for back-office operations. Data protection is critical for outsourcing arrangements wherein an Indian company is assigned with a foreign company's confidential data or trade secrets, and/or customers' confidential and personal data. Many feel that the amendments made to the Indian IT Act are more of a knee-jerk reaction from the Government to the recent data thefts and other incidents, and that they have more to do with issues related to cybercrimes and eCommerce transactions than data protection.

Data Protection and Privacy Rights

Article 21 of the Constitution and other constitutional provisions protecting fundamental rights bestow an individual with the right to privacy. According to Article 21 of the Constitution, no person shall be denied life or personal freedom except according to the procedure recognized by law. In a number of cases, the Supreme Court of India has ruled that the right to privacy is contained in the right to life and personal liberty guaranteed to Indian citizens. However, constitutional rights can normally be claimed only against the State or State-owned enterprises and not against private individuals or establishments. An underlying purpose of the data protection principles is to protect privacy with regard to the "processing of personal data." The underlying purpose is to provide protection to the person about whom data are processed. In general, this is achieved through an amalgamation of rights for the "data subject" and obligations on those who process data or who exercise control over such processing.

The Indian Personal Data Protection Bill, 2006

Common law does not know a general right of privacy and the Indian Parliament has so far been reluctant to enact one. In view of this, the Personal Data Protection Bill 2006 was drafted to provide protection of personal data and information of an individual collected for a particular purpose by one organization and to prevent its usage by other organization for commercial purposes and to entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his/her consent.

The Bill defines personal data as "information or data which relates to a living individual who can be identified from that information or data whether collected by any Government or any private organization or agency, that is, the notion of "personally identifiable data" does exist under the Indian Personal Data Protection Bill of 2006. The Bill is aimed at protecting personal data of individuals. The Bill states that the personal data of any person obtained for a specific reason or obtained in connection with any transaction, whether by appropriate Government or by any private organization shall not be put to processing without the consent of the person concerned (i.e., the "data subject" as the term is used in the European Data Protection Legislation).

The Indian Personal Data Protection Bill, however, mentions the following exemption to the prohibition, mentioned above, regarding processing of data without the consent of the person concerned:

1. The prevention or detection of crime;
2. the prosecution of offenders;
3. the assessment or collection of any tax or duty.

The Personal Data Protection Bill imposes sanctions if the "personal data" of any person, collected by an organization (Government or Private) is disclosed to any other organization for the purposes of direct marketing or for any commercial gain and states every person whose personal data or details have been processed or disclosed for direct marketing or for any commercial gain without consent shall be entitled to compensation of damages in such manner as may be prescribed. However, the personal data of any person may be disclosed to charity and voluntary organization after obtaining prior consent of the person whose personal data is concerned. The Bill mandates that certain duties are to fulfilled by every organization (Government or Private), if the organization participates in the commercial transaction and collection of personal data. The Bill mandates that such organization shall:

1. Report to the Data Controller the type of personal data and information collected by them and the purpose for which it is being or proposed to be used.
2. Take sufficient care to maintain confidentiality and security in the handling of personal data and information.
3. Collect such information only when it is essential for completion of any transaction with the person.

Further Reading

Additional Useful Web References

1. Read article *Does India have a Data Protection Law?* at: http://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html (21 December 2010).
2. Read article *Does India need a separate data protection law?*at: http://www.knspartners.com/files/BNA%20Article-180106.pdf (18 December 2010).
3. For the Express Computer Article *Know Your Card,* visit: http://www.expresscomputeronline.com/20070910/technology02.shtml (22 December 2010).
4. For stories on data breaches, visit: http://www.guardianapps.com/index.php/resources/ (22 December 2010).

Books

1. Comprehensive coverage of privacy topics is available in Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Framework and Best Practices*, Wiley India, Delhi. Refer to Chapter 29 (Privacy – Fundamental Concepts and Principles).

2. Ibid, Chapter 2 – Threats to Information Systems
3. Bunker, G. and Fraser-King, G. (2009) *Data Leaks for Dummies*, Wiley Inc.
4. Miller, L.C. (2009) *Data Leakage for DUMMIES*, Wiley Inc.