Chapter 19
Hexa-Dimension Code of Practice for Data Privacy Protection

Wanbil William Lee
Wanbil & Associates, Hong Kong

ABSTRACT

Cyberspace inhabitants live under threat of a complex data privacy protection problem in a technology-dependent and information-intensive phenomenon grown out of a vicious circle. The frontline information security professionals are among the first to bear the brunt and are in dire need of guidance for enforcing effectively the policies and standards and mitigating the adverse consequences of data privacy breaches since the policy statements are invariably dated due to the rapid advances of the technology, limited to cope with techno-socio threats, inadequate to deal with the well-equipped and cunning cyber-criminals, and vague and less than user-friendly, or simply difficult to absorb and follow. A framework that comprises the newly developed hexa-dimension code of practice based on the six-dimension metric (represented by the LESTEF model) and an operationalization scheme are proposed, where the code in which the gist of the adopted policies is incorporated promises to be a handy reference or a quick guide capable of alleviating the information security staff's burden.

INTRODUCTION

Contemporary cyberspace inhabitants live and work in a *technology-driven information-intensive* era, a *phenomenon* born out of a *vicious circle*. The consequence is a mixture of blessing and nightmare. Data protection emerges as a critical concern and data privacy protection an urgent and vital problem for information security management. Given the situation, the front-line information security personnel is among the first to bear the brunt and in dire need of a pragmatic guidance.

A recently developed set of International Data Privacy Principles as a reference can be considered for tackling the *first need* (Zankl, 2016). Hong Kong's Personal Data (Personal) Privacy Ordinance (PDPO, 1966), a data protection principle-based law like many others legislated in western jurisdic-

DOI: 10.4018/978-1-5225-7492-7.ch019

tions, which has been in force for a number of years (Chang, 2016), can make a contribution the *second need*. To address the *third need*, a framework that comprises a 6-d code based on the 6-d metric and an operationalization scheme is recommended.

A first-cut version of the framework, which was recently presented to an audience of Information Security Management specialists (Lee, 2015a), together with the rationale of the metric, the definition of the code and its worthiness for recommendation, and an indicative guideline to operationalize the code, are described in this article.

BACKGROUND

The Vicious Circle and Technology-Driven Information-Intensive Phenomenon

Netizens are provided with such technologies as *Customer Relationship Management*, *Web-lining* and *Call Centre*, and so on; they can by means of these facilities conduct their daily activities more efficiently and effectively, and optimize the outcome of these activities, because they are better-informed and able to innovate marketing, to accelerate business promotion, to enlarge data storage capacity and communication coverage, to increase retrieval facilities, and to improve transaction speed in a more transparent and open environment. But then they will need to rely increasingly heavily on the technologies. While transparency and communication keep on improving, more and more data are consumed and correspondingly generated. This is akin to a vicious circle that "the happier the consumers of information and the higher the demand for more information leading to heavier reliance on the technology". Or in other words, as the suppliers of goods or providers of services generate more and more data in order to sustain transparency and maintain the market share thus gained, the consumers demand more and more information after having enjoyed good bargains, and consequently, the technology expands storage capacity to process the increase in volume of the data generated, and upgrades processing power to handle the increase in complexity of the applications required. This can be called a technology-driven information-intensive phenomenon. (See Figure 1).

The consequence of the technology-driven information-intensive phenomenon is good and bad. The good is the accelerated arrival of such technologies as Big Data, Cloud Computing, Internet of Things and social engineering tools. These technologies enable integration of massive, scattered datasets, efficient interpretation of the integrated data, and speedier communication of the information. An obvious benefit is that with a huge amount of information being made available, the cyber-world becomes more transparent and netizens are better informed. And the bad is that there emerges numerous additional security threats bred in the loopholes in the new technologies, in the use of them or in the facilities enabled by the massive volume of data they generate, which the cyber-miscreants are ever lurking around to exploit when detected. However, it is noteworthy that some clandestine activities which are brought to light, for example, the Snowden episode (*South China Morning Post*, 2013) and the Panama Papers leak (Wilson, 2016), can be beneficial to some people/organizations and adversary to others.

Data Privacy Protection Problem

The problem is rooted in the *way* the data are collected about and are used adversely against data subjects, and in the *right* of the data subjects to that data. It has to deal the *techno-ethical-risk* which is originated