Editorial

Heechang Shin

Hagan School of Business,
Iona College,
715 North Avenue,
New Rochelle, NY, USA
E-mail: hshin@iona.edu

1 Introduction

Business environments are constantly changing, and organisations are under pressure of responding to those changes quickly. They need to make quick managerial decisions to survive such environments. Business intelligence (BI) supports them by providing accurate information of organisational performance in real-time and tools to analyse huge volumes of data being collected everyday. Therefore, BI is increasingly essential to organisational success.

Recently, there has been a realisation that BI has impact on security. One aspect of this is that BI can be used to improve an organisation's security, e.g. for intrusion detection. Another aspect is that misuse of BI capabilities can pose potential privacy and security threats. For example, marketing BI tools integrated with location data can be used to design sales territories and marketing campaigns. The problem is that location information has the potential to infer a person's personal preferences (if the location is a specialty shop), employment status (if the location is a premise of an organisation), social network information (if the location is a house of one's friends), or health conditions (if the location is a specialised hospitals such as cancer treatment specialisation centre). Therefore, BI can impose potential security and privacy threats to users.

In light of this, this special edition of the *International Journal of Business Continuity and Risk Management* focuses on presenting innovative, high-quality research results in matters related to the growing field of BI and security management. The collection of articles herein includes both theoretical and practical solutions to the following issues: use of BI for decision support, organisational security management, security and privacy threats imposed by BI techniques and possible solutions, and risk management of critical infrastructure.

2 Use of BI for decision support

Soluade addresses the issue of software testing using the BI technique, called orthogonal defect classification (ODC). He indicates that initial release of software generally requires full exhaustive testing of all the features. Since such exhaustive testing is very costly in terms of time and money, after the initial release, only subset of full exhaustive testing cases are tested for subsequent releases according to him. In his paper, Soluade discusses how to select such testing cases. He presents three possible solutions. Among them, his focus is to use a mathematical technique, called ODC, which breaks down all the features of the software into categories, and with the aid of standard orthogonal arrays, selects which test cases to run. He indicates that experimental results show that there has been no reduction in quality as a result of testing using ODC.

Rodriguez and Shin aim to design BI methodologies for the customer churn prediction problem in wireless telecommunications industry. Customer churn is the term used to describe customers who terminate their relationship with a company according to them. They point out that since churn means a loss of revenue to a company, it is important to identify customer churn and provide incentives to them in order to retain them to the company. One main obstacle to design a model to predict customer churn is high dimensionality of customer churn dataset. It is because the performance of prediction methods is significantly degraded if inappropriate features are selected and used for building a model according to them. Various feature selection methods to identify important features (or attributes) that have significant effect on customer churn and their results are presented in their paper. Also, a set of prediction model schemes and their results are evaluated.

3 Organisational security management

Alkaabi and Maple conduct a study of security management practices on the Gulf Cooperation Council (GCC) countries and identify that there is a significant level of sensitive information-sharing among employees in the region, which will compromise user digital authentication, eventually, putting users' accounts at risk. Technology and security solutions that aim to protect the organisation's assets will be limited if staff are not fully aware and convinced of the concept of information security according to them. They discuss the consequences of this phenomenon on the GCC countries and suggest solutions based on the special characteristics of the Arab culture, which also considers human behaviour.

4 Security and privacy threats imposed by BI techniques and possible solutions

Today's BI tools allow decision makers to process data efficiently and conveniently by collecting information through Web services. Chun et al. observe that security and privacy threats imposed by mashup services, which are contents created by extracting and combining data and services from diverse data sources in an automated manner using Web services. They indicate that although mashup services make it easier for individuals to create contents and for the third party mashup organisations to access and combine individuals' data and contents, the relative ease of creation and amount of data available has unintended consequences in terms of lost privacy when data from multiple sources are combined with unexpected results. To adequately protect the privacy of individuals, they present a privacy model that has the capability of expressing privacy preferences of data source organisation, individual data holder, and mashup organisation. If the proposed privacy model is enforced, mashup services can be generated while privacy of users are still protected according to them.

Zheng et al. address the security and privacy issues raised by using mobile devices such as smartphones and tablets. They point out that as the number of mobile applications (apps) has grown rapidly, there are various apps written with malicious intents. All these apps could allow an attacker to use mobile devices as attacking tools for hacking and cyber criminality according to them. They present various attack methods that could be launched through mobile devices and also provide advices for countering such attacks.

5 Risk management of critical infrastructure

Risk management of critical infrastructure such as airports is a matter of priority for governments and private operators. Engemann conducts a case study of the 2012 labour union strike at Frankfurt International Airport, which threatened to disrupt overall operations of the transport company, Fraport AG. She finds out that amidst financial losses and relative operational chaos, Fraport not only mitigated the effects of the strike action, but also recovered quickly and remained profitable. According to her, this success invites an opportunity for US airport industry that struggles to remain viable: the federal funding system does not provide adequate resources to support the industry's improvement efforts, while the inconveniences of air travel continue to deter potential customers and limit airport-generated revenue in US airport industry. She suggests that the positive impact of Fraport's integrated business model on its recovery from the strike in 2012 can be used as benchmarks to US airline industry for better risk management.