Security Balancing for IT-Enabled Service Innovation

Ada Hui-Chuan Chen[1], Huei-Chung Chu[2], and Sou-Chein Wu[3]

[1] Ching Yun University, Department of IM, Taoyuan, Taiwan
No.229, Jianxing Road, Zhongli City, Taoyuan County, Taiwan
adahchen@cyu.edu.tw
[2] Huafan University, Department of MIS, New Taipei City, Taiwan
No. 1, Huafan Rd. Shihding Dist., New Taipei City 223, Taiwan
hcchu@cc.hfu.edu.tw
[3] National Chengchi University, Department of MIS, Taipei, Taiwan
NO.64, Sec.2, ZhiNan Rd., Wenshan District, Taipei City 11605, Taiwan
100356507@nccu.edu.tw

Abstract. As IT-enabled service innovation becomes one of the sustainable competitive advantages in organizations, ensuring the security of service information transition without dissatisfying users is a major challenge. This study indicates the drawbacks of Information Security Management System (ISMS), takes audit check list of ISO/IEC 27001 as example, reviewing five practical auditing items, and asserts that the users' view should be integrated for balancing information security.

Keywords: Information security, IT-enabled service innovation, ISMS, ISO/IEC 27001.

1 Introduction

As the economies are becoming increasingly service oriented, many organizations regard IT-enabled interactive service innovation as new business opportunities. Owing that the interactive service is a process of service co-producing, Information Technology (IT) and networks have currently played significant roles in the service chain. The major reason is that IT and related technologies are easy to get user involved the process, help users to actively participate the service producing, and the organization can also more understand the users' requirements.

Therefore, the wide spread electronic data processing through the networks requires comprehensive protection against the risks of loss, misuse, disclosure or damage. Currently, Information Security Management System (ISMS) is broadly adopted by organizations for ensuring the security of their information assets, and many related information security standards take different approach for implementing ISMS, for instance, process approach as COBIT (Control Objectives for Information and related Technology) and ITIL (IT Infrastructure Library), best practices approach as ISO 17799 and ISF SoGP (Information Security Forum Standard of Good Practice), controls as ISO 13335 and SP 800-53, and risk management as OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)[1]. However,

James J. (Jong Hyuk) Park et al. (eds.), *ITCS & STA 2012*,
LNEE 180, pp. 273–277, DOI: 10.1007/978-94-007-5082-1_34

those helpful policies/controls/countermeasures mostly adopt organizational perspective and seldom involve the users' participation or preferences. Inflexible or inadaptable security management become the retardant of service chain and may dissatisfy users, moreover, erode the bottom line. Thus, the issue of security balancing for both service providers and users should be pre-considered in information security management.

This article indicates the drawbacks of Information Security Management System, takes audit check list of ISO/IEC 27001 as example, reviewing five practical auditing items, and asserts that the users' view should be integrated for balancing information security.

2 Literature Review

2.1 IT-Enabled Service Innovation

Information Technologies-enabled service innovation refers to the use of information technologies (IT) (including the communication and networking) for development, deployment, and diffusion of a new interactive service [2]. Commerce developments in the past decade have shown that IT and the Internet have become the backbone of commerce. They underpin the operations of individual companies, tie together far-flung service chains, and increasingly, link businesses to the customers they serve [3]. A successful IT-enabled service should take into account the core essence of service, namely, a provider-client interaction that creates and captures value [4]. Therefore, all the efforts for ensuring the value realization during service providing should involve the users' view and their preferences.

2.2 Information Security Management System (ISMS)

The advent of Internet shifts the conventional business to E-commerce, and the mounting use of information technologies poses the severe security threats to all organizations. The more system or data exposure means the more possible security breaches which will imperil all kinds of corporations. The awareness of information security has urged corporate to adopt ISMS to protect their information assets from a wide range of threats. ISMS is part of overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security [5]. Owing to the attraction of offering certification, ISO/IEC 27001 becomes the most well-known standard among the ISO family. It specifies the requirements of implementing information security controls for the needs of various organizations. Generally, ISO/IEC 27001 asserts that the organizations need to [6]:

1. Analyze risks related to information security
2. Define specific and optimal security goals
3. Define methods which all activities should follow
4. Document all risks, goals, and methods
5. Implement measures to mitigate and manage risks
6. Assign accountability for risk management

7. Measure information security
8. Embed continuous improvement approach

Thus, this top down approach clearly enumerates a set of controls for information management. However, the perspective from service provider without considering users' view may erode the performance of information security system, especially in the contemporary business environment.

3 Security Balancing in Practice

It is undoubted that the strict audit procedures of ISO/IEC 27001 can enhance the information security and measure the results. The following five examples adopted from SANS audit check list of information security management [7]. The practical concern about users' perspective is included.

Table 1. Examples of integrating users' view into audit check list of ISO/IEC 27001

Reference		Audit area, objective, question		Integrate users' view
Checklist	Standard	Section	Audit Question	
Security Policy				
1.1	5.1	Information security policy		
1.1.1	5.1.1	Document	Whether there exists an information security policy, which is approved by the management, published and communicated as appropriate to all employees.	Information security policy should take into consideration of users' preference.
Organization of information security				
2.1	6.1	Internal Organization		
2.1.2	6.1.2	Information security coordination	Whether information security activities are coordinated by representatives from diverse parts of the organization, with pertinent roles and responsibilities.	The coordination process should involve the role of users.

Table 1. (*continued*)

2.2	6.2	External Parties		
2.2.2	6.2.2	Addressing security when dealing with customers	Whether all identified security requirements are fulfilled before granting customer access to the organization's information or assets.	Security requirements should pre-consider the users' preference.
Human resources security				
4.2	8.2	During employment		
4.2.2	8.2.2	Information security awareness, education and training	Whether all employees in the organization, and where relevant, contractors and third party users, receive appropriate security awareness training and regular updates in organizational policies and procedures as it pertains to their job function.	Awareness training program should include users.
Communications and Operations Management				
6.2	10.2	Third party service delivery management		
6.2.1	10.2.1	Service delivery	Whether measures are taken to ensure that the security controls, service definitions and delivery levels, included in the third party service delivery agreement, are implemented, operated and maintained by a third party.	The third party agreement should consider users' preference if the service is related to end users.

Source: Thiagarajan, V. (2006)

4 Conclusions

This study highlights the issue of security balancing in information security management system, which can affect the success or failure of service chain. Most extant standards of ISMS adopt organizational perspective to fulfill information security requirements. However, contemporary IT-enabled service innovation accentuates the process of co-producing between service providers and users. Thus,

involving users' preference in security policy establishing, requirements setting, and security awareness enhancing…etc. should be deliberately pre-considered. We illustrate five examples of ISO/IEC 27001 audit check list to verify the lack of users' involvement. The future work can be conducted to comprehensively reexamine information security standards and propose explicit approach to balancing information security.

References

1. Aceituno, V.: ISM3: A Standard for Information Security Management. ISSA Journal, 22–25 (2006)
2. Chen, A., Chang, H.L., Tsaih, R.H., Chou, S.K.: Challenges of IT-enabled Service – A Case Study of ITV Service. In: Proc. of INFORMS (2010)
3. Carr, N.: IT doesn't matter. Harvard Business Review 81(5), 41–49 (2003)
4. IBM Research, http://www.research.ibm.com/ssme/services.shtml (retrieved March 8, 2010)
5. BSI. BS 7799/ISO 27001 Auditor/Lead Auditor Training Course (2006)
6. Maxi-Pedia. ISO 27001 (ISO/IEC 27001:2005), http://www.maxi-pedia.com/ISO+27001 (retrieved)
7. Thiagarajan, V.: SANS audit check list of information security management. SANS Institute (October 2006)