Information Security Management for Higher Education Institutions

Simon K.S. Cheung

The Open University of Hong Kong
Good Shepherd Street, Homantin, Kowloon, Hong Kong
kscheung@ouhk.edu.hk

Abstract. Information security aims at protecting the information assets of an organization from any unauthorized access, disclosure and destruction. For information security to be effectively enforced, good management practices comprising policies and controls should be established. This paper investigates the information security management for higher education institutions. Based on the conventional CIA (confidentiality, integrity and availability) triad of information, eight control areas on information security are identified. They include information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. A governance framework is important for establishing the policies and executing the controls of information security. It is necessary to maintain a right balance between the technical feasibility and the flexibility and efficiency in administration.

Keywords: information security management, information security policies, information security controls.

1 Introduction

Nowadays, computer systems are highly connected through the internal networks (Intranet) and external networks (Internet) to facilitate accesses to information. This however creates the issue of information security – the protection of information assets from any unauthorized access, disclosure, modification and destruction, in order to ensure its confidentiality, integrity and availability [1, 2]. Information security is conventionally defined as the assurance of the CIA triad of information (confidentiality, integrity and availability) [1, 3], and its extension (authenticity, non-repudiation and accountability) [4, 5].

With the recent advances of communication and mobile technologies, Internet and Intranet accesses to information from client-end devices (especially mobile devices) via wired or wireless networks are very popular, such as on e-mail communication, and e-commerce and e-government services. This inevitably adds more technical complexity in ensuring that the information assets of an organization can be well protected [6, 7, 8], and therefore, some intelligent and sophisticated access protocols are developed [9, 10, 11, 12].

J.–S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 1*,
Advances in Intelligent Systems and Computing 297,
DOI: 10.1007/978-3-319-07776-5_2,

Although there are many technical solutions to help protect the information assets of an organization, the risk of information leakage, modification or destruction cannot be completely eliminated. As this may incur great losses, information security is essential to any organization which counts information assets as critical to their business operation. This is especially important for government and public bodies because the adverse impacts are much greater than that of other organizations [7, 8, 13]. Similarly, for a higher education institution where a large amount of student information is hosted student administrative systems, learning management systems and platforms [14, 15, 16], any information leakage or loss would have large impacts. Information security compliance and awareness have become emerging issues in higher education institutions [17, 18, 19].

In many countries, there are laws, regulations and policies, governing information security, such as the Data Protection Act and Computer Misuse Act in the United Kingdom and the Federal Information Security Management Act in the United States. In Hong Kong, a set of baseline policies have been established for enforcing information security in government offices [20]. Besides, many national and international standards for information security management have been established. Among these standards, the ISO 27001 Information Security Management System is the most widely adopted one [21].

This paper investigates the information security management for higher education institutions. Eight control areas for providing the rules of governance and control of information security are identified, and a framework for governance and control is discussed. These control areas include information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. The rest of this paper is organized as follows. Section 2 states the principles of information security. Section 3 elaborates the eight key control areas on information security for higher education institutions. Section 4 then discusses the governance of information security. Section 5 briefly concludes this paper.

2 Principles of Information Security

Conventionally, the CIA triad (confidentiality, integrity and availability) forms the principles of information security [1, 3]. In the literature, it has been argued that the CIA triad should be extended with three more principles, namely, authenticity, non-repudiation and accountability [4, 5]. Figure 1 shows these principles.

Confidentiality is the ability to protect information from unauthorized accesses. A typical example of unauthorized accesses is the use of another person's account and password to access an online banking system, which he or she does not possess the necessary access rights. Integrity is the ability to protect information from undetected modification or deletion. For example, in an e-mail communication, some information in the e-mail message is intercepted, modified or omitted during the message sending process. Availability is the ability to protect information from attacks denying or inconveniencing authorized accesses. It ensures that information is readily accessible to the authorized users at all times.

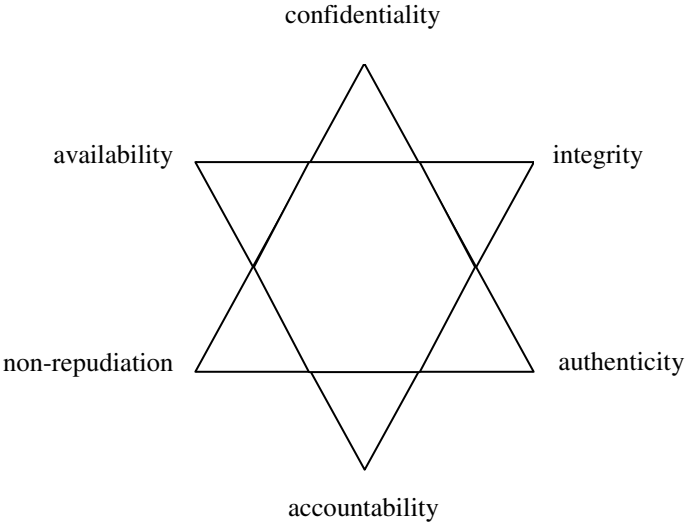

Fig. 1. Six principles of information security

Authenticity is the ability to ensure that transactions or communications of information are genuine. In order to validate accesses to information, authentication system with proper access control and password protection is adopted. Non-repudiation refers to one's intention to fulfill the accepted obligations. For example, in the transmission of information, the sender cannot deny having sent the information and the receiver cannot deny having received the information. Digital signature is often used to ensure non-repudiation. Accountability is the ability to track user identity and actions applied to the information. Accountability is a useful element for executing non-repudiation that proves the performance of an action, for example, sending or receiving information, and when and where the action was performed.

3 Information Security Controls

It is necessary for a higher education institution to establish policies and control measures for ensuring information security [17, 18]. These essentially transform the principles of information security to implementation.

The ISO 27001 Information Security Management System provides a thorough coverage of the key control areas of information security [21]. By making reference to ISO 27001, there are at least eight control areas for a higher education institution, namely, information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity.

3.1 Information Asset Controls

Policies should be established to ensure that appropriate levels of protection and accountability are maintained for information assets. This should be made in accordance with the sensitivity, criticality and values of information assets, regardless of the media on which they are stored, the manual or automated systems that process them, and the methods by which they are distributed. In a higher education institution, information assets should be classified, and the owner, custodian and users of the information assets should be well defined. It is a good practice that an institution should maintain a master record control table which shows a full list of information assets and the owner, custodian and users of the information assets. This control table is referenced in implementing control measures.

3.2 Personnel Controls

Policies should be established to ensure that everyone in an organization clearly understand his or her roles and responsibilities to reduce the risk of theft, fraud or misuse of information assets. For a higher education institution, all staff should be aware of the information security threats and concerns, and are equipped to support information security in the course of their normal work and reduce the risk of human errors. For example, staff in the Registry and Student Affair Office used to handle a large amount of student information. They have the responsibilities of protecting the student information from theft, fraud and misuse. Control measures should be in place to reduce the risk of theft, fraud or misuse of student information. In many institutions, downloading of student information to portable storage is prohibited, unless absolutely required.

3.3 Physical Controls

Policies should be established to ensure that appropriate physical security and control should be maintained to protect against any unauthorized accesses to some defined secure areas such as data centres. For a higher education institution, computer systems and storage of critical and sensitive information shall be housed in data centres with proper physical access controls. Only authorized persons are allowed to have physical accesses to the data centres, and the access logs should be maintained. Besides, proper environment controls should be in place to protect the computer systems and storage from physical damage. Temperature and humidity should be kept at an acceptable level. Gas-based fire extinguishing systems, instead of water-based fire extinguishing systems, should be installed in data centres to minimize the risk of physical damage to data storage devices in case of fire.

3.4 Access Controls

Policies should be established to ensure that access control to information systems and information processing facilities, and that access rights are properly authorized,

allocated and maintained. Control measures should be implemented to enforce authorized accesses to information as well as to reduce the risks of unauthorized access, loss or damage to information. These measures should also be applied to mobile and remote accesses. In a higher education institution, there should be proper access controls for information systems and information processing facilities, where student information and financial information are stored. An access control table should be defined for each information system. Besides, password controls should be enforced, for example, adoption of strong passwords and compulsory changes of passwords over a certain time period.

3.5 Communication Controls

Policies should be established to define procedures for the management and operation of network and communication facilities. Control measures should be implemented to maintain the confidentiality, integrity and availability of communication facilities, such as electronic mailing systems and network storage for information exchange. For a higher education institution, electronic communication is very common. Electronic mails containing student information or sensitive information should be handled with care. It is a good practice to use secured electronic mail systems to protect sensitive information from undetected interception, modification or omission. Encryption and password protection should also be applied to data files on network storage as well as mobile and portable storage devices.

3.6 Operation Controls

Policies should be established to define procedures for the management and operation of computer systems and information processing facilities. Control measures should be implemented to maintain the confidentiality, integrity and availability of the computer systems and information processing facilities. System fixes and patches, especially those related to information security, should be timely applied. Backup procedures should be tightly followed, and tapes and disks should be properly stored. It is a good practice to arrange regular system drills to ensure that all critical systems and facilities can be correctly restored in case of information security incidents. System administrator passwords should be properly maintained, and strict password controls, such as the use of strong passwords and compulsory periodical password changes, should be enforced.

3.7 Information System Controls

Policies should be established to ensure proper controls to prevent information systems from any unauthorized modification and misuse of information. Information security requirements should be clearly identified at the beginning of system development. For a higher education institution, the input, processing and output of student information should be properly defined and implemented. These should be enforced during the acquisition, development and maintenance of information

systems. All changes on information systems should be logged. It is a good practice that regular review on these information systems should be conducted to identify and fix information security loopholes if any.

3.8 Incident Management and Business Continuity

Policies should be established to ensure that information security incidents are communicated in an appropriate manner, allowing timely corrective actions to be taken. Clear procedures should be set out for handling incidents that might have an impact on information security. Incidents should be classified in term of severity and impact. According to the level of severity and the scope and impact of an incident, an appropriate incident coordinator should be appointed. On the other hand, it is a good practice that critical business processes identified and integrated with information security requirements, in order to minimize the impact to an acceptable level. For a higher education institution, teaching and learning are critical, and hence, control measures should be enforced to maintain continuity of teaching and learning activities in case of information security incidents.

4 Governance of Information Security

A governance framework is important for establishing the policies and executing the controls of information security. This section discusses the governance of information security in a higher education institution.

It is a good practice to appoint an information security officer who is responsible for the overall governance of information security. In practice, there are two models for information security governance, namely, executive-led model and committee-led model. In the executive-led model, the information security officer is a senior officer who takes the overall responsibility of information security for the institution, including decision-making and policy-making. In the committee-led model, an information security committee is established to take up the roles of an information security officer. Chaired by a senior officer, the committee comprises the owners and custodian of major information repositories, such as the Registrar, Secretary, and the Director of Information Technology.

The information security officer or information security committee is wholly responsible for the design, implementation and execution of the policies and measures on information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. It is important that appropriate authority should be given to the information security officer or information security committee for discharging these duties and responsibilities, especially in handling information security incidents and problems.

Besides implementing the policies and executing the controls, the information security officer or information security committee should conduct regular review on the compliance of information security. A typical way to review the compliance is to

conduct an information security audit. Like many security audits, an information security audit aims to check the compliance of information security with respect to the established policies, guidelines and procedures [22, 23, 24, 25]. It is a good practice for a higher education institution to establish its own audit schedule on information security. Some well-known standards can be referenced in establishing an information security audit framework [24, 25].

Finally, a higher education institution should always ensure that all its staff and students have the awareness on information security, and a thorough understanding of the prevailing policies and controls of information security. To serve this purpose, regular trainings and briefing sessions on information security should be conducted. They are especially useful for new staff and new students, and therefore better be held at the start of each semester. In addition to these trainings and briefing sessions, from time to time, any updates on the information security policies and controls should be communicated to all staff and students.

5 Conclusion

Information security is essential to higher education institutions as any information leakage and damage would incur great losses. There is a need for a higher education institution to enforce information security. Based on the principles of information security, we identify eight control areas on information security, namely, information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity. Policies, guidelines and control measures should be established. While the policies provide rules of governance of information security, the guidelines and control measures help execute and implement the policies.

It is important to address a salient point in establishing the policies, guidelines and controls on information security. In reality, flexibility and control are contradictory to each other. In order to enforce information security, it is necessary to implement control measures which inevitably create inflexibility and inconvenience. A right balance between flexibility and control is however difficult to achieve. There are also administrative considerations in implementing the policies, guidelines and control measures, such as on the availability of resources and efficiency in administration. A strong support from senior management is absolutely necessary.

References

[1] Bishop, M.: Computer Security, Art and Science. Addison-Wesley (2003)
[2] Raggad, B.G.: Information Security Management: Concepts and Practices. CRC Press (2010)
[3] Peltier, T.: Information Security Policies and Procedures: A Practitioner's Reference. CRC Press (2004)

[4] Parker, D.B.: Toward a New Framework for Information Security. In: Kabay, M.E. (ed.) The Computer Security Handbook. John Wiley (2002)
[5] Anderson, J.M.: Why We Need a New Definition of Information Security. Computer and Security 22(4), 308–313 (2003)
[6] Matbouli, H., Gao, Q.: An Overview on Web Security Threats and Impact to e-Commerce Success. In: Proceedings of the International Conference on Information Technology and e-Services, pp. 1–6. IEEE Press (2012)
[7] Singh, S., Karaulia, D.S.: E-Governance: Information Security Issues. In: Proceedings of the International Conference on Computer Science and Information Technology, pp. 120–124. IEEE Press (2011)
[8] Hwang, M.S., Li, C.T., Shen, J.J., Chu, Y.P.: Challenges in e-Government and Security of Information. Information & Security 15(1), 9–20 (2004)
[9] Akhawe, D., Barth, A., Lam, P.E., Mitchell, J.: Towards a Formal Foundation of Web Security. In: Proceedings of the IEEE Symposium on Computer Security Foundations, pp. 290–304. IEEE Press (2010)
[10] Pansa, D., Chomsiri, T.: Web Security Improvement by using Dynamic Password Authentication. In: Proceedings of the International Conference on Network and Electronic Engineering, pp. 32–36. IACSIT Press (2011)
[11] Chen, C.M., Wang, K.H., Wu, T.Y., Pan, J.S., Sun, H.M.: A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices. IEEE Transactions on Information Forensics and Security 8(8), 1318–1330 (2013)
[12] Chen, C.M., Chen, Y.H., Lin, Y.H., Sun, H.M.: Eliminating Rouge Femtocells based on Distance Bounding Protocol and Geographic Information. Expert Systems with Applications 41(2), 426–433 (2014)
[13] Cheung, K.S.: Development of Organizational Information Security Policies. In: Proceedings of the International Conference on Intelligent Computing and Intelligent Systems, pp. 753–756. IEEE Press (2011)
[14] Cheung, K.S.: A Comparison of WebCT, Blackboard and Moodle for the Teaching and Learning of Continuing Education Courses. In: Tsang, P., et al. (eds.) Enhancing Learning Through Technology, pp. 219–228. World Scientific (2006)
[15] Yau, J., Lam, J., Cheung, K.S.: A Review of E-Learning Platforms in the Age of E-Learning 2.0. In: Wang, F.L., Fong, J., Zhang, L., Lee, V.S.K. (eds.) ICHL 2009. LNCS, vol. 5685, pp. 208–217. Springer, Heidelberg (2009)
[16] Cheung, K.S., Lam, J., Yau, J.: A Review of Functional Features of E-Learning Platform in the Continuing Education Context. International Journal of Continuing Education and Lifelong Learning 2(1), 103–116 (2009)
[17] Rezgui, Y., Marks, A.: Information Security Awareness in Higher Education: An Exploratory Study. Computers & Security 27(7), 241–253 (2008)
[18] Kvavik, R.B.: Information Technology Security: Governance, Strategy and Practice in Higher Education, Center for Applied Research, EDUCAUSE (2004)
[19] Kam, H.J., Katerattanakul, P., Gogolin, G., Hong, S.: Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective. In: Proceedings of the Pacific Asia Conference on Information Systems. Association for Information Systems (2013)
[20] OGCIO, Baseline IT Security Policy, The Office of the Government Chief Information Officer, The Government of the Hong Kong Special Administrative Region, Hong Kong (2009)

[21] ISO, ISO 27000 : Information Security Management System : Family of Standards, Joint Technical Committee, International Organization for Standardization and International Electrotechnical Commission (2005)
[22] Onwubiko, C.: A Security Audit Framework for Security Management in the Enterprise. In: Jahankhani, H., Hessami, A.G., Hsu, F. (eds.) ICGS3 2009. CCIS, vol. 45, pp. 9–17. Springer, Heidelberg (2009)
[23] Lo, E.C., Marchand, M.: Security Audit: A Case Study. In: Proceedings of the Canadian Conference on Electrical and Computer Engineering, pp. 193–196. IEEE Press (2004)
[24] Kelson, N.: Information Security Management Audit and Assurance Programme. In: ISACA (2010)
[25] ISO, ISO 27007 : Guidelines for Information Security Management Systems Auditing, Joint Technical Committee, International Organization for Standardization and International Electrotechnical Commission (2011)