CONF-IRM 2008 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2008

Factors Affecting the Objectives of Information Security Management

Qingxiong Ma
University of Central Missouri, qma@ucmo.edu

Pauline Ratnasingam
University of Central Missouri, ratnasingam@ucmo.edu

44F. Factors Affecting the Objectives of Information Security Management

Qingxiong Ma
University of Central Missouri
qma@ucmo.edu

Pauline Ratnasingam
University of Central Missouri
ratnasingam@ucmo.edu

Abstract

The issue of information security management (ISM) had been widely studied with different approaches and from different perspectives. To have the right security objectives is the primary step to achieving an effective security program. Based on the contingency theory, a conceptual model of factors that determine ISM objectives was proposed. To validate this model, a web-based survey with open-ended question was conducted. The responses from 120 certified information security practitioners were categorized and analyzed. The paper contributes to theory as it extends previous studies applying the technological, organizational and environmental framework to include factors that impact ISM. Further, it contributes to practice as it increases the awareness and importance of ISM.

Keywords

Information Security Management, Objectives, Web-based survey, Qualitative analysis

1. Introduction

Like any management initiative, to establish an acceptable level of information security management (ISM) objectives is the primary step to achieving an effective security program. The objectives allow organizations to be proactive, instead of reactive (Locke & Latham 1990). Although the ISM program will vary from organization to organization with different business context and there may be no ISM objective that can fit everywhere, the factors that influence people's values and increase the understanding of ISM, based on which the decisions on the ISM objectives are made, may be shared across organizations. The knowledge of these factors not only help understand the context in which the security issues occur and the basis of the security objectives suggested by both researchers and practitioners, but also help understand the gaps between academic research and security practitioners expectation and identify the directions for future ISM research. This study aims to identify the determinant factors of ISM objectives based on the contingency theory and the qualitative analysis of the findings from certified security professionals.

2. Theoretical Background

2.1 ISM Objectives and Values

Information security has been considered to consist of three main objectives: information confidentiality, integrity, and availability (Blackwell 1998, Fried 1994, Peltier 2003). Confidentiality is the protection mechanism that keeps information from being read by unauthorized people. Breaches of confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such breaches can take place by word of mouth, printing, copying, e-mailing or creating documents and other data, etc. Integrity refers to a state of completeness, wholeness, and soundness, including mechanisms such as checking sequence numbers, check-sums, and hash totals to assure that information stored in the computer is not contaminated or changed in a way that is not appropriate. The whole system (hardware, software, communications) must be able to maintain and process data correctly without unauthorized modification or disclosure (Hutt, Bosworth, and Hoyt 1995). Availability is ensuring that data can be accessed by all authorized people. The system must provide efficient response and adequate capacity in order to support acceptable performance.

Byrnes and Porter (2003) asserted that security is more than just trying to meet the confidentiality-integrity-availability objective elements. They suggested a fourth element: *non-repudiation*. Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. It is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message (EarthWeb 2003). Other objective elements include authentication, authorization, and identification (Boykin 2003; Host 2001; Parker 2002).

To achieve the goal of ISM, a specific level of each objective element has to be defined. For example, to what level of confidentiality, a type of information or information system should be protected. Similar decision needs to be made in the level of availability. Is 99.99% level of availability enough? These decisions of security objectives are based on the process of information assets classification and risk analysis. However, there are many factors affecting the security objectives. Especially, with the Internet technology, organizational information can be accessed from many different sources throughout the world.

Previous researchers suggest that objectives are created based on people’s assumptions and values (Keeney 1992). Dhillon and Torzadeh (2006) argued that the value-focused thinking is an appropriate approach when we need to develop a comprehensive list of objectives when the reference theory may not always be appropriate for developing new constructs. Based on value-focused thinking perspective, they did a study on the assessment the information system security in organization. In the same vein, Drevin, Kruger and Steyn (2006) studied the assessment of information communication and technology security awareness in an academic environment, and they identified the fundamental objectives that are the key areas of concern and can be used in decision making in security planning.

2.2 Contingency Theory

Setting reasonable objectives ISM requires an understanding of organizations. According to James D. Thompson, one of the foremost sociological thinkers about the dynamics of complex organizations and the first systematic contingency theorist (Rushing 1976), an organization is a “open systems, hence indeterminate and faced with uncertainty…" (p 10). Survival of the system is the goal, and the parts and their relationships presumably are developed through an evolutionary process. Organizational structure is shaped by rational action to the environment. The environment includes institutions or forces (such as suppliers, customers, competitors, government regulatory agencies, public pressure) that are outside the organization, but over which the organization has little control. There must be a fit between the organizational structure and the organizational environment (Donaldson, 1995; Karlene, 1995). Environmental change causes a misfit with organization structure. When the organizational structure is "not in balance" with the environment, the organization will have low performance. Technology and other contextual and environmental factors are the main determinants of organizational structure.

Based on contingency theory, many information systems researchers have identified user requirements. For example, in the research of software project coordination, Andres and Zmud (2002) suggested that the work group's information processing needs must "match" or "fit" the information-processing capacity associated with the coordination strategies utilized. "The contingencies faced by a work unit (such as task interdependence, task uncertainty, and goal conflict) dictate the extent of information exchange and decisional autonomy required to effectively complete project tasks" (p 42). Other researchers applying contingency theory include Bailey and Pearson (1983), Baroudi, Olson, and Ives (1986), Nidumolu (1996), Lee and Grover (2000), and Becerra-Fernandez and Sabherwal (2001).

The contingency theory not only explains why organizations have to react to the organizational information security change, but also indicates that the process of this reaction is dynamic, not static. Ironically, most current security "best practices" and security management strategies are static, ineffective, and dogma-based (Tippett, 2002).

2.3 Factors Affecting ISM

Von Solms (1998) indicated that security objectives and activities must be conducted based on business objectives and requirements, and led by business management. Nosworthy (2000) recommended the following factors that should be considered during ISM implementation: people, culture, people's attitude, security education and training, ownership and responsibility. Some managerial factors were found to facilitate ISM include the support and commitment of top management, security education and training, and appropriate regulations. While the factors inhibit the ISM include, but not limited to, the lack of understanding, awareness, and financial resources. Studies also found that organizational factors such as industry type and organization size have significant impacts on the effectiveness of implementing ISM (Chang & Ho 2006; Kankanhlli et al. 2003).

In the process of technology innovation and transfer, Tornatzky and Fleischer (1990) identified three aspects of a firm's context that influence the process by which it adopts, implements, and uses technological innovations. *Technological context* describes both the existing technologies in use and new technologies relevant to the firm. *Organizational context* refers to descriptive measures about the organization such as scope, size, and the amount of slack resources available internally. *Environmental context* refers to the arena in which a firm conducts its business—its industry, competitors, and dealings with government. This technological-organizational-environmental (TOE) framework has been used by many IS researchers (Iacovou et al. 1995, Chau and Tam 1997, Thong 1999). One of the important examples is the study of E-business adoption by Zhu et al. (2005, 2006). We believe that the TOE framework is also appropriate for studying the objectives of ISM.

3. Research Model

Grounded in contingency theory, ISM objectives, and the TOE discussed above, we proposed a conceptual model of antecedents of ISM objectives (presented in Figure 1). In this framework, contingency theory and the TOE framework provides a theoretical basis for linking antecedents and ISM objectives. The ISM objectives are set by top management and are formulated in an unambiguous way based on the analysis of security threats, national/international laws, agreements, standards, and organizational business objectives. Every enterprise, department, and group (sometimes even individuals) must have a clear sense of purpose towards its information security goals. The contingency theory also helps us understand why the process is dynamic and why it is necessary to make changes to improve ISM mechanism such as an information security department or special team, appointing a Chief Security Officer (CSO), or outsourcing the security function. Thus the model provides a direction or guideline for management that ISM is an evolving process. Table 1 identifies the key constructs taken from the conceptual model and presents its definitions.

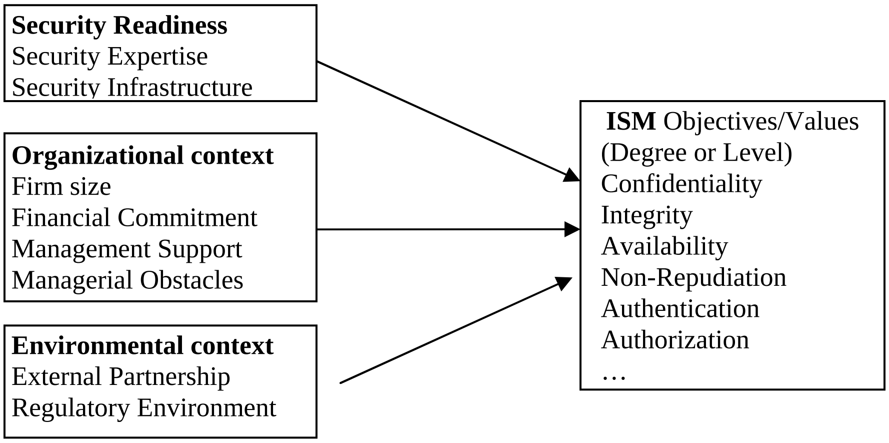

Figure 1. The Conceptual Model

4. Research Method

A web based survey with open ended question on ISM objectives was used in this study. The qualitative feedbacks were analyzed and categorized into the factors that determine ISM objectives.

4.1 Sample Subjects

One hundred twenty certified information security professionals participated in this study. The contact information was obtained from the website of the International Information Systems Security Certificate Consortium (ISC)2, a not-for-profit consortium and certification organization. This organization is charged with maintaining various Common Bodies of Knowledge (CBK) for information security professionals and for individuals seeking various certifications (including CISSP and SSCP). The directory on this website can be accessed through a search engine with search options such as certification or location (country). Utilizing this search capability, we obtained contact information for certified information security professionals who resided within the United States.

Construct	Definition
Security Expertise	IS professionals possessing the knowledge, skills and expertise to implement IS security measures in a business.
Security Infrastructure	Technological solutions that enable security control such as authorization mechanisms and anti-virus software.
Firm Size	Firm size is measured by the number of employees
Financial Commitment	Money specifically funded or budgeted to cover the expenses incurred from enforcing IS security measures.
Management Support	Practices enforced by management to facilitate IS Security implementation and management on an ongoing basis.
Managerial Obstacles	Challenges, obstacles or barriers in implementing and managing IS security such as restructuring, process changing, and acquiring new expertise.
External Partnership	IS security is affected by other businesses such as partners in the supply chain, IT security consulting services or outsourcing firms.
Regulatory Environment	Regulations of government or industry affecting a business in IS Security implementation or routinization.

Table 1. Constructs Definitions in the Conceptual Model

The majority of subjects who participated in this study are males. About 17 percent of respondents are under 30 years old, while 46 percent of the respondents are over the age of 40. Approximately 75 percent of certified information security professionals have six or more years of work experience. Over half of the respondents in this study are in management positions.

4.2 Instrument Design

The purpose of this research is to identify the determinants of ISM objectives. Unfortunately, no instrument can be borrowed or refereed from previous studies. Based on an empirical study, the researcher identified six most cited objectives, which are presented by 26 items (Appendix A). Since values are the basis on which objectives can be created (Dhillon & Torkzadeh, 2006), the respondents were asked to make any comments on these items with open-ended question. Open-ended questions allowed us to gather rich information and discover information that was not included in the objectives list.

4.3 Data Collection

The respondents were primarily contacted via email. Each e-mail contained a request to participate. Altogether, six hundred information security professionals were contacted, and 150 completed responses were received. After screening the data, we removed 21 “invalid” responses, and there were 120 usable responses remained in the dataset, which represented a response rate of 21 percent (120/600). This response rate was considered acceptable given the nature of the study.

4.4 Response Classification

Based on the proposed framework, the collected responses were categorized into one of the eight constructs. In order to validate the classifications, five independent assistants participated in this process. They were asked to classify the responses based on a given protocol (Appendix B), in which the definitions of each category and a classification table were provided. Consensus was then reached by a focus group discussion and selecting the category that received the most designation by the assistants for each response. The consensus classification was then compared to the proposed model resulting in a 60% percent agreement level. Cohen's unweighted kappa is 0.5, which is significant according to Landis and Koch (1977).

5. Findings and Discussions

The key findings after undertaking a qualitative analysis of the comments from the IS professionals are presented under the following categories.

5.1 Security Readiness

Security readiness was represented via two items: security expertise and security infrastructure. Security expertise examines the employees' level of technical skills and security infrastructure examines the technical solutions available to protect the IT system, information, and environment of the organization.

5.1.1 Security Expertise

The focus of security expertise is on the employees, especially the certified security professional's level of technical skills, knowledge and expertise in ISM. The findings suggest the need to involve both IT department and end users in managing security. Traditional risk management has been effective in addressing the security needs of a single organization and its relationships. However, globalization, business relationships, and technology pose challenges in terms of identifying roles and responsibilities pertaining to security. There is a difference in opinion among management about the awareness and importance of security. It is important to identify the roles of the employees in the IT department as to who will focus on security based on their security expertise. Further, there is a constant need to educate and train managers on the importance of security (as in training IS professionals to detect errors and correct them in a timely manner).

5.1.2 Security Infrastructure

The focus of security infrastructure is on the ability to put best use of the existing technological solutions to monitor security. The findings suggest it is important to maintain the security infrastructure as it facilitates the management of security within and outside of the organization. In particular, devices such as the use of biometrics should be center-managed, well maintained and restricted to only authorized users. Although firewalls, encryption mechanisms, authentication mechanisms, and non-repudiation mechanisms are used to facilitate ISM, they need to be continuously checked for consistency and operating properly. The emphases should be placed in the ISM processes such as risk analysis, architecture review, code inspection and security testing. Very often the lack of proper monitoring mechanisms revealed the lack of complete and effective security management.

5.2 Organizational Context

Organizational context was measured by four items: firm size, financial commitment, management support, and managerial obstacles.

5.2.1 Firm Size

Firm size examines the extent of both financial and human resources that can be available for improving ISM. The findings suggest that the size of the firm influences the quality of ISM. A large firm may have more human and technological resources available to implement a quality security procedure versus a smaller firm whose focus is on the economic returns. Further, the larger firm is able to take greater risks in implementing a variety of security mechanisms versus the smaller firm who relies on the standard operating procedures. There were also concerns with large firms on the distributed and heterogeneous environment they operate posing a lack of control in ISM due to its large scale of business processes and operations.

5.2.1 Financial Commitment

Financial commitment examines the funding allocated to improve security management. The findings suggest that effective security management costs money. Financial commitment was a great concern and challenge for IS managers as they need to value the cost budgeted and planned for security management versus the actual amount of funds spent on ISM. Further, funds were needed for non security objectives and these funds were taken from the same budget. Management needs to enhance the cohesiveness in financial decision making as they operate in a distributed management. Senior management should clearly communicate and cooperate with other managers when it comes to allocate funds to ISM and rigorously pursue efficiencies for valued items in security objectives, streamline regulatory system, and cut “red tape”.

5.2.2 Management Support

Management support focuses on the business practices where top management involvement and commitment is seen in enforcing and implementing security procedures continuously. Although the findings reflect the importance of security management, they suggest a lack of management support. Sometimes there is resistance from management when it comes to the improvement of security. Hence, the objectives of both manager of IT security and the CEO of the firm were inconsistent and lacked flexibility. Management needs to put aside their power struggles and establish an environment that entails a high degree of trust and certainty in order to ensure effective security practices.

5.2.4 Managerial Obstacles

Managerial obstacles focus on the challenges and barriers top management encountered when implementing and managing ISM. The challenges faced by the managers revealed they lacked effective ways to resolve problems. The most serious concern is that security is viewed as an afterthought, that is, after the breach and loss has occurred. Although standards and polices existed, there were no mechanisms to monitor if the standards, policies and “best business practices” were actually enforced. The IT security managers understand the importance of security, but the business unit managers were only interested in the business operations and profit by reducing cost. In most cases managers believe that their employees can be trusted which is not true in all cases. Most of them do not understand the effects and impact of security. Hence, management is faced with the challenge to enforce collaboration and restore good communication and training among all the employees on the importance of ensuring security mechanisms and best business practices.

5.3 Environmental Context

Environmental context was measured external partnerships and regulatory environment. While external partnerships examine the external stakeholders who interact with the firm and how it impacts their ISM, regulatory environment examines the audit, security policies and standards imposed to manage information security.

5.3.1 External Partnerships

The findings suggest that sometimes there is a need to outsource or seek external expertise when implementing security mechanisms such as encryption. Again managers have to ensure they consider external partners in their security planning and risk management strategies because heterogeneous stakeholders playing varying roles and also the fact that the organization may compose of diverse organizational cultures.

5.3.2 Regulatory Environment

Regulatory environment focuses on the industry and government standards and regulations that impact security implementation. Regular audit was conducted to ensure that the data centers were compiling with the security policies that were approved by corporate security. The employees would like to see that security audit was properly conducted by qualified practitioners. Even though senior management assumes that their branch office complied with the security policies, security vulnerability assessments, and used ISO evaluation criteria, there were no mechanisms in place to prove if this was actually the case. This suggests that there is a need to further improve security audit measures.

5.4 Implications

If an organization wishes to develop an information security program, the first step is to set appropriate ISM objectives based on a comprehensive understanding and assessment of their business environment as well as organizational goals.

The environmental factors should include both external and internal factors. The internal factors include business strategy, organizational size, structure, capital, available IT/IS security infrastructure and resources. External factors are institutions or forces such as suppliers, customers, competitors, government regulatory agencies, public pressure that are outside the organization, but over which the organization has little control. Businesses in some industries (government, healthcare, insurance, finance) tend to be interested in compliance with external agencies reporting requirements, and the motivation of information security is the mitigation of legal action. In these situations, it is likely the information security initiatives come from external pressure rather than internal forces.

The findings of this study were consistent with that of annual computer security survey report conducted by the Computer Security Institute (2007). The report shows that all organizations participated in the survey use firewalls, antivirus software, 80% percent use anti-spyware and 84% use VPN and 18% use biometric authentication. 78% of respondents indicated that "Network security" is important. Thus, the security infrastructure is generally considered important too. The findings also suggested that the importance for security was not emphasized as most of the organizations allocated 5% or less of their overall IT budget to ISM. The prevalence of outsourcing cybersecurity and significant level of information sharing indicated external partners are important in ISM. Last, the survey also found that “legal issues and compliance” was one of the top concerns for the respondents.

6. Conclusions

In this paper we proposed a conceptual model showing the determinants of ISM objectives based on previous studies on contingency based theory and the technological, organizational and environmental framework. Then we tested the model via open ended questionnaire with 120 certified IS professionals. The qualitative analysis paved the way to different categories of determinant factors for ISM from technological, organizational and environmental perspectives leading to effective ISM. We highlighted the key findings from each of these categories and suggested ways on how IS practitioners can enforce these factors in ISM analysis.

The paper contributes to theory as it extends previous studies by applying the technological, organizational and environmental factors that impact security management. It contributes to practice as it increases the awareness and importance of information security management and how businesses can survive in today’s competitive and uncertain web environments. Further, we discuss the implications of this study and provide suggestions and recommendations that future IS practitioners could use.

References

Andres, H. P., and Zmud, R. W., (2002). A Contingency Approach to Software Project Coordination, *Journal of Management Information Systems*, (18)3, 41-70.

Bailey, J. and Pearson, S. (1983). Development of a tool for measuring and analyzing computer user satisfaction. *Management Science*, 29, 530-545.

Baroudi, J. J., Olson, M. H., and Ives, B. (1986). An Empirical Study of the Impact of User Involvement on System Usage and Information Satisfaction. Communications of the ACM, (29)3.

Becerra-Fernandez, I., and Sabherwal, R. (2001). Organization Knowledge Management: A Contingency Perspective, J*ournal of Management Information Systems*, (18)1, 23-55.

Blackwell, E. (1998). Building a solid foundation for intranet security, *Information Systems Management*, Spring 1998, (15)2, p26, 8p.

Boykin, P. O. (2003). Practical Cryptography and Internet Applications, Classnotes (Powerpoint slides) Accessed on Feb. 25 2003,at http://www.ee.ucla.edu/~boykin/crypto_course/crypto_alg.ppt.

Byrnes, F. C. and Proctor, P. (2002). Information Security Must Balance Business Objectives (Article is provided courtesy of Prentice Hall PTR), InformIT.com, MAY 24, 2002.

Chang, S. E., and Ho, C. B., 2006 Organizational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems*, (106)3, pp. 345 – 361.

Chau, P. Y. K and Tam, K. Y. (1997) Factors Affecting the Adoption of Open Systems: An Exploratory Study, *MIS Quarterly*, (21)1, pp. 1-24.

Dhillon, G. and Torzadeh G. (2006) Value-focused assessment of information system security in organizations, *Information Systems Journal.* (16), pp. 293-314.

Donaldson, L., (1995). American anti-management theories of organization: a critique of paradigm proliferation. New York: Cambridge University Press.

Drevin, L., Kruger, H. and Steyn, T. (2006) Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment, Security and Privacy in Dynamic Environments, Springer Boston ISBN: 978-0-387-33405-9. pp. 448-453.

EarthWeb, (2003). IT management, (digital) Accessed on April 25, 2003. at http://itmanagement.webopedia.com/TERM/N/nonrepudiation.html.

Fried, L., (1994). Information security and new technology, *Information Systems Management*, Summer 1994, (11)3, p57-64.

Hutt, A. E., Bosworth, S., and Hoyt, D. B. (1995). Computer Security Handbook, Wiley.

Karlene, H. R., & Martha, G., (1995). Organization, Technology and Structuring, in Stewart R. C., Cyntha H., and Walter R. (editors), Handbook of Organization Studies. SAGE Publications, London. p.409-423.

Keeney, R. L. (1992) Value-focused thinking. Harvard University Press, Cambridge, MA. USA.

Landis, J., & Koch, G.G. (1977). The measurement of observer agreement for categorical data. Biometrics, 33, 159-174.

Lee, C. C. and Grover, V. (2000). Exploring Mediation Between Environmental and Structural Attributes: The Penetration of Communication Technologies in Manufacturing Organizations, *Journal of Management Information Systems*, (16)3, 187-213.

Locke, E. A., and Latham, G. P. (1990). A theory of goal setting and task performance. Englewood Cliffs, NJ: Prentice-Hall.

Nidumolu, S. R. (1996). A Comparison of the Structural Contingency and Risk-based Perspectives on Coordination in Software-Development Project, *Journal of Management Information Systems*, (13)2, 77-113.

Nosworthy, J.D. (2000). Implementing Information Security in the 21st century – Do you have the balancing factors? *Computers and Security*. (19)4.

Peltier, T. R. (2003). Preparing for ISO 17799, Security Management Practices, Janurary/February 2003, p21-28.

Rushing, William A. (1976). Organizations and Beyond, Lexington Books D.C. Heath and Company Lexington, Massachusetts, 1976.

Richardson, R. (2007) CSI/FBI Computer Crime and Security Survey. Accessed at http://www.gocsi.com/

Thong, J. Y. L. 1999. An integrated model of information systems adoption in small business. *Journal of Management Inform. Systems*, (15)4. pp: 187–214.

Tippett, P. (2002). *Is IT Overspending on Security?* November 20, 2002, CNET Networks, INC. Accessed at http://news.com.com/2010-1071-966448.html.

Tornatzky, L. G., M. Fleischer. 1990. *The Processes of Technological Innovation*. Lexington Books, Lexington, MA.

Von Solms, R. 1998. Information Security Management (2): guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*. (6)5. pp.221-223.

Zhu, K. and Kraemer, K. L. (2005) Post-Adoption Variations in Usage and Value of E-Business by Organizations. *Information Systems Research*, (16)1, pp. 61–84.

Zhu, K., Kraemer, K. L., and Xu, S. (2006) The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business. *Management Science* (52)10, pp. 1557–1576.

Appendix A Items for Security Objectives

Category	Definition/items
Confidentiality	Ensuring that information is not accessed by unauthorized people.
	Servers with highly classified information reside on an isolated network. Physical access to servers is strictly controlled. Confidential data is encrypted before being transmitted. Employee and customers' privacy is appropriately handled. Users do not share accounts. Users take responsibility to protect their data. Information is shared only among authorized entities. Information is protected or secured from unauthorized use.
Integrity	Ensuring that the completeness, wholeness, and readability of information are unchanged by unauthorized persons in a way that is not detectable by authorized users.
	Only the administrators can change files. All systems must have anti-virus software present. Any new data copied on a server must be logged. The company should be honest to its partners. The information should be trusted and reliable. The information should be complete.
Availability	Ensuring that a system is accessible and usable upon demand by an authorized entity, usually through redundancy.
	The systems are accessible when needed by those who need them. Backup must be available. The company should have redundancy in hardware (e.g. power supply and hard-drive) All servers must be continuously available.
Accountability	Ensuring that activities on a system can be traced to individuals who may then be held responsible for their actions.
	All account security events must be logged. All confidential file access activities must be logged All confidential data transfer must use authentication system to identify users. All connections through the secured access point must be logged.
Authentication & Non-repudiation	Ensuring that users are the persons they claim to be and the sender of a message cannot later deny having sent the message or the recipient cannot deny having received the message.
	Using password authentication Making it impossible for an unauthorized user to access the network. Using biometrics such as fingerprint, eye-scan or face-recognition. Using systems that a party cannot subsequently repudiate (reject) a transaction. All parties to a transaction must be confident that the transaction is secure.

APPENDIX B Response classification instrument

Instructions: Below is a table with each row identifies as A, B, C, D, E, F, G, and H, which are corresponding to the definitions provided. Based on the definitions, assign each response to the corresponding letter in the table below by indicating the response number in the right column after the letter. In some cases, a response may relevant to more than a single category. If this occurs, repeat the appropriate response number in all relevant rows.

A	
B	
C	
D	
E	

F	
G	
H	