Research Journal of Finance and Accounting
ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online)
Vol.9, No.24, 2018

Information Risks at Universities

Abdulmunim Shakir Abdullah Al-Duri
Al-Fiqh Department, The Great Emam University College / Iraq

Abstract
Universities, like other businesses, use information communication technology (ICT) to promote globally the opportunities of knowledge sharing, provide students and teachers the proper information and knowledge, and facilitate the administration and management decision making. Consequently, the chance of compromising the valuable assets is high. Compromising could be represented by the absence of confidentiality, availability or integrity (CIA) that could affect a university reputation negatively in addition to the cost.Therefore, universities should identify the risks that could infringe and exploit the vulnerabilities of the information systems in order to keep their assets away from malicious breaches by imposing the suitable precautions and controls in the university.
Keywords: Risk assessment, IT at university, Security at university, Common risks, Cyber security.

1. Introduction

In the current information age, Information Communication Technology (ICT) has a great affection of every aspect of people activities and plays a wide role in the field of education and training. ICT promotes, through the world, the opportunities of knowledge sharing, helping teachers and students getting up-to-date accurate information and knowledge [1]. ICT includes computers, software, special hardware, multimedia enabled devices and different types of communication facilities. It provides a free and open access tools to world wide information and has the ability to effectively support student learning [2]. Moreover, ICT plays an effective and great role in enhancing the quality of education through the wide use of applications in administration and management due to its ability to facilitate their activities in decision making, knowledge management and data storage capacity. All of that let administrators to work effectively and efficiently in their daily jobs [3].

According to the different types of activities that are supported by the networks of a university, universities, similar to other sectors, face a lot of threat attempts to obtain potentially information from users and networks that may have, to some extent, an important value for attackers.

Therefore, the importance of developing successful approaches to face such attempts is crucial and commensurate with the amount of the owned great value digital data [4].

Identifying the types of risks threatening the information systems of any university is considered essential to protect its assets from being compromised by creating an active business continuity plan and business impact analysis.

2. Business Continuity Plan (BCP)

A business continuity plan (BCP), sometimes called business continuity and resiliency planning (BCRP), is a tool that allows institutions to moderate risk in addition to continuously deliver products and services despite disruption [5].

Hence, a BCP could be considered as prevention and recovery systems to deal with potential threats to a company in order to keep operations continue under adverse conditions, such as a disaster striking and shutting down the company's headquarters. It identifies the core underlying process of the organization that affects its bottom line directly and finds alternate processes when the disruption happens.

It could be summarized as a business plan or roadmap used to follow when a case of threatens attempt to stop business continuity [6].

3. Business Impact Analysis (BIA)

Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects and to predict the consequences of an interruption or disruption to critical business operations as a result of disaster, accident or emergency.

Moreover, a BIA is necessary to gather information needed to reveal vulnerabilities and a planning component to develop recovery strategies for minimizing risk; therefore, a BIA is an essential component of an organization's business continuity plan (BCP). The result is a business impact analysis report, which describes the potential risks concern the examined organization [7].

4. Risk

Risk is existed in every aspect of our lives and many different disciplines focus on risk as it applies to them [8]. The technological era has bought with it an expectation that organisations will be accessible and operational

around the clock, so that, operating disruptions can occur with or without warning, and the results may be predictable or unknown [9].

From the information technology (IT) security point of view, risk management is the process of understanding and responding to factors that may cause a failure in the confidentiality, integrity or availability (CIA) of an information system (IS). IT security risk is the harm to a process or the related information, resulting from some intentional or accidental event that impacts the process or the related information negatively [10].

There are different interpretations of risk, and is often used to describe dangers or threats to a particular person, environment, or business. One of those interpretations with respect to information systems (IS) is:

"Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization."

To understand risk clearly, it is important to understand the different elements and how they fit together. For instance, from business perspective considerations, it is crucial to figure out the different types of threats to the organization, the organization's assets that threats may attack and need protection, the organization vulnerability to different threats, the probability of a threat will occur, its impact, the ability to reduce such threat, and how to mitigate its impact if it happens [11].

4.1 Risk Assessment (RA)

A risk assessment (RA) is to distinguish and recognise the points of weakness that make an asset of a business exposed to harm. It determines the potential hazards like fire, flood, earthquake, hurricane, supplier failure, utility outage, or cyber attack, and evaluates areas of vulnerability that may cause such hazards [12].

4.2 Cyber Security Problem facing Universities

According to the diversity of activities that university networks support, universities, like other sectors, face a lot of threat attempts to obtain potentially valuable information from users and networks.

Therefore, the importance of developing successful approaches to face such attempts is commensurate with the amount of the owned great value digital data. Digital information definitely is the main pillar of all-important activities and safety in a university. However, the security of such information is crucial due to its sensitivity and importance, such as data produced by the university represents its intellectual assets, commercial contractors which may have commercial efforts or some politically sensitive data.

Also, universities depend sometimes on data collected from third party organizations that is considered commercially, operationally, personally sensitive or might be considered sensitive by the law, as clinical data [13].

4.3 Security Awareness Risk

It could be considered that the weakness in the technology control environment is not the biggest risks to an organization's information security. Instead, security incidents could be resulted from the action or inaction by employees and personnel. For instance, disclosing information could be achieved through social engineering or accessing sensitive information unrelated to the user's role without following the proper procedures.

Therefore, it is very necessary for organizations to apply a security awareness program in order to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information.

Employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success. Monetary penalties against the organization, reputational harm to the organization and employees, and impact to an employee's job are examples of potential consequences that may occur. It is important that personnel have the complete awareness of the potential organizational harm, recognizing how such damage to the organization can affect their own jobs.

In any organization, the base of the security awareness program could be performed by establishing a minimum awareness level for all personnel. Many different ways may be used to deliver security awareness. Such ways could be formal training, computer-based training, e-mails and circulars, memos, notices, bulletins, posters. The security awareness program should be delivered in a way that fits the overall culture of the organization and has the most impact to personnel [14].

4.4 Common Information Systems Risk at University

Information systems risks could be categorized into two groups; physical and logical. Each should have its measurement to keep business protected and work properly.

4.4.1 Physical risks

These risks include identified natural and environmental hazards. Suitable barriers and controls governing the physical access to, and the maintenance of, the integrity of critical university ICT assets must be deployed commensurate with the identified risk. Barriers and controls may include, electronic access control to servers and

critical network infrastructure, installations of grillwork surrounding and enclosing video systems, fire suppression, and power management systems. Multifunction devices, servers, communication switches, personal computers, cameras, printers, scanners, multimedia projectors, books and manuals are physical ICT assets but shall not be limited to.

4.4.2 Logical risks

Authentication and authorization functions must be employed for all users of university electronic data and information resources; otherwise, they represent a noticeable vulnerability that threatens the university assets. Examples are user passwords for network and application access, biometric access mechanism, tokens and electronic key devices.

Moreover, upgrading and installation of the most released versions and security patches for the used software and firmware in all computers, switches, routers and other network-attached devices in a university are so important to lessen the risk of threats [15].

Another risk is Malware. It is software used to perform malicious actions by cyber criminals. Actually, the term malware is a combination of two words: malicious and software. It targets any computing device, including computers, smartphones and tablets [16] and may be represented by, but is not limited to, spyware, viruses, worms and spam [15].

The purpose behind using malware by cyber criminals includes, but not limited to, stealing confidential data, harvesting logins and passwords, sending spam emails, launching denial of service attacks and identity theft. However, to minimize the risk of malware threats attacks every computer and mobile devices in a university could be achieved by installing anti-virus software (sometimes called anti-malware) from trusted vendors and updating it regularly due to the constantly innovation of cyber attackers [16].

Network Interconnections are impossible to avoid in the ordinary course of business. Such interconnections among networks are gates for unauthorized access and entry to university networks. Thus, they will pose significant risk to the university data and information resources.

Consequently, some prudence should be taken in account so all networks interconnections should be guarded and audited by processes and such perimeter defense and intrusion detection systems, as are appropriate to manage and mitigate these risks.

Access to university critical systems may represent an impact risk. The university major systems used for its daily operations are essential. Any unauthorized breaches to their integrity or availability for a certain period of time could negatively affect the service delivery availability that may lead to lose the university reputation. Such systems may include the student administration system, online teaching and learning platforms, the financial management system, the enterprise planning and/or human resource management information system. Hence, these critical systems that represent a great value for any university shall be provided with an elevated level of security. These additional measures shall include, but are not limited to, internal firewalls, secondary access challenges and biometric access controls [15].

4.5 Importance of Risk Management

Risk assessment involves three processes: risk assessment, risk mitigation, and evaluation and assessment. It is a process that permits the IT managers to balance both costs; operational and economic, of protective measures and achieve gains in mission ability by keeping IT systems and data used to achieve the organization's mission protected. Indeed, such process pervades decision-making of every chain in our daily lives. For instance, many people may install monitoring systems and pay a monthly fee to a service provider for the better protection of their properties, balancing between the protecting system and the monitored assets cost.

In any organizational unit, the headmaster should be certain and ensure that the organization have the capability needed to achieve its mission. On the other hand, the organization owners should take in account the standalone security capabilities of their IT systems to provide the drawn level of mission support which face the real-world threats.

Most organizations have tight budgets for IT security; therefore, as similar as other management decisions, IT security spending must be reviewed carefully. Using effectively a well-structured risk management methodology can help management identify appropriate controls for providing the mission-essential security capabilities [17].

5. Conclusion

Risks, in general, could be of different ways and images depending on the assets of the business they exploit and their value. Universities should pay more attention to the predictable and non-predictable risks intentionally or accidentally happened that lead to interrupt or disrupt a university operations and reputation. Universities should implement and follow a business continuity plan (BCP) and focus on a business impact analysis (BIA) that results a business impact analysis report, which describes the potential risks specific to the university studied.

Moreover, Common risks at universities have several types; physical and logical. Physical risks should be

deployed suitable barriers and controls to govern the physical access and maintenance of any critical university ICT assets and must be deployed with the identified risk commensurably. Logical risks could be authentication and authorization functions, upgrading and installation of the most released versions and security patches for the used software and firmware in all computers, switches, routers and other network-attached devices. Logical risks could also be malware and network interconnections, all are noticeable vulnerabilities and may represent an impact risks at the university.

References

[1] Irshad Hussain and Muhammad Safdar (2008). Role of Information Technologies in Teaching Learning Process: Perception of the Faculty. Turkish Online Journal of Distance Education-TOJDE. 9(2), 46.

[2] Dipak R. Kawade, Sidheshwar N. Kulkarni (2012). Use of ICT in Primary School. *14th National Conference*. Pioneer Journal. Retrieved on May 5, 2017 from http://pioneerjournal.in/conferences/tech-knowledge/14th-national-conference/3798-use-of-ict-in-primary- school.html.

[3] Simin Ghavifekr, Mojgan Afshari, Saedah Siraj and Kalaivani Seger (2013). ICT Application for Administration and Management: A Conceptual Review. *13th International Educational Technology Conference*. Procedia - Social and Behavioral Sciences 103 (2013). 1344 – 1351.

[4] Bill Wyman, Walt Scrivens, Phil Hoffman and Bob Rudis (2014). What is Malware. *Ouch!* SANS Securing the Human. Retrieved on May 5, 2017 from https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201402_en.pdf

[5] The Office of Critical Infrastructure Protection and Emergency Preparedness. A Guide to Business Continuity Planning. Minister of Public Works and Government Services, Government of Canada. ISBN 0-662-33764-6. Retrieved on May 6, 2017 from https://www.gov.mb.ca/emo/pdfs/bcont_e.pdf

[6] Charles Intrieri (2013). Business Continuity Planning. *Operations and Supply Chain, Flevy Blog*. Retrieved on May 6, 2017 from http://flevy.com/blog/business-continuity-planning/

[7] Margaret Rouse (2015). Business Impact Analysis (BIA). *Business Continuity and Disaster Recovery Plans: Essential Guide*. TechTarget. (pp. 1-2). Retrieved on May 7, 2017 from http://searchstorage.techtarget.com/definition/business-impact-analysis.

[8] Steve Elky (2006). An Introduction to Information System Risk Management. *InfoSec Reading Room*. SANS Institute 2007. (1). Retrieved on May 7, 2017 from https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

[9] Business Continuity Planning (2013). *IT Examination Handbook*. Federal Financial Institutions Examination Council. (1). Retrieved on May 8, 2017 from https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum06/bcp.pdf

[10] Steve Elky (2006). An Introduction to Information System Risk Management. *InfoSec Reading Room*. SANS Institute 2007. (1). Retrieved on May 9, 2017 from https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

[11] Risk Assessment Special Interest Group (SIG) PCI Security Standards Council (2012). *Information Supplement: PCI DSS Risk Assessment Guidelines*. 3-8.

[12] Margaret Rouse (2015). Business Impact Analysis (BIA). *Business Continuity and Disaster Recovery Plans: Essential Guide*. TechTarget. (pp. 1-2). Retrieved on May 9, 2017 from http://searchstorage.techtarget.com/definition/business-impact-analysis.

[13] Universities UK. *Cyber Security and Universities: Managing the Risk*. November (2013).

[14] Security Awareness Program Special Interest Group PCI Security Standards Council (2014). *Best Practices for Implementing a Security Awareness Program*. PCI Data Security Standard (PCI DSS). Ver. (1). (pp. 1-5).

[15] The University of The West Indies (2008). *Information & Communication Technology Security Policy*. Retrieved on May 9, 2017 from https://sta.uwi.edu/resources/policies/ICT_Security_Policy.pdf

[16] What is Malware (2014, February). *Oach!*. SANS. Retrieved on May 10, 2017 from https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201402_en.pdf

[17] Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002, July). *Risk Management Guide for Information Technology Systems.* Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST) Special Publication 800-30. Retrieved on May 10, 2017 from NIST http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf