Information Security Updates

Information Security Management

Issue 5

Related Article

Vodafone UK receives information security management system certification

Vodafone UK has received a globally recognised certification relating to the provision of IT services such as application hosting, data management, technical support and consultancy for its business customers.
By attaining the ISO 27001 certification, it demonstrates that it continues to deliver the most reliable and secure information systems for customers on the UK's network.

(http://www.iwr.co.uk/business/3010444/Vodafone-UK-receives-information-security-management-system-certification)

Related Article

Universities push to turn out cyber guards as demand explodes

U.S. agencies face a shortage of professionals to protect America's computers and networks from assault, warns the head of Carnegie Mellon University's Information Networking Institute.
"There's not enough emphasis and work at colleges and universities to get people to pursue cyber security training," McManus said. "And because of the shortage, much of the work is being done by contractors, so it costs taxpayers more money."

(http://www.pittsburghlive.com/x/pittsburghtrib/news/pittsburgh/s_698162.html)

I. Background

Industry Story

Once More into the Breach

Security breaches have been found in higher education sector during the last few years. University of California, San Francisco (USCF) has discovered an unauthorised access to a file server storing Social Security numbers and bank account information, which has caused a potential data security breach impacting 46,000 individuals. Another security breach in University of California, Los Angeles has been reported that approximately 800,000 student, faculty, and staff records had been compromised in a series of intrusions.

According to John DiMaria of BSI Group, security breaches stem from poor risk analysis / management and consistency of processes. Most organisations think that technology is the answer to mitigating risk while they ignore the "Egg Shell" security problem (hard-core technology on the outside; firewalls, penetration testing, passwords, segmentation, etc., but no controls governing the information within the organisation's walls, lack of training and awareness, no classification of information, no formal controls, absence of or poor access and incident management, and so on). In essence, information security management is of the same importance of the technologies used for preventing security breaches.

A popular solution to information security management, as suggested by John DiMaria, is to adopt the international standards such as ISO 27001, which are used around the world and promotes the adoption of a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security management system.

See the article:
(http://campustechnology.com/Articles/2007/04/Once-More-unto-the-Breach.aspx?sc_lang=en&Page=1)

Information Security Management System (ISMS)

An ISMS is a systematic approach to managing universities' sensitive information so that it remains secure. An ISMS includes a set of policies and procedures concerned with information security protection, encompassing three key elements: 1) people; 2) processes; and 3) IT systems.

Some well-known international standards of ISMS are ISO 27001, Standard of Good Practice (SOGP), COBIT and ITIL. Among them, ISO is the best known standard for ISMS, which helps to establish and maintain an effective information management system via a continual improvement approach.

Reference:
http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/
http://www.bsi-emea.com/InformationSecurity/Overview/WhatisanISMS.xalter

Related Article

Sydney Water IT security manager talks governance strategy

Information security governance should not be treated like corporate governance, IT security steering committees must have the right stakeholders and the board can remain largely unaware of security issues. Those are key strategies for effective security governance, says IT security and assurance manager at Sydney Water, Stephen Frede.
"One of the things I want to make sure is the policy we have is workable and is enforceable in practice. We create interim guidelines and ask people to follow it and make refinements around that," Frede said.

(http://www.cio.com.au/article/359412/sydney_water_it_security_manager_talks_governance_strategy/?fp=4&fpid=21)

Related Article

Mandatory requirements of ISO/IEC 27001:2005

ISO/IEC 27001 is written as a formalised specification such that accredited certification auditors are meant to be able to use the standard as a formal description of items that their clients must have in order to be certified compliant. It does indeed specify certain mandatory documents explicitly. However, in other areas it is more vague and, in practice, other documents are commonly demanded, including certain items which provide the auditors with evidence or proof that the ISMS is operating.

(http://www.iso27001security.com/html/27001.html)

II. Management

ISMS Life Cycle

Management should establish an ISMS life cycle to support the ISMS within universities. A good example of ISMS life cycle is the "Plan-Do-Check-Act" model utilised by ISO 27001, which aims to establish, implement, monitor and improve the effectiveness of information security management in a continuous manner. The model has the following four phases:

a) **"Plan" phase** – establishing the ISMS
b) **"Do" phase** – implementing and operating the ISMS
c) **"Check" phase** – monitoring and reviewing the ISMS
d) **"Act" phase** – maintaining and improving the ISMS

ISMS Coverage

Management should ensure ISMS cover all areas that critical to universities information security protection. In ISO 27001, there are 11 domains to address the main security issues from the management's point of view:

1) **Security Policy** – Key information security directives and mandates for the entire organisation required by top management.

2) **Organising Information Security –** Internal and external information security governance structure.

3) **Asset Management** – Policies and procedures that determine what information assets an organisation holds, and how to manage their security appropriately.

4) **Human Resources Security** – Human resource background screening, security awareness, training and educational activities.

5) **Physical and Environmental Security** – Requirement on physical protection of IT equipment against malicious or accidental damage, theft, overheating and power outage etc.

6) **Communications and Operations Management** – Security controls over systems and network management.

7) **Access Control –** Logical access controls over IT systems, network and data to prevent unauthorised use.

8) **Information System Acquisition, Development and Maintenance** – Systems Development Lifecycle (SDLC) processes for specifying, building / acquiring, testing, implementing and maintaining IT systems.

9) **Information Security Incident Management –** Management procedures for information security events, incidents and weaknesses.

10) **Business Continuity Management** – Procedures for IT disaster recovery planning, business continuity management and contingency planning.

11) **Compliance** – Compliance with laws, regulations, security policies and standards, technical compliance, and Information systems audit considerations.

References:
http://www.ogcio.gov.hk/eng/prodev/download/s17.pdf
http://www.iso27001security.com/html/27002.html

II. Management (Cont'd)

Roles and Responsibilities of the Management

1. **Oversee ISMS**
   Universities' management is responsible for overseeing the development, implementation, and maintenance of ISMS. This includes defining the information security objectives of the organisation, allocating sufficient financial or human resources in information security, and ensuring the compliancy and enforcement of implementation.

2. **Establish Information Security Management Committee**
   University management, IT department, administrative departments and various faculties may have different perspectives on information security. One of the ways to bridge this gap is by setting up an Information Security Management Committee.

   The IS Management Committee is responsible for identifying information security risks of each operation unit within the university and determine how ISMS implementation should respond.

   A successful IS Management Committee should delegate the responsibility of operating the ISMS to different parties within the university, taking into account the organisational size, complexity, culture, nature of operations, and any other relevant factors. Furthermore, segregation of duties, accountability and capability of individuals should also be observed during the delegation process.

3. **Integrate Security Controls**
   Management should ensure integration of security controls throughout the university by performing the following:

   - Ensuring security processes are governed by university's policies and practices that are consistently applied;
   - Requiring information with similar criticality and sensitivity characteristics be protected consistently regardless of where they reside;
   - Enforcing compliance with the security program in a balanced and consistent manner across the university; and
   - Directing resources to enhance security awareness of staff and student on an on-going basis.

4. **Assign a Team for Security Administration**
   The team or the information security department should directly manage or oversee risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. Information security officers should have the authority to respond to a security event by ordering emergency actions to protect the university from an imminent loss of information or value. They should have sufficient knowledge, background, and training, as well as an organisational position, to enable them to perform their assigned tasks.

Related Article

eRevMax Recertified for ISO/IEC 27001:2005

eRevMax Technologies, pioneer in hotel online distribution, channel and revenue management tools, has been recertified for its information security management standards. Following a stringent audit overseen by DNV, an internationally accredited certification organisation, eRevMax received ISO/IEC 27001:2005 for the next three years. The initial certification was achieved in 2007.

With effective ISMS implementation, eRevMax continues to identify and address all the key information security risks with appropriate mitigation and contingencies to ensure smooth business operations.

(http://press-releases.techwhack.com/103170-erevmax-technologies)

Related Article

An ISMS Implementation Practice in Environments with Limited Resources

SMEs are prime security targets as they heavily rely on Microsoft. More than half of the SMEs that receive successful Internet attacks won't know they were attacked. 70% attacks that cause more than $50,000 in damage involve an insider.

It's possible to have affordable ISMS solution for units with simple networks. We may apply this model to a group of units with similar network environments?

(http://www.oecd.org/dataoecd/11/21/35492482.pdf)

References:
http://www.iso27001security.com/html/27002.html
http://www.cybersecurity.my/data/content_files/11/51.pdf?.diff=1176336743
http://www.ogcio.gov.hk/eng/prodev/download/s17.pdf

Related Article

Security awareness: Turning your people into your first line of defence

A new report from PricewaterhouseCoopers LLP (PwC) explores how organizations should be making employees the first line of defence against damaging security incidents.

The report suggests that the response of organizations to improving protection and reducing risks has historically been strongly biased towards further investment in technology. In essence, they have been solving what are perceived to be technical issues with technical solutions.

(http://www.ukmediacentre.pwc.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1750)

Statistical Report

Global security threats have reached record levels

IBM has released the results of its X-Force 2010 Mid-Year Trend and Risk Report, which showed that vulnerability disclosures are increasing dramatically, having reached record levels for the first half of 2010.

Overall, 4,396 new vulnerabilities were documented by the X-Force Research and Development team in the first half of 2010, a 36 percent increase over the same time period last year. Over half, 55 percent, of all these disclosed vulnerabilities had no vendor-supplied patch at the end of the period.

(http://www.continuitycentral.com/news05323.html)

III. General Users

Security Awareness

User security awareness training is one of the most common means available to achieve recognition of responsibility and computing asset worth. Universities may require each of their staff, students or third party users to sign an agreement that includes the protection of information assets prior to the commencement of employment, study or service. All external users connected to universities' network should also sign confidential or non-disclosure agreements as a condition of being allowed to access universities' information assets.

Job Function

All universities' members should understand that information security is an important part of their job functions. Liability of observing information security policies and procedures should be incorporated into each job description. Security function or expectations required by the universities should be explicitly spelled out within the job description to establish users' commitment to information security, as well as emphasises that it is part of their job duties. After it is made part of the job description, it becomes something that can be considered in performance evaluations.

Roles and Responsibilities of the General User

Information users, including university's staff, students and any other third party users, are only authorised to access and use information in accordance with ISMS framework established by the university. In addition, being granted with access to information does not imply or confer users' authority to grant other users with access to that information.

Users should know, understand, and be held accountable for fulfilling their security responsibilities. There are variable means of ensuring users understanding and recognition of their responsibilities. Typically, users should be responsible for the following acceptable use of universities' information asset:

- Using the information only for the purpose intended by the information owner or custodian, and on a need-to-know basis;
- Complying with all information security controls established by the information owner or custodian; and
- Ensuring that all classified or sensitive information is not disclosed to anyone without permission of the owner or custodian.

Conclusion

Information security requires ongoing efforts of the university to exercise their due care and due diligence in protecting the information assets. Implementing an ISMS within the university will provide an effective and structured solution to achieve this objective.

References:
http://www.cybersecurity.my/data/content_files/11/51.pdf?.diff=1176336743
http://www.ogcio.gov.hk/eng/prodev/download/s17.pdf