Information Security Updates

Compliance Management

Issue 15

Related Article

Cloud legal issues III: Data privacy laws in Asia

Cloud service providers have been hearing customer concerns regarding a potential 'seizure' of data that resides in Hong Kong data centres by the Chinese government for various reasons. As Hong Kong essentially operates in a legal jurisdiction that is totally separate from that of China, cloud service providers and potential cloud service customers will welcome a clearly worded position paper from the Hong Kong government, which clarifies the ownership of data between the Hong Kong and China.

(http://www.asiacloudforum.com/content/cloud-legal-issues-iii-data-privacy-laws-asia)

Related Article

Hong Kong Privacy Commissioner Solicits Views on Proposal for Data User Returns

The Hong Kong Privacy Commissioner has issued a proposal to require a wide range of data users to submit information about their activities to the Office of the Privacy Commissioner for Personal Data. If the proposal moves forward, data users could be required to provide information such as the kinds of personal data they control, and the purposes for which the data are used, in their data user return.

(http://www.huntonprivacyblog.com/2011/07/articles/international/hong-kong-privacy-commissioner-solicits-views-on-proposal-for-data-user-returns/)

I. Background

Industry Story

INTERNET LAW – Hong Kong's Criminal Copyright Infringement: What Constitutes a Copy Capable of Distribution?

Hong Kong not only tightened its copyright laws, but its authorities are actively prosecuting copyright violations – a smart move in an increasingly globalised economy.

In the case of Chan Nai Ming vs. HKSAR, the respondent was charged with attempting criminal copyright infringement for unlicensed dissemination of copyright films via the Internet, particularly through the use of "BitTorrent" technology. It was proven that respondent downloaded a copy of the copyright film in his computer's hard drive and made arrangements to allow transmission of this file.

Thus, a digital copy constitutes a copy under Hong Kong's copyright law and distribution of copyright works through software of other technological means may constitute distribution under the same law.

See the article:
(http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2257)

Compliance Management Overview

Compliance management is the procedure adopted by universities to comply with applicable statutory, regulatory and contractual requirements related to information security.

It is an integrated approach implemented within universities which usually include the following components:

- Identification of Compliance Requirement on Information Security;
- Monitoring of Compliance Status;
- Reporting on and Handling of Noncompliance; and
- Education and Training.

Reference:
http://www.infosec.gov.hk/english/technical/files/overview.pdf

Relevant Ordinances

Computer Crimes Ordinance

The main piece of legislation which has been introduced against computer related crime is the Computer Crimes Ordinance.

Enacted in 1993, it has, through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), created some new offences and broadened the coverage of existing offences including:

- Telecommunication Ordinance S. 27A, Cap. 106
- Crimes Ordinance S. 59 and 60, Cap. 200, S. 85, Cap. 200, S. 59, Cap. 200, and S. 161, Cap. 200
- Theft Ordinance S. 11, Cap. 210, and S. 19, Cap. 210

(http://www.infosec.gov.hk/english/ordinances/corresponding.html)

Related Article

Corporate Compliance Program and Effective Corporate Ethics

Leading organisations build regulatory compliance training into a cycle of oversight to promote a code of business conduct throughout every level of an organisation.

Taking a business process approach to corporate governance and accountability proactively manages ethics and compliance risk throughout the definition & prevention of legal risks, detection, & response of noncompliance and evaluation of improvement opportunities.

(http://www.lrn.com/resources/corporate-compliance-program-and-effective-corporate-ethics.html)

II. Management

Identification of Compliance Requirement on Information Security

In Hong Kong, there are a variety of statutory and regulatory requirements applicable to information security. The following lists a few legislations that are closely related to university environment.

- **Personal Data (Privacy) Ordinance**

  In order to protect the privacy interests, this Ordinance includes any data relating directly or indirectly to a living individual, from which it is practicable to ascertain the identity of the individual. Alternatively speaking, the Ordinance applies to any person who controls the collection, holding, processing or use of personal data.

  There are many kinds of information governed by the Ordinance in universities and such information is usually stored and processed within the information systems. For example, student records with application information and examination scores; employment records with HKID numbers and home addresses.

- **Copyright Ordinance**

  The Copyright Ordinance currently in force in Hong Kong provides comprehensive protection for recognised categories of literary, dramatic, musical and artistic works, as well as for films, television broadcasts and cable diffusion, and works made available to the public on the Internet.

  Copyright penetrates the daily operations of universities in every aspect. Research papers, patents and software are common things that come with copyright issues. The convenience brought by the Internet through resource sharing also created more possibilities for violating this Ordinance.

- **Crimes Ordinance**

  The Crimes Ordinance has extended the meaning of property to include any program or data held in a computer or in computer storage medium as "Property". Therefore, criminal activities (e.g. misuse, damage, unauthorised access, etc.) made to properties should be charged under the Crimes Ordinance.

  Compared to business organisations, universities are relatively open environments with many places accessible by the public. Especially many universities offer the students or the public with free access to their wireless network and websites, containing a wide range of electronic resources including e-books, teaching materials or even software.

Besides the statutory and regulatory requirements, there are also contractual requirements that universities have to comply with. Universities should ensure that all contracts with third parties are regularly examined for any contractual requirements relevant to information security.

References:
http://www.pcpd.org.hk/english/ordinance/ordglance.html
http://www.ipd.gov.hk/eng/pub_press/publications/hk.htm
http://www.infosec.gov.hk/english/ordinances/corresponding.html

Recent Incident

A university in Hong Kong lost students and tutors' data

In March 2009, one university in Hong Kong ("the university") had lost a USB flash drive which contained personal data of students and tutors.

In relation to this incident, the Hong Kong Privacy Commissioner is in the course of conducting a compliance check to find out whether or not the university had taken practicable security measures to protect the personal data held by it from unauthorized or accidental access.

The Commissioner wishes to draw the attention of all data users to Data Protection Principle 4 of the Personal Data (Privacy) Ordinance, which requires them to take all practicable steps to ensure that the personal data held by them are protected against unauthorized or accidental access, processing, erasure or other use.

(http://www.pcpd.org.hk/english/infocentre/press_20090313.html)

Related Article

Principles of Legal Compliance

There are 6 principles for building an effective compliance management procedure:

1. Commitment
2. Ownership
3. Demonstrable (Transparency)
4. Comprehensive
5. Systematic
6. Ongoing Development

(http://www.solgm.co.nz/AboutUs/PrinciplesofLegalCompliance.htm)

II. Management (Cont'd)

Monitoring of Compliance Status

Once identified the applicable statutory, regulatory and contractual requirements that are applicable to universities, management should invest appropriate resources to know whether these requirements are complied with relevant parties.

The compliance lies with the process or asset owners, therefore, they own the responsibilities to ascertain the process or procedures in place to ensure the compliance. Periodic checking can be performed to collect compliance status from the process or asset owners, including noncompliance issues occurred, changes to processes that may affect universities compliance with certain statutory, regulatory or contractual requirements. The checking results should be reviewed by the management to ensure any noncompliance issues are timely followed up for further remedial action.

Reporting on and Handling of Noncompliance

Noncompliance reported to the process or asset owners should be timely dealt with and escalated to senior management level as appropriate. The remediation should be identified and timely deployed. Management should also monitor the progress of remedial actions till completion.

For substantial noncompliance issues, including singular or systemic / recurring ones, they should be attended with higher priority and considered for more frequent monitoring.

Universities may utilise their existing incident handling and escalation procedures to incorporate the noncompliance reporting and handling process. Noncompliance can be defined as one of the incident types with possible consequences anticipated and corresponding handling procedures designed.

Education and Training

Achieving compliance requires the commitment not only from the management but also the efforts from the staff members, students and third party contractors. Adequate trainings should be delivered to them to introduce the relevant statutory, regulatory or contractual requirements and necessary steps towards full compliance. The training can include the following points:

- Legislations in Hong Kong that have applicable sections related to information security;
- Procedures that should be followed in order to comply with the above legislations; and
- Reporting procedures for noncompliance.

Process or asset owners should inform the relevant personnel (e.g. Compliance Officer) regarding any changes to the statutory, regulatory or contractual requirements, as well as the resulting changes to the operational procedures.

References:
http://policy.cqu.edu.au/Policy/policy_file.do?policyid=1843

Related Article

Hong Kong cyber crime cases soar in 2009

Computer usage is synonymous to Hong Kong homes and business.

Hong Kong people often use these machines for day to day life, whether checking stocks and communicating with friends to discussing projects and office deadlines at work. No wonder the incidence of cybercrime has been soaring during the past year.

Up to November of 2009 there were 1,378 cases were reported. This was a sharp increase compared to 791 of the entire 2008 and 678 in 2007, police data has revealed.

(http://asiancorrespondent.com/27176/hong-kong-cyber-crime-cases-soar-in-2009/)

Related Article

Discussion Paper Addressing Information Security Issues in the HKSAR

There has been growing concern cover information security in Hong Kong, given the increasing number of security-related incidents reported by the media in recent years.

In addition to the traditional viruses and hacking activities, the recent phishing scams and the nuisances caused by spamming have shaken public confidence in the security of IT products and services.

(http://www.sinchungkai.org.hk/demo/eng/work_with_the_industry/pdf/task_force/0405/information_security/discussion_paper_on_information_security.pdf)

III. General User

Roles and Responsibilities

General users play a vital role in the compliance management of universities. They must understand what should do and what should not do in order to achieve compliance with the relevant statutory, regulatory and contractual requirements.

The following are some of the major responsibilities for general users in the compliance management:

- Attend the trainings and familiarise themselves with the legislations and contract terms related to information security;
- Follow the instructions and established procedures by universities to ensure compliance or avoid noncompliance;
- Consult the responsible staff (e.g. Helpdesk, Process or Asset Owners) when they cannot tell whether certain actions may lead to noncompliance issues;
- Be alert and report to the right party for any noncompliance noted; and
- Assist the management in investigating and remediating noncompliance issues.

Conclusion

With the increasingly tightening of statutory, regulatory or contractual requirements on the information security, universities should invest sufficient resources to ensure that adequate controls are implemented to achieve effective compliance management process. Such process should govern the whole compliance lifecycle including compliance requirement identification, monitoring, noncompliance handling and user education.

References:
http://benchmarks.cisecurity.org/tools2/windows/CIS_WindowsXP_Benchmark_v2.01.pdf