HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

29 Nov 2006

Examinations on Controls over Customer Data Protection

Our Ref: B1/15C

29 November 2006

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Examinations on Controls over Customer Data Protection

The Hong Kong Monetary Authority (HKMA) has recently completed a round of on-site examinations of selected authorized institutions (AIs) on their controls over customer data protection.

In general, all AIs examined have strengthened their security controls after completing the data security self-assessment requested by the HKMA in 2005. Nevertheless, given the increasing usage of portable IT equipment and the need to access customer data by a wider range of staff, we consider it necessary for AIs to step up their measures for safeguarding sensitive customer data that are stored in relatively less controlled peripheral devices (such as notebook computers, PDA devices, USB memory devices and CD-ROMs) and on hardcopy documents, and that are processed and maintained by outside service providers.

To ensure that the risk of confidential data leakage is properly and adequately managed, I set out in Annex 1 and Annex 2 respectively for your reference a list of major common issues and some good practices adopted by certain AIs identified during our on-site examinations. I would also like to take this opportunity to remind your institution of the need to regularly assess the adequacy of data security controls within your operating environment as well as the control environment of any outside service providers having regard to the latest security threats and technological advancement.

Should you have any questions about the content of this circular, please contact Mr. Shu-pui Li at 2878-1826 or Mr. Raymond Suen at 2878-1817.

Yours faithfully,

Arthur Yuen
Executive Director
(Banking Supervision)

Encl

Annex 1 - Common Controls Issues Identified

Compliance with Personal Data (Privacy) Ordinance and regulatory requirements

- Some AIs have kept certain personal data (e.g. rejected credit card application files and supporting documents) longer than the data retention period stated in the customer agreements. AIs should thoroughly review their existing data retention arrangement making reference to data protection principles of the Personal Data (Privacy) Ordinance (PDPO)[1], and update their data retention policy if necessary.
- A number of AIs have not performed more stringent background checks (e.g. verification of any previous convictions of offences) for those potential employees and contractors who need to access sensitive customer data (e.g. information security administrators, technical support staff, customer service and call centre supervisors, computer operators and printing room staff). The data protection principles set out in the PDPO[2] and Section 73(1)(b) of the Banking Ordinance are relevant references in this regard. AIs should therefore consider enhancing their pre-employment screening procedures to verify the potential employees' history of terminated employments and convictions of offences to the extent practicable (e.g. verifying through negative vetting systems either maintained internally or provided by external vendors).
- Compliance reviews (e.g. thematic audits, self-assessments, surprise checks) of the relevant statutory and regulatory requirements as well as the AI's internal security policies should be conduced on a regular basis.

Security controls over electronic data

- There is generally a lack of security policy or control for protecting sensitive customer data stored in portable computing devices (such as notebook computers, PDA and Blackberry devices) and removable storage devices (such as USB memory keys and CD-ROMs). AIs should establish adequate security policies and controls (e.g. data encryption technology) for protecting sensitive customer information maintained in these devices.
- Several AIs have not adopted data encryption for their computer tapes, particularly backup tapes, that store sensitive customer data and are required to be transported between their premises (e.g. between the production and backup data centres). This increases the risk of data leakage in case of accidental loss or theft of the tapes in transit. AIs should consider encrypting sensitive information stored in computer tapes (particularly for those required to be transported outside of their premises).
- Some AIs have not implemented appropriate security controls to prevent users from copying customer data from their computer workstations into removable storage devices such as USB memory keys and CD-ROMs. Some of these workstations also have Internet connection for web browsing. Sensitive customer data can therefore be easily transferred to external parties through users' Internet email account. AIs should consider implementing controls, where applicable, to remove the "copy" or "downloading" facilities in all computer workstations, and to disable floppy drives, USB

ports on, and Internet access of, computer workstations that have access to customer data.

- Audit logs of customer data access activities, such as data retrieval and downloading, should be developed for regular reviews to identify any irregularities (such as unauthorised access and transfer of customer data).

Security controls over hardcopy documents

- A number of AIs have not developed guidelines and procedures to provide staff and service providers (e.g. credit card promoters) with guidance for handling sensitive hardcopy documents (such as photocopies of customers' HKID card and income proof) outside the bank premises. For instance, some AIs allow staff to keep sensitive customer information at home without proper protection during weekends. AIs should develop adequate procedures for controlling the transportation and storage of sensitive hardcopy documents (e.g. delivering all customer documents securely under supervision of authorised personnel to a nearby office/branch of the AIs immediately after collection).
- Several AIs have insufficient surveillance controls (e.g. close-circuit TVs) in certain highly sensitive areas (e.g. statement / PIN mailers printing rooms, document scanning areas and computer tape rooms). AIs should consider installing appropriate surveillance systems at all highly sensitive areas to monitor any unauthorised activities and to capture relevant evidence for possible investigation if required.
- The confidential wastes bags are in some cases left unattended after office hours in the public office areas where external contractors (including office maintenance, cleaning workers, etc) and unauthorised staff can gain access to these confidential documents. AIs should properly secure the confidential wastes bags after office hours before these bags are transported to the wastes destruction center.

Other areas for improvement

- A number of AIs have not fully set out the contractual liabilities and obligations of their service providers in their outsourced service contracts (e.g. data input function, card embossing and statement printing services). For instance, some of the service agreements examined do not require the service providers to return and destroy all customer data when the AIs determine to terminate the contract. AIs should review and enhance their contractual agreements with their outside service providers to minimise any reputation and legal risks arising from data leakage. AIs should also make reference to the terms and conditions set out in the "Model Contract" (in accordance with Section 33(2)(f) of the PDPO) when enhancing the existing service contracts.
- Consideration should be given to arranging regular security training for all relevant employees of outside service providers to promote their awareness of and to ensure compliance with the required data security requirements.
- AIs should establish adequate incident management procedures for loss or unauthorised access of customer data. These procedures should cover incident handling and escalation procedures and arrangement for reporting to all relevant external parties (e.g. the HKMA, SFC and the affected customers).

[1]Section 26 and Schedule 1 principle 2(2) of the PDPO require that personal data shall not be kept longer than is necessary for the fulfilment of the purpose for which the data are to

be used.

[2]Schedule 1 principle 4(d) of the PDPO requires that appropriate security measures should be taken for ensuring the integrity, prudence and competence of persons who need access to the data.

Annex 2 - Good practices adopted by certain AIs

Information security policies and staff awareness

- Control procedures and baseline security requirements have been developed to safeguard application programs, operating systems, system software and databases. In addition, staff members are required to confirm in writing their awareness of the security requirements.
- Regular awareness training (e.g. briefings, posters, web-based interactive training programme) is provided to all levels of staff within the institution regarding relevant policies and guidelines on the importance of customer data protection.
- Outside service providers are required to sign properly prepared non-disclosure and confidentially statements. Confidentiality undertaking is also signed by all relevant employees of the outside service providers involved in the processing of customer data.

Controls over electronic data and hardcopy documents

- Reviews or certifications of security configurations of critical and core banking systems are conducted on a regular basis (e.g. at least yearly). Formal control procedures for the use of the privileged and super-user accounts are also established.
- Advanced technology has been adopted to allow outside service providers to access documents containing customer information in an image format through designated terminals while data still reside in the AIs' back-end computer systems. Copying and printing of customer information from the service providers' workstations are restricted.
- Appropriate encryption controls have been implemented to protect all sensitive data transmitted over external networks.
- A formal process is established to ensure that all confidential wastes (including customer documents) are shredded before they are collected by an external party for final destruction.

Audit and compliance reviews

- A designated unit is established within the institution with an overall responsibility to ensure on-going compliance with relevant statutory and regulatory requirements. In addition, self-assessments of controls over customer data protection are performed on a regular basis.
- Certain dedicated staff are assigned to monitor the activities of their outside service providers (e.g. data input processing). Spot checks are also performed at roadshow venues to ensure that the required data control procedures are appropriately followed by third-party promoters.

Last revision date : 01 August 2011