Management of Security Risks in Electronic Banking Services

A Guidance Note issued by the Monetary Authority (the "MA")

PART I: INTRODUCTION

1. Purpose

1.1 This Guidance Note is intended to provide guidance to the senior management of Authorised Institutions ("AIs") on the key principles and recommended sound practices in managing the security risks in their transactional electronic banking ("e-banking") services. In this Guidance Note, transactional e-banking services mean banking services offered primarily through the internet and/or wireless communication networks (e.g., mobile phone banking) other than the mere provision of publicly available information[1]. As AIs' dependence on information systems increases and due to the interconnections of public networks and AIs' internal networks, AIs that offer transactional e-banking services will be subject to security threats from a wide range of sources (see **Annex 1** for examples). There is thus a need to strengthen the management of security risks[2] for these institutions in general and their transactional e-banking services in particular.

1.2 It should be emphasised that this Guidance Note is not intended to prescribe uniform or all-inclusive principles and practices in managing the security risks for all kinds of transactional e-banking services. Effective management of security risks can be implemented through a variety of technologies or internal control systems appropriate to the types of services offered, which change quickly over time. The general principle is that institutions are expected to implement security arrangements that are "fit for purpose", i.e. commensurate with the risks associated with the types and amounts of transactions allowed, the electronic delivery channels adopted and the risk management systems of individual institutions. Other than the recommendations provided in this Guidance Note, institutions should also take into account other relevant industry security standards and

---

[1] Many of the principles and recommended sound practices would also be applicable to e-banking through other electronic delivery channels, such as automatic teller machines ("ATMs"), phone banking, personal computer ("PC") banking through leased lines, although these channels are in general less exposed to security threats. Moreover, AIs should take into account the principles and recommended sound practices to implement appropriate security measures for their informational websites. It is because any successful attacks on AIs' informational websites may also affect the institutions' reputation and customers' confidence in the institutions' e-banking services.

[2] Security risk is only one of the day to day operational risks confronted by an AI. This Guidance Note does not address operational risks concerning issues such as business continuity/system availability and prevention of computer viruses. The MA has however in the past issued a Guideline on Internal Control Systems under section 7(3) of the Banking Ordinance to set out some general principles on internal control systems in a computer environment, including segregation of duties, system documentation and testing, contingency planning and prevention of computer viruses.

sound practices[3] as appropriate, and keep up with the most current information security issues, for instance, by receiving relevant information from well-known security resources organisations[4].

PART II: INFORMATION SECURITY POLICIES AND PRACTICES

2. Senior management of AIs should issue and maintain comprehensive information security policies, ensure that they are properly implemented and strictly enforced, and encourage the development of a security culture in the institution.

2.1 While the adoption of appropriate technology is a necessary condition in managing the security risks in transactional e-banking services, it is not a sufficient condition to ensure security in relation to the provision of such services. One of the weakest aspects of security risk management is often the lack of comprehensive security policies or the strict enforcement of these policies, or inadequate awareness or knowledge of the security policies and procedures within the institution.

2.2 It is therefore crucial for the senior management of AIs to issue and maintain, on an ongoing basis, comprehensive information security policies relating to the use of technology in general and to transactional e-banking services in particular. The documents should set forth the policies, procedures and controls to safeguard the institutions' operations against security breaches, define individual responsibilities, and describe enforcement and disciplinary actions for non-compliance. At a minimum, information security policies should cover the following matters:

(a) Classification of levels of protection needed for different information, system and network facilities and other resources, in light of their importance and the assessment of any associated security threats;

(b) Specific security measures including procedures and controls to safeguard different information, system and network facilities and resources, and the task owners responsible for devising, implementing and reviewing the measures;

(c) Procedures and controls for detecting and recording security breaches or weaknesses, and reporting and handling of such security incidents;

---

[3] Examples of industry security standards and sound practices include: "BS(British Standards) 7799: Code of practice for information security management", "ISO/TR13569: Banking and related financial services - Information Security Guidelines".

[4] An example of security resources organisation is the SANS (System Administration, Networking, and Security) Institute - website address: www.sans.org. SANS is an international co-operative research and education organisation through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face. Some of the SANS's objectives are to help the community keep up with the most current information security issues and to help them respond to those issues by addressing them with regular up-to-date research projects and publications. Recently, SANS has published a list of the common mistakes made by end users, senior executives and IT people that may lead to security breaches. Examples of other useful websites include the Computer Emergency Response Team (CERT) - website address: www.cert.org, and Security Assurance Services for Internet-connected Companies (ICSA.net) - website address: www.icsa.net.

(d) Procedures and controls to ensure continued effectiveness and regular review of information security policies or specific security measures;

(e) Procedures and controls to ensure strict enforcement and disciplinary actions for non-compliance.

2.3 Given that the formulation, implementation and enforcement of information security policies entail co-operation between the IT function and different business units, senior management should establish effective management structures to co-ordinate such processes. For instance, an institution may assign a dedicated information security manager or unit to take overall responsibility for the development and implementation of its information security policies. Separately, the senior management should strictly enforce the policies and commission periodic audits to ensure compliance with the policies within the institution.

2.4 Apart from the issuance and maintenance of information security policies, the senior management should also promote a security culture within the institution by demonstrating their commitment to high standards of information security, and widely communicating this to all relevant staff. In particular, AIs should provide sufficient ongoing training to relevant personnel at different levels to help ensure that they have the knowledge and skills necessary to understand and effectively comply with information security policies, and keep abreast of the technological and industry advancements including the latest security threats. As attacks can originate from internal sources (e.g., disgruntled former or current employees, temporary employees, contracted staff), AIs should also incorporate adequate security controls into day to day management of all relevant internal personnel, such as during the recruitment process, performance appraisal and task assignment.

2.5 Senior management should not assume that all staff are aware of widely known bad security practices such as opening unsolicited e-mail attachments without verifying their source or installing unauthorised screen savers or games. Such common bad practices should be explicitly dealt with through the institution's security policies and procedures, and ongoing promotion of security awareness of its staff.

3. AIs should implement adequate physical security measures to prevent unauthorized physical access to the critical computer or network equipment of their e-banking services.

3.1 To prevent unauthorized physical access, damage to and interference with institutions' e-banking services and their information, AIs should house all critical or sensitive computer and network equipment (see Part III) in physically secure locations, protected by defined security barriers and entry controls. AIs should set stringent control policies on access to such locations. Nevertheless, the level of protection required should be commensurate with the risk assessment and importance related to the equipment.

3.2 In implementing physical security measures, AIs should consider the following:

(a) Security barriers (e.g., external walls, windows) and entry controls (e.g., card controlled entry gate, manned reception desk) of the secure locations should be physically sound. Doors and windows must be locked when unattended;

(b) Minimum indication of the purpose of the secure locations should be given and personnel should only be aware of the existence or details of the locations on a need to know basis;

(c) Suitable intruder detection systems should be installed and regularly tested to cover all external doors and accessible windows, etc.;

(d) All denied and authorized physical access to secure locations should be logged in audit trails and the trails should be securely maintained. Points of access and critical locations should be monitored by closed circuit television and reviewed by parties independent from those who have access to the locations;

(e) Access to cabling, junction boxes, service ducts should be physically restricted.

4. AIs should put in place adequate security measures including comprehensive contractual agreements to control the security risks arising from business counterparties and other external parties.

4.1 Given the complexity associated with the technology of transactional e-banking services, it is common that AIs need to work with different business counterparties (e.g., hardware and software vendors, consultants, telecommunication operators, internet service providers) in developing, operating or supporting their e-banking services. Some AIs may also outsource certain parts of their e-banking services to common outsourcing operators to leverage their resources and expertise. AIs should perform due diligence regularly to evaluate the ability of these parties to maintain an adequate level of security and to keep abreast of changing technology. Moreover, AIs should also ensure that the contractual agreements with these parties have clearly defined the security responsibilities of these parties such as ensuring adequate security in handling AIs' information.

4.2 AIs should also put in place adequate security measures to control security risks arising from other external parties (e.g., visitors, contractors, technicians) that may have access to the AIs' premises but are not involved in the e-banking services. In particular, AIs should safeguard against "social engineering" – i.e. a scheme using social techniques (e.g., misrepresentation by attackers as technicians) to gain access to information or an organisation's premises. (For further details, please refer to **Annex 1**). Moreover, AIs should exercise extra care in disclosing any sensitive information about the technical platforms of their networks and systems to external parties including their customers and the media.

5. AIs should provide easy-to-understand and prominent advice to their customers on security precautions in relation to their transactional e-banking services.

5.1 As with traditional banking services, customer misuse, both intentional and inadvertent, is another source of security risks. Security risks may be heightened when a customer of an institution does not know nor understand the necessary security precautions (e.g., protection of passwords) relating to the use of the transactional e-banking service. To complement AIs' own security measures, it is therefore important for AIs to provide prominent and easy-to-understand advice to their customers on the importance of security precautions (please refer to **Annex 2** for some examples of precautionary advice).

6. Senior management of AIs should commission periodic evaluations of the continued effectiveness of the information security policies and practices, as well as the system and network security relating to their transactional e-banking services.

6.1 Given the paramount importance of security risk management for transactional e-banking service and the rapid pace of technological developments, the MA expects senior management of institutions to commission periodic independent assessments of the security aspects of their e-banking services. The MA expects such independent assessments to be carried out by trusted independent experts before launch of the services, and thereafter at least once a year, or whenever there are substantial changes to the risk assessment of the services or major security breaches. In general, the MA expects that such trusted independent experts should be from the external sources (e.g., external auditors or third-party security consultants) with necessary expertise. However in some cases, it may also be acceptable for AIs' internal staff (e.g., internal auditors) or an independent unit of the vendors of the relevant e-banking systems to conduct the independent assessments provided that they can demonstrate that they have the necessary expertise to carry out such assessments. However, they must be independent from those parties that develop, implement or operate the services.

6.2 The MA expects each independent assessment to evaluate the information security policies, internal controls and procedures, as well as system and network security, taking into account the recommendations in this Guidance Note, the latest technological developments and security threats, and industry standards and sound practices. AIs should make an assessment of the particular risks attached to the e-banking service in question in determining the extent of reviews and level of assurance expected from each independent assessment. For institutions offering e-banking services of higher risk (e.g., services that allow large value fund transfer to non-registered third-parties), they should consider to include in their independent assessments penetration testing[5] having regard to different types of online attacks. In between such independent assessments, AIs should evaluate the effectiveness of their security arrangements on an ongoing basis, and regularly make use of scanning tools[6] to scan for security weaknesses in their networks and systems. If an institution's e-banking services are provided by an outside vendor or service provider, management should ensure that the vendor or service provider will perform adequate independent assessments, provide management with the results of such assessments and regularly evaluate the adequacy of its security arrangements in between the assessments.

7. AIs should implement adequate measures to detect and record security breaches or weaknesses on an ongoing basis, and put in place procedures to report and handle such security incidents.

7.1 To detect and discourage unauthorised access to AIs' systems and networks, AIs should ensure that adequate audit logs are produced at critical control points (e.g., at web servers and firewalls) to record details of accesses to and activities of their networks and systems. The audit logs should be protected against unauthorised manipulation and

---

[5] Penetration testing is the process of identifying, isolating, and confirming possible flaws in the design and implementation of passwords, firewalls, encryption and other security controls by simulating the probable actions of attackers. .

[6] Scanning tools are commercially available tools that could be used for identifying and analysing security vulnerabilities in network, operating systems and database.

retained for a period of at least six months to facilitate any dispute resolution and fraud investigation if necessary. To ensure the completeness and accuracy of audit logs, particular attention should be paid to the security of the logging facilities and the correct settings of the relevant computer clocks that would affect the time-stamp recorded in the logs.

7.2 AI should proactively monitor these audit logs and their networks and systems on an ongoing basis to detect any unusual transactions, patterns of anomalous activities and suspected intrusions, taking into account factors such as reasonableness of the transactions performed by their customers. AIs should assign designated personnel with adequate expertise to review the logs and there should be segregation of duties between such personnel and those whose activities are being monitored. AIs should also consider the need to make use of intrusion detection systems ("IDSs") to automate the process so that the audit logs can also be monitored continuously by the IDSs.

7.3 AIs should establish procedures for timely reporting and handling of suspected or actual security breaches or weaknesses. AIs should also put in place arrangements that allow them to solicit timely technical advice from internal or external experts whenever necessary. If a security breach occurs that may result in reputational damage or material financial loss, reports should be made promptly to senior management and the MA on the cause and extent of the breach.

PART III: SYSTEM AND NETWORK SECURITY

8. AIs should implement adequate security measures for their internal networks and network connections to public network or remote parties.

8.1 The security of an institution's internal networks and their external connections is a major component of security risk management because the security weaknesses of an organisation's network or its external connections could allow successful online attacks. For instance, online attacks using "random dialling" techniques could gain unauthorized access to an organisation's internal networks through modems that are connected to the networks without proper authorization or adequate security protection. The attackers would identify and exploit any such modems by sequentially or randomly dialling every number on a known telephone exchange. For further details, please refer to **Annex 1**. Network security is particularly crucial for AIs' offering transactional e-banking service because their internal systems and database need to be connected to external parties or the internet.

8.2 The following provides AIs with some recommended practices for implementing network security:

(a) AIs should centralise all critical network devices and network connection points (including all firewall components and those devices used to manage them) in secure locations to enhance physical access control and facilitate maintenance;

(b) AIs should segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. For instance, the production systems should be located in dedicated network segments separated from other segments so that production network traffic would

be segregated from other traffic. Data traffic between different network segments should be properly controlled. In particular, communication between network management stations and network equipment (e.g., routers and firewalls) should be encrypted to protect administrative traffic (e.g., network commands for managing routers) from being tampered with;

(c) All terminals connected to internal networks should be able to access authorized data or network services only, and the network routes for such access should be properly controlled;

(d) User terminals should be disconnected from the network after a period of inactivity. AIs should identify any unusual network connections such as those established during odd hours (e.g., at night);

(e) Any remote access to the internal network should be subject to strong authentication and controls, and confined to authorized users or parties only. Moreover, AIs should properly monitor and control the network traffic between internal and external networks;

(f) Authorisation should be needed for any modems connected to the internal network or devices on the network. In particular, AIs should prohibit any unauthorized use of modem and remote control software that may open up a security loophole in the internal networks (e.g., subject to attack through "random dialling" as mentioned above).

9. AIs should properly design and configure the servers and firewalls that support and protect their transactional e-banking services particularly internet-based e-banking services.

9.1 In offering transactional e-banking services, AIs need to install certain servers to relay the messages received from the electronic channels to their internal systems for processing, and vice versa. In addition, AIs should install firewalls (see below) to screen and monitor the messages transmitted between their internal networks and external networks in particular the internet. If these servers or firewalls are not properly designed or configured, they will be vulnerable to security attacks leading to significant risk of unauthorized access to AIs' internal systems or databases.

9.2 The following provides AIs with some recommended practices for the design and configuration of such servers and firewalls. While the following recommended practices are more relevant to internet-based e-banking services, many of these practices and principles may also be applicable to e-banking services delivered through wireless communication networks particularly if the Wireless Application Protocol (WAP) technology is used.

Web servers

Web servers are computers dedicated to connect with the internet and provide information for access from anywhere on the internet. In certain types of implementation, web servers would also handle the front-end processing of the internet-based e-banking system, such as validation of data entered by customers or responding to customers. Given the exposure of web servers to attacks from

any user via the internet, it is important for AIs to implement adequate security controls for web servers. For instance,

(a) No confidential data should be stored in web servers. Confidential data should be stored in separate database servers (see below) or AIs' internal systems. This would protect the data even if an attacker were able to gain control of the web servers;

(b) As there are different types of system development tools (including scripting languages that define the commands to be executed) that can be used for developing internet application programs, AIs should evaluate the security features that can be provided by different tools to ensure adequate security protection when they select the tools. Moreover, application programs residing at web servers should be carefully designed and developed because improper design or implementation of application programs on web servers is one of the common reasons for successful penetration of web servers. For instance, programs should be designed in such a way that even if these programs were to be subverted by an attacker, the attacker would not be able to initiate other system functions to gain unauthorized access or cause undue damage to the system or data.

Database servers

Confidential data should be stored in separate database servers or AIs' internal systems or databases. Moreover, the database package should provide adequate database level security for storing and retrieving data. For instance, the database programs should have access control mechanisms to allow users to access only certain sets of data (e.g., data fields or tables) in the database for which they are authorised. In addition, the storage of sensitive data in the database should be encrypted.

Firewalls

Firewalls are devices (with hardware and software) that block unwanted communications into and out of AIs' internal networks, while allowing acceptable communications to pass. Firewalls can examine the pieces or packets of data flowing into and out of a network segment and determine whether that piece of data should be given access into the network segment. Despite these general features of firewalls, installation of firewalls does not necessarily provide adequate protection against unauthorized access to AIs' internal systems or networks unless the firewalls are properly chosen, configured and installed. For instance,

(a) There should be "external firewall(s)" to control the traffic between the internet and the web servers so that only acceptable communication methods for connecting to the web servers would be allowed as attackers may exploit certain communication methods to pose threats to the web servers[7]. Moreover, AIs should consider the need to install another tier of "internal firewall(s)" to control the traffic between the web servers and the

[7] For instance, "Telnet" is a communication method that allows remote users to sign on to web servers (other than through browsers), thereby raising the risk of these users seizing control of the web servers.

database servers or AIs' internal systems, so that only the allowed types of traffic can pass through from the web servers to the database servers or AIs' internal systems. These "internal firewall(s)" may also further prevent unauthorised access to the database servers or AIs' internal systems through AIs' internal networks. In addition, if two or more tiers of firewalls are used, AIs should consider using firewalls of different types to prevent similar security vulnerabilities from being exploited in different firewalls;

(b) AIs should carefully select the firewall(s) to be installed having regard to their functions. The security level of a firewall is generally determined by the nature of checking that it would perform on data flowing through it. For instance, some firewalls have "stateful inspection" function[8], where the firewalls can thoroughly inspect all packets of information. It is relevant to note that from time to time, some organisations conduct testing on the functionality and security features of certain firewalls and publish the results of the testing. AIs may wish to take into account such testing results before they determine the firewall(s) to be installed;

(c) The effectiveness of firewalls as a security tool is heavily dependent upon how the firewall is configured and the policies in place in respect of its configuration and maintenance. Firewalls can perform the guardian role only if they are properly configured and maintained. Most successful firewall penetrations are due to improper configuration of the firewalls. Because firewall design and implementation can be complex, the parameters of the rules under which firewalls operate should be simplified as much as possible to make validation and maintenance easier. It is also important that AIs should formulate and document formal policies for the configuration, monitoring and maintenance of their firewalls, so that all changes to the configuration are properly controlled and tracked;

(d) As security threats or weaknesses are evolving, AIs should perform frequent reviews and timely updates of the firewall configurations to enhance protection from newly identified vulnerabilities and system weaknesses. Given the complexity involved in this process, it is important for AIs to carefully select vendors of firewalls who are able to keep abreast of the latest technology developments including the improvements needed in the firewalls to protect from the latest attack techniques;

(e) Network traffic for firewall administration should be confined within a system administration segment of AIs' internal networks, which is separated from the network segment connected to the production systems, so that the production network and systems would not be affected by the firewall administration activities.

---

[8] The "stateful inspection" firewalls establish databases of the "state" of each message in a dialog. This allows the "stateful inspection" firewalls to recognise inappropriate responses by a server to messages or inquiries, and to terminate the connection accordingly.

Security measures that are applicable to servers and firewalls

(a) Any unused programs and computer processes of the servers and firewalls should be deactivated or removed, and the latest security patches and updates should be applied as appropriate to the systems. This is because attackers may exploit the weaknesses of those programs and processes to gain unauthorized access to the systems. AIs should regularly monitor any potential security vulnerabilities of the hardware or software of the servers and firewalls reported by the vendors so that corrective actions can be taken accordingly;

(b) Access rights of the user accounts (e.g., to what extent the data or programs can be accessed, modified or controlled by the user accounts) of the servers and firewalls should be carefully designed. Only the minimum number of user accounts that are necessary for the operation of the systems should be maintained. In particular, default accounts, which are those accounts that are originally incorporated in the systems, should be deactivated or their default passwords should be changed in order to minimise the risk of password attack (for more details, please refer to **Annex 1**). In addition, all access to the servers and firewalls using privileged user accounts (e.g., system administrator or "super user") should be tightly controlled and recorded explicitly. For example, logins from these user accounts should be restricted only from physically secure terminals. Moreover, access rights and functions of these user accounts should also be segregated so that no single user account will have access to and control over all aspects of the systems; and

(c) The programs and other information kept in the servers and firewalls should be updated only by strongly authenticated user accounts. They should also be subject to stringent change control procedures. For instance, any changes to the programs in production systems should be properly approved by designated persons as defined in the institution's security policy and implemented by authorised users. In addition, periodic integrity checks on the programs and static data kept in the systems should be conducted to validate that they have not been altered.

(d) Problems are often dealt with by quick fixes in the interests of time. AIs should ensure that such fixes are adequately followed through so that effective long-term solutions to the associated problems are implemented.

10. AIs should implement proper techniques to protect confidentiality of information while it is stored or in passage over external and internal networks.

10.1 Transactional e-banking services entail transmission of sensitive information (e.g., customer passwords) over the internet or wireless communication networks and AIs' internal networks. AIs should therefore implement proper techniques to maintain secrecy of sensitive data while they are in passage over external and internal networks. Of course, secrecy of sensitive data should also be maintained when they are stored.

10.2 The following provides AIs with some recommended practices on these matters:

Encryption technology

Encryption technology can be used to protect the confidentiality of data by transforming the data into an unreadable format. The strength of an encryption technology typically depends on the cryptographic algorithm adopted and the length of the cryptographic key(s) used in encryption. No encryption is perfectly safe. Therefore, AIs should choose encryption technologies that are appropriate to the sensitivity and importance of data and the extent of protection needed. AIs are recommended to choose encryption technologies that make use of internationally recognised cryptographic algorithms where the strengths of the algorithms have been subjected to extensive tests.

It should be noted that certain encryption technologies will only protect data transmitted between the customers' devices (e.g., personal computers) and web servers over the internet, thereby exposing the data to security risks between the web servers and AIs' internal systems. The MA however expects that sensitive data should also be encrypted while they are transmitted between the web servers and AIs' internal systems. In particular, AIs should consider the need to apply strong "end-to-end" encryption to the transmission of highly sensitive data (e.g., customer passwords) so that the data are encrypted all the way between customers' devices and institution's internal systems for processing the data. This would help to ensure that such highly sensitive data would not be compromised even if AIs' web servers or internal networks were to be penetrated. However, if the technology selected by AIs does not allow "end-to-end" encryption and there is a decryption process at some point between the customers' devices and institution's internal systems, AIs should take appropriate measures[9] to protect the sensitive information.

Management of cryptographic keys

To ensure the effectiveness of the encryption technologies adopted, AIs should implement sound key management practices to safeguard the associated cryptographic keys, especially if the maintenance or distribution of the keys entails the involvement of external parties (e.g., mobile network operators, outsourcing service providers, certification authorities). Cryptographic keys should be generated in a secure environment under proper authorization and should be changed periodically and revoked as soon as practicable if they are considered to have been compromised. Consideration should also be given to employing tamper resistance devices[10] to protect the keys so that any attempt at tampering with cryptographic hardware would result in the device being locked and the device's keys being wiped. Moreover, cryptographic keys should not be shared for

[9] One of the possible measures is that any cryptographic process (e.g., decryption) should be performed in a secure device such as tamper resistance devices (see footnote 10).

[10] Tamper resistance devices possess specialised features and functions which can detect or prevent unauthorised modification or tampering. For example, unauthorized retrieval of sensitive data such as cryptographic keys stored in such devices will result in physical and noticeable damage to the devices.

different applications to prevent multiple security failures of different applications as a result of compromise of one set of cryptographic keys.

11. AIs should implement proper techniques to authenticate the identity and authority of their customers and their e-banking systems, and to ensure the integrity of information transmitted over networks.

11.1 AIs should select reliable and accurate authentication techniques to validate the identity and authority of their customers, on the basis of the risk assessments of their customers and the services offered. While customer authentication can be achieved by any one of the following methods: (i) something a customer knows (e.g., passwords); (ii) something a customer has (e.g., digital certificates, smart cards or security token); (iii) something a customer is (e.g., fingerprints), stronger customer authentication combines at least two of the above methods.

11.2 Institutions using only customer IDs (e.g., account numbers) and passwords to authenticate their customers should implement adequate measures to protect their customers' passwords (please refer to **Annex 3** for some recommended sound practices). Institutions should also put in place other necessary controls to mitigate the damage due to any false authentication. Examples of such controls include: establishing different passwords for login and funds transfer respectively, mandating pre-registration of accounts to which funds can be transferred, and establishing limits on amount of transactions. In general, the MA expects AIs to employ stronger authentication techniques for authenticating their customers' transactions with higher risk, e.g., when large-value funds transfer to unregistered accounts is allowed. Regardless of the authentication techniques adopted, AIs should regularly review the adequacy of the authentication techniques in light of latest technological and industry development.

11.3 In addition to customer authentication, AIs should also implement appropriate measures for the customers to validate the identity and genuineness of AIs' web sites for accessing internet-based e-banking service. For instance, in the implementation of certain encryption technologies, an AI could implement its e-banking system such that its web server is installed with a digital certificate[11] to authenticate that the web server belongs to the institution. The institution could advise its customers to make use of certain functions of the customers' browsers to examine the digital certificate of the web site being accessed by the customers to validate that it is a genuine web site of the institution.

11.4 AIs should also implement adequate measures to safeguard the accuracy and completeness of information transmitted over external and internal networks to help ensure legal enforceability of banking transactions conducted via their e-banking services. For instance, public key cryptography[11] is one of the techniques that can be used to ensure authentication, confidentiality as well as integrity of information being transmitted. It allows the recipient of a message to authenticate the sending party, and also check that the contents of the message have not been modified in any manner. To promote the use of public key cryptography in the community at large, the Government has taken a number of initiatives to establish a local public key infrastructure. In particular, the Electronic Transactions Ordinance provides for a voluntary recognition regime for Certificate Authorities ("CAs") and stipulates that Hongkong Post is a recognised CA. Hongkong Post has already started to provide CA services to the public. The Electronic Transactions

[11] Please refer to the MA's circular of 25 November 1997 for further details.

Ordinance also stipulates the conditions under which electronic records and digital signatures used in electronic transactions will be given the same legal status as that of their paper-based counterparts. There is thus a more favourable environment for the use of public key cryptography in Hong Kong.

Monetary Authority
July 2000

Annex 1

Examples of common types of online attacks and possible preventive and detective measures

Different types of attackers (e.g., serious hackers, interested computer novices, dishonest vendors, disgruntled current or former employees) could pose a potential threat to an institution's information security. The internet provides different sources of information on known security flaws in hardware and software. Using almost any search engine on the internet, average internet users can quickly find information describing how to break into various systems by exploiting known security weaknesses. Attackers may also breach security by using automated tools to probe network systems, then exploiting any identified security weaknesses to gain unauthorized access to the network. Apart from attacks originated from external parties, many break-ins occur due to poor information security policies and procedures, or internal misuse of information systems. Also, new security risks could arise from evolving attack methods or newly detected holes and bugs in existing software and hardware.

AIs should therefore stay abreast of new security threats and vulnerabilities, and the latest security patches and version upgrades that are available to fix security flaws and bugs. The following table summarises for AIs' reference some common examples of online attacks and the possible preventive and detection measures to guard against these attacks.

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
Back doors	Back doors are also known as trap doors. These are pieces of program code written into applications or operating systems to grant programmers access to programs without the need to go through the normal security controls. The back door can either recognise some special sequence of input, or is triggered by being run from a certain user ID which is then granted special access rights accordingly. Programmers typically use back doors to achieve faster access to facilitate debugging or monitoring of the programs that they are developing.	• Obtain certification from vendors that the products contain no undocumented back doors and accept systems only from trusted sources; • Put in place stringent system development and change control procedures such that systems can normally be put into production use only after thorough testing to confirm that no back doors have been included in the systems; • Regular integrity checks on programs used in production to ensure that the programs have not been altered.

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
	Back doors become a problem when the programmer forgets to remove a back door after debugging. Further, an attacker can create a back door for his future access after gaining access to an account (see "Brute force" attack).	
Brute force	Brute force attack is a technique to capture encrypted messages, and then use software to break the code and gain access to messages, user IDs, or passwords. If the attacker gains access to a user ID that has sufficient privileges, he can create a back door (see above) for future access, even if the password of the user ID is subsequently changed.	• Deploy strong encryption technology and effective key management practices to protect confidentiality of messages, user IDs and passwords; • Enforce sound password policies (e.g., mandating minimum length of passwords, or periodic changes in passwords); • Perform penetration testing to identify vulnerability to unauthorized interception and assess the strength of encryption; • Provide adequate education to customers on security precautions (particularly on setting passwords).
Denial of service[1]	Denial of service ("DoS") is an attack that is not targeted at gaining access to a network or system. Instead, it aims at disrupting the service of the network or system under attack by flooding it with more information or service requests than it can handle.	• Implement adequate network security to block unnecessary network traffic to the systems; • Arrange with internet service providers ("ISPs") to accept traffic from authorized sources only;

[1] Although the direct impact of "Denial of service" attacks may be disruptions to services, rather than immediate security breaches, their occurrence may affect the working of certain security measures and hence increase the probability of security breaches.

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
	DoS attack can be initiated at one or multiple sources. In a distributed denial of service ("DDoS") attack, a single attacker deliberately introduces DoS attack programs into dozens or even hundreds of other systems by various techniques of online attack. The attacker then simultaneously initiates all those DoS attack programs to bombard the target network or system.	• Prepare adequate standby system capacity; • Put in place adequate backup and recovery arrangements; • Use scanning tools[2] or perform penetration testing to assess the ability of the network and system to withstand DoS or DDoS attacks.
Exploiting known security vulnerabilities	Attackers may exploit known security flaws to gain unauthorized access to a particular system. The internet provides various sources of such information. Alternatively, attackers may make use of automated tools to probe particular systems to identify security weaknesses. Security vulnerabilities can be related to the hardware or software of web servers, firewalls or development tools used for developing applications of web servers. For instance, certain security vulnerabilities would allow intruders to modify the content of web pages.	• Remove or disable any unused programs and computer processes of the servers and firewalls; • Apply the latest security patches and updates to the operating systems and applications of the systems; • Select hardware and software vendors who are able to keep abreast of the latest technology developments to protect from the latest attack techniques; • Use scanning tools or perform penetration testing to identify known security vulnerabilities such as program bugs or protocol flaws.

[2] Scanning tools are commercially available tools that can be used for identifying and analysing security vulnerabilities in network, operating systems and database.

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
Guessing passwords	Guessing passwords is a technique using software to test all possible combinations to gain entry into a system or network. Some attacks speed up this process by trying commonly used combinations first (e.g., words in dictionaries).	• Enforce sound password policies (e.g., mandating minimum length of passwords, or periodic changes in passwords); • Enforce stringent access controls (e.g. disable user IDs after multiple unsuccessful logon attempts); • Meticulously change all default passwords on critical network components; • Provide adequate guidance to customers on security precautions (particularly on setting passwords).
Hijacking	Hijacking is an attack in which a connection is stolen after a victim has authenticated himself or herself to the system. Hijacking attacks generally take place on a remote computer (e.g., a customer's personal computer), although it is sometimes possible to hijack a connection from a computer on the route between the remote computer and the banks' internal systems. The victim may be aware that the connection is affected.	• Implement adequate network security to ensure strong authentication techniques for remote access, e.g. require periodic re-authentication for the continuation of highly sensitive sessions to limit hijacker's access to sensitive information; • Install properly configured firewalls at appropriate locations; • Perform monitoring of network traffic or potential intrusions on an ongoing basis; • Use scanning tools or perform penetration testing to identify vulnerability to hijacking attacks; • Deploy strong end-to-end encryption of highly sensitive data (as a mitigation measure).

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
Random dialling or war dialling	Random dialling or war dialling is a technique where an attacker sequentially or randomly dials every number on a known telephone exchange with the objective of detecting modems that bypass network firewalls and other security measures so that the attacker can gain access to the networks through the modems.	• Implement adequate network security to ensure that all modems have been authorized and controlled, e.g. periodically "war dial" all the numbers on the institution's telephone exchange to detect unauthorized modems; • Centralise all modems in physically secure locations and separate the network segment connected to the modems from other important segments of the internal network so that even if attackers can gain unauthorized access to the internal networks through the modems, they would not be able to access other critical network segments; • Configure the modems or other similar devices in a "dial-back" mode such that remote network connections through these modems can be initiated only from the modems to pre-approved remote parties but not the other way round; • Use scanning tools or perform penetration testing to identify vulnerability to war dialling risk.
Sniffers	Sniffers, also known as network monitors, are software used to capture keystrokes from a particular PC, or are similar to a wiretap device that plugs into computer networks to eavesdrop and intercept information in transit over networks.	• Implement adequate network security to prevent unauthorized interception of messages (e.g. separate internal networks into segments so that dissemination of sensitive data is restricted to a controlled subset of users by

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
		using firewalls or routers etc.); • Perform monitoring of network traffic or potential intrusions on an ongoing basis; • Use scanning tools or perform penetration testing to identify vulnerability to interception of messages transmitted over networks; • Provide adequate guidance to customers on security precautions (particularly on avoiding loading sniffers into their devices); • Deploy strong end-to-end encryption of highly sensitive data and strong authentication techniques (as mitigation measures).
Social engineering	Social engineering is a scheme using social techniques to attempt to gain information or access. An attacker may claim to be someone authorized to access the system such as a help desk technician, vendor or contractor and attempt to get the victim to reveal his user ID or passwords, or even request the set up of a new account for the attacker himself. An attacker may also call the organisation's help desk impersonating an authorized user to gain information about the system (e.g. requesting the help desk to change the original system password to one designated by the attacker).	• Put in place adequate security measures against unauthorized access from external parties; • Train relevant personnel such as helpdesk technicians to be alert about social engineering techniques and provide them with firm policies to follow regarding providing information that could result in unauthorized access to confidential information; • Provide adequate guidance to customers on security precautions to safeguard against "social engineering".

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
Spoofing	Spoofing aims at deceiving the network so that it recognises an unauthorized desktop system as if it were an authorized desktop system to gain access to networks and/or sensitive data. For example, while a victim's device (e.g., a personal computer) is communicating with an organisation's web site within an authenticated session after the victim has properly entered his user ID and password, an attacker may intercept the transmissions, obtain the Internet Protocol ("IP") address of the victim's device and use the same IP address to impersonate the victim in an attempt to gain access to that system. In this case, the victim may not be aware of this attack as his connection is not affected.	• Implement strong authentication techniques for authenticating messages transmitted within an authenticated session, which are based on not only the IP address but also on an encrypted identity that is unique to the session; • Install properly configured firewalls at appropriate locations; • Perform monitoring of network traffic or potential intrusions on an ongoing basis.
Trojan horses	Trojan horses are programs that contain additional (hidden) functions that usually allow malicious or unintended activities such as gathering information or performing surreptitious acts to gain control of the system, without any disruption to normal transactions. Trojan horses can be attached to e-mails (e.g., as a computer game) and may create a back door (see above) that allows unrestricted access to a system. The programs may automatically exclude logging and other information that would allow the intruder to be traced. One of the oldest forms of Trojan horse is	• Put in place stringent system development and change control procedures such that systems can normally be put into production only after thorough testing to confirm that no trojan horses have been introduced to the systems; • Regular integrity checks on programs used in production; • Formulate information security policies and provide adequate training to internal personnel on relevant security precautions to safeguard against trojan horses (e.g., stringent policy against improper use of internet or e-mail);

Types of online attacks	Brief description of attacks	Examples of possible preventive and detection measures
	software that displays a fake login screen of a system to capture the user IDs and passwords entered by users.	• Provide adequate guidance to customers on security precautions such as in opening e-mail attachments and in use of internet.
Viruses[3]	Computer viruses are computer programs that may be embedded in other code and can self-replicate. Once active, they may carry out unwanted and unexpected actions that can result in destructive outcomes in network or systems. The virus program may also move into multiple platforms, data files, or devices on a system and spread through multiple systems in a network. Virus programs may be contained in an e-mail attachment and become active when the attachment is opened.	• Obtain certification from vendors that products are virus-free; • Use updated virus scanning tools; • Formulate information security policies and provide adequate training to internal personnel on relevant security precautions to safeguard against computer viruses (e.g., stringent policy against improper use of internet or e-mail); • Provide adequate guidance to customers on security precautions such as in opening e-mail attachments and in use of internet.

[3] Although the direct impact of computer viruses may be disruptions to services or loss of data, rather than immediate security breaches, their occurrence may affect the working of certain security measures and hence increase the probability of security breaches.

Annex 2

Examples of advice on security precautions

This Annex provides AIs with some examples of possible advice on security precautions that could be given to their customers. Please note that some of the following good security practices are also applicable to AIs' internal personnel

a) Customers should not disclose their customer IDs (e.g., account numbers) or passwords to anyone else. In particular, they should destroy the original printed copy of the password and they should not write down or record the IDs/password without disguising it;

b) AIs should provide specific guidance to their customers on the types of passwords that should not be used, such as any particular names or dates, and previously chosen passwords. Customers should be advised to use passwords that may be difficult to guess and could not be found in the dictionary;

c) Customers should be advised to change their initial passwords when they first access the system;

d) AIs should advise their customers to periodically change their passwords (say every 60 days), and prevent their customers from reusing. Customers should also notify AIs as soon as practicable if they think that the passwords have been compromised;

e) Customers should not leave their e-banking devices (e.g., computers or mobile phones) unattended if they are in the middle of a session;

f) Once the customers have finished using the e-banking service, they should promptly log out from the service;

g) If the computer used to access e-banking services is likely to be shared with others, customers should exercise care in using their e-banking devices. For instance, AIs could advise their customers to remove the temporary files[1] stored in the memory or in the hard disks of the customers' personal computers during usage of e-banking services, as the temporary files may contain sensitive information of the customers such as account numbers;

h) AIs should provide guidance to customers to help avoid any unauthorized capturing of customer passwords by attackers. For instance, customers may be advised to exercise extra care in handling doubtful e-mails received or accessing suspicious websites because attackers may make use of these channels to secretly install

[1] Depending on the browser software used by the customers, it may be possible to remove the temporary files by specifying certain parameters of the browser.

"sniffers"[2] in the customers' devices to capture customers' keystrokes about the passwords;

i) AIs should provide guidance to customers as to what types and versions of web browsers should be installed, and specify the security requirements that the security settings of their customers' browsers should meet. For instance, AIs should remind customers to install the appropriate version of their web browsers or apply the appropriate related patches to avoid known security loopholes.

j) AIs should provide guidance to customers to safeguard against attack using "social engineering" techniques (see **Annex 1** for further details). For instance, guidance should be given to customers to avoid any disclosure of their passwords to attackers impersonating the institution's staff; and

k) Customers should regularly check their account balances and statements to identify unusual transactions.

[2] Sniffers are programs that monitor and record all information sent over the networks

Annex 3

Examples of institutional practices to protect customer passwords

Given the importance and sensitivity of customer passwords and that some online attacks (e.g., brute force, guessing passwords) might attempt to crack or intercept customers' passwords, it is important that AIs should implement adequate measures to protect the passwords of their customers. This is particularly important for AIs using only customer IDs (e.g., account numbers) and passwords to authenticate their customers.

This Annex provides AIs with some recommended sound practices for protecting the passwords of their customers. Please note that some recommendations may also be applicable to safeguarding the passwords of AIs' internal personnel.

(a) AIs should implement their systems to set minimum length for customers' passwords and consider the need to restrict the format of passwords to combinations including both numeric and alphabetic characters. These measures would increase the difficulty of guessing or cracking the passwords;

(b) AIs should consider the need for their systems to mandate or remind their customers to periodically change their passwords, and prevent their customers from reusing previously used passwords;

(c) The customer should be suspended, pending administrator intervention, after a defined number of incorrect attempts at login. Such suspensions should be recorded and reviewed in a timely manner;

(d) AIs should issue to customers their customer IDs and passwords separately so that it would be difficult for any other third parties to associate the passwords with the customer IDs. AIs should also develop procedures to validate that the customers have received the customer IDs and passwords before these can be used for accessing the systems; and

(e) While passwords entered by customers should not be displayed in the login screen, some application development tools may allow automatic memorisation of the last customer IDs and passwords entered in the login screen so that the users can easily log into the systems. AIs should not implement or allow such features.