

IT OUTSOURCING SECURITY

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Introduction.....	3
II. Managing IT Outsourcing.....	5
IT Outsourcing Risks	5
IT Outsourcing Management	6
On-going Monitoring	7
Other Best Practices	9
III. Conclusion.....	11

SUMMARY

When any IT operation of an organisation is contracted out, the external service provider (or the outsourcing vendor) may effectively become an “insider”, handling sensitive and important information for the company. While the services provided by an outsourcing vendor may be beneficial and cost-effective, proper security management processes and procedures must be in place to protect sensitive data and customer privacy in outsourced IT projects or service. Data owners need to monitor and review all access rights granted to outsourcing vendors so as to protect key data at all times. The bottom line is; an organisation can outsource its operations, but not its responsibilities.

I. INTRODUCTION

Organisations face the challenge of meeting the ever-increasing demands of customers and the marketplace with limited resources. Many have turned to outsourcing as one of their key organisational strategies. IT outsourcing refers to the contracting out of IT services or functions, which have previously been carried out by internal staff. This paper will address some of the risks involved with outsourcing information systems to third party service provider(s).

There are two driving forces when an organisation considers the option of outsourcing. One is the availability for specialists in external service providers to provide a more efficient and effective service than is possible within the organisation, and the other is the possibility of cost savings. By outsourcing non-core functions and processes, an organisation can devote more of its key resources to core business activities.

IT Outsourcing can cover a range of different services including application development and maintenance, network management, desktop management, IT helpdesk services and computer data centre management. IT Outsourcing can also be engaged on different scales, such as on a project basis or on a department-wide basis¹.

There have been reports of the leakage of sensitive or personal information around the world in recent years. These have imposed significant financial loss and damage of reputation on the organisations concerned. Apart from realising the tangible and intangible benefits to be gained through IT outsourcing, organisations need to become

¹ http://www.info.gov.hk/digital21/eng/sme/sme_intro.html

more wary of an outsourcing vendor's security procedures for the protection of sensitive and personal information².

² http://www.lawyersweekly.com.au/articles/Outsourcing-the-poisoned-chalice_z69057.htm

II. MANAGING IT OUTSOURCING

IT OUTSOURCING RISKS

When a third party service vendor starts providing an outsourcing service, the vendor may be given access to internal information which can pose certain risks to the organisation:

1. the provider gains intimate knowledge of the people, IT infrastructure, procedures, approval channels, and even the weaknesses and limitations of systems (including both IT and non-IT systems) currently in place;
2. the provider may be processing and handling critical information, systems and assets, and hence have access to sensitive or personal information;
3. the provider may have valid user IDs and passwords with authorisation to access certain highly sensitive systems logically and/or physically.

Attackers and those with criminal intent may try to get hold of this internal operation information and use it for malicious social engineering activities. Together with the rapid advancement in technology such as email and the Internet, removable storage devices (e.g. small USB flash drives), and easy remote access to the organisation's information system, the risks associated with misuse of the system and data theft (including intellectual property theft) due to insider infiltration cannot be underestimated. In fact, untimely termination of systems accounts and revocation of access rights to staff who are leaving the organisation may introduce security loopholes. In the worst case, if the systems in place do not provide for accountability and proper logging procedures, fraud as well as data security and breaches of privacy can occur without any trace being left behind.

IT OUTSOURCING MANAGEMENT

When an information system is outsourced to one or more third party service providers, proper security management processes must be in place to protect data, as well as to mitigate any security risks associated with the outsourced IT project and/or service. The following areas should be considered:

1. When preparing an outsourcing service contract, the organisation should clearly define the security requirements of the information systems to be outsourced, such as how all personal and sensitive data should be handled throughout the contract. These requirements should form the basis of the tendering process and become an integral part of the performance metrics.
2. The outsourcing contract should include requirements for all staff of third party service providers and vendors to sign non-disclosure agreements to protect sensitive data in the systems. The contract should also include a set of service level agreements (SLAs). SLAs are used to define the expected performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. In addition to defining SLAs, the contract should include an escalation process for problem resolution and incident response, so that incidents can be handled according to a pre-defined process to minimise any impact on the organisation.
3. When engaging IT service providers, an organisation should ensure that the vendor employs adequate security controls in accordance with their own organisational IT security policies, wider regulatory requirements (such as requirements from the Hong Kong Monetary Authority for the banking sector) or other industry best practices. Service providers should be subject to

the same information security requirements and have the same information security responsibilities as those specified for internal staff.

4. The security control compliance of service providers and users should be monitored and reviewed actively and periodically. The organisation must reserve the right to audit responsibilities defined in the service level agreement, and have those audits carried out by an independent third party.
5. The organisation should ensure the adequacy of contingency plans and back-up processes provided by the service provider.
6. The security roles and responsibilities of the service provider, internal staff and end-users pertaining to the outsourced information system should be clearly defined and documented.
7. It is essential to ensure that all data to be handled by the outsourcing party are clearly and properly classified, and security privileges for access should only be assigned on an as-needed basis for the performance of their work or the discharging of contractual obligations.
8. Although an information system can be outsourced, the overall responsibility and liability of any breach to sensitive or personal data remains entirely with the organisation.

ON-GOING MONITORING

The business environment is dynamic and ever-changing, and so is technology. The technology used for security controls, as well as for controlling roles and responsibilities might change over time. Regular reviews of the security operation and corresponding access controls should be conducted. Before an outsourcing contract begins, it is possible that a service provider might have overlooked some of details in the outsourcing

operation. A regular review provides a channel for both parties to evaluate the service and make adjustments as necessary.

Security best practices, including the timely update of virus signatures, detection and repair engines, proper implementation of security patches for operating systems and applications, and enforcement of password policies should be maintained at all times. On certain occasions, access to privileged accounts such as the *Administrator* account in Windows servers or *root* in UNIX systems, might have to be granted to third party service providers. The use and activities carried out with these privileged accounts should be monitored, logged and reviewed periodically and compared against the change requests raised. When a support employee working for the service provider resigns or leaves a project, all user IDs and privileges assigned to that person must be revoked or changed as early as possible.

To ensure an effective and comprehensive review, inventory detailing

1. a list of servers and systems within the scope of the project, and which servers / systems are storing sensitive or personal information,
2. a list of support staff from third party service providers as well as the user ID and access privilege granted to individual support staff,
3. a list of data, especially sensitive or personal data, transferred to the third party service providers

should be maintained accurately and kept up-to-date. An inaccurate or incomplete inventory might be the first sign of problems in the governance of an outsourcing project. Regular audits should be conducted to assure that the agreed security controls are actually in place.

OTHER BEST PRACTICES

An organisation can outsource its IT systems and processes to external vendors, but no organisation can outsource its responsibilities; in particular, the legal obligations to its customers. Business owners, data owners and end-users all have a role to play in ensuring security when outsourcing.

IT Practitioners

If the outsourcing service involves hosting information systems at a third party data centre, an on-site visit to assess the security environment of the hosting company should be conducted before making any final decision to outsource.

Similarly, if customer data or other sensitive information is to be transferred to servers owned by a service provider, a security risk assessment covering the physical and logical security controls at the premises hosting the servers should be conducted before sensitive data is released to the service provider. The service provider should set up an isolated environment to segregate the organisation's data from that of other clients. Communication paths used to transfer the data must be secure, and sensitive data should also be encrypted using strong encryption algorithms. When the servers involved are based in another country, the impact due to different jurisdictions should also be assessed.

Because staff of a third party vendor might need to access the organisation's data after outsourcing has begun, the data owner should always be aware of where the data is actually residing, and who has access to that data. Before approving any access by third party staff, the organisation needs to be fully informed as to why the access is needed, and what the minimal access right is needed to perform the required task. Regular ID and

access right reviews should be conducted to ensure that no excessive access rights are granted. Audit trails should also be regularly reviewed to check whether there are any suspicious activities (e.g. a sudden increase in the number documents downloaded), which might be an indication of a security breach.

In addition, if there is a need to connect machines from third party service providers to the organisation's internal networks, full system virus scans with the latest virus signatures and detection and repair engines should be conducted regularly.

End-Users

For end-users, automatic protection features in servers, computer terminals, workstations or microcomputers (e.g. password protected screen savers, keyboard locks, and so on) should be activated if there has been no activity for a predefined period of time to prevent any attempts at illegal system access. Alternatively, the logon session and connection should be terminated after a predefined period. User workstations should also be shut down, if appropriate, before employees leave work for the day or before a prolonged period of inactivity.

III. CONCLUSION

The running and monitoring of a large-scale outsourcing project is not easy. Any failure in IT governance can have a substantial impact on business. While enjoying the cost savings or other benefits brought about by IT outsourcing, management should bear in mind that an organisation can only outsource its operations, but not its responsibilities. Security impact analyses and risk assessments should be started as early as drafting of the contract and cover the vendor's IT environment as well as the organisation's. On-going monitoring and regular reviews must also be conducted to ensure proper management of the IT outsourcing project and/or service.