Information Security Updates

Newsletter for General Users

Issue 2 – IT Outsourcing

Statistical Report

Data breach – Third-party services dilemma

System glitches such as a third-party sending out unauthorised statements, stood at 36% of the root causes of the data breach. Overall, 42% of all cases in the Ponemon data-breach study involved third-party mistakes and flubs.

(http://www.networkworld.com/news/2010/012510-data-breach-costs.html)

Legislative Update

Data Protection Laws and Outsourcing

Data protection is a vital aspect of business, especially in the outsourcing industry. Throughout the process of outsourcing, a lot of data – both common and sensitive – is exchanged between a service provider and its client. Service providers in many countries are requesting their authorities to come up with a law that can assure the safety of data that is transferred by the client to the service provider to work on a project.
http://www.flatworldsolutions.com/blogzone/?p=101

I. Background

Why IT Outsourcing?
With today's economic conditions providing severe challenges in various industries including the education industry, more companies are evaluating the effective use of external providers to help them support and expand their IT organizations.

The following technology and industry trends reshape some of the ways in which companies operate and are in turn helping to support the increased use of outsourcing:

- **Cost savings:** Today's global economic crisis is inspiring companies to explore ways to reduce their operating costs and improve efficiencies.
- **Sustainable IT:** To expand the computing power or IT resources without making larger investments in buying hardware or spending more on IT infrastructure costs, outsourcing can help consolidate and virtualise the infrastructure and purchase IT capacity to produce a lower total cost of ownership.
- **Flexibility:** Instead of merely seeking the lowest cost, more sophisticated approach of outsourcing is to blend flexible capacities from a range of outsourcers in diverse locations into an effective, customised mix that addresses the information and communication needs.

See the article (KPMG publication – "A New Dawn – China's Emerging Role in Global Outsourcing")

What are the IT Outsourcing risks?
– Fast pace of change in technology use is leaving businesses at risk
As organisations are looking for ways to cut their IT costs, they have increasingly turned to external providers who host applications on their behalf. These services, including software as a service (SaaS), are now used by over majority of the organisations polled.

At the same time that companies are increasing their dependence on other organisations for their IT services, there has been an explosion of new cyber attacks. 61 percent of large organisations have detected attempts to break into their network in 2009, twice as many as two years ago. Worryingly, only 17 percent of those with highly confidential data at external providers ensure that it is encrypted.

Outsourcing IT services does not make the security risk go away, but few companies are taking enough steps to ensure their outsourced services are not vulnerable to attack.

See the article (http://continuitycentral.com/news05097.html)

II. Management

Shifting a function to outsourcing can be beneficial to the university because of cost saving and flexibility. Nevertheless, management has the primary responsibility to oversee the outsourcing activities and ensure the risks associated with outsourcing are managed in order to maximize the benefit of outsourcing.

Role and Responsibilities

From the information security perspective, management is responsible for assessing the risks associated with the outsourcing activities, overseeing the vendor selection process, designating function owners for the outsourced functions, and ensuring that information security policies and procedures are followed.

Management should designate function owners for each outsourced function to manage the operational risks of the outsourcing activity.

Assessing Outsourcing Risks

Prior to the establishment of outsourcing relationship, management should decide whether the university will benefit from the outsourcing based on the risk assessment performed by the function owners.

In the risk assessment, business operation and information security aspects should be taken into account. If the risks involved are assessed as high while the commercial benefits are marginal, management should not outsource the function.

Choosing an Outsourcer

Aligning the University's outsourcing objectives with the outsourcer's business models is a key success factors in IT outsourcing. Managing outsourcer is completely different from managing an in-house team. The outsourcers have their own agenda and objectives.

When selecting an outsourcer, the following criteria should be taken into account:

- Company's reputation and history;
- Quality of services provided to other customers, particularly the education sector;
- Number and competence of staff and managers;
- Financial stability of the company and commercial record;
- Retention rates of the company's employees; and
- Professional standards followed regarding quality assurance and security management.

Statistical Report

What's Your Outsourcing Vision?

Opinions on the quality of work relative to the overall cost of outsourcing were split fairly evenly across all categories, with two exceptions: 46% of respondents felt their outsourced end user support was lower quality and lower cost... so much for a great help desk. Those who are outsourcing to different cloud or SaaS vendors had a different view: 37% felt outsourcing provided higher quality at a lower cost. (http://www.informationweek.com/blog/main/archives/2010/03/whats_your_outs.html)

Related Article

IT Outsourcing – 9 Signs It's Time to Fire your Vendor

Breaking up is hard to do, and when it comes to IT outsourcing, it can be expensive and risky, too. Issues with an outsourcer--such as deteriorating service levels, lack of investment, excessive turnover, or even fraud are potentially even more costly than the actual break-up. (http://www.networkworld.com/news/2010/032410-it-outsourcing-9-signs-its.html)

References:
http://www.iso27001security.com/ISO27k_model_policy_on_outsourcing.doc
http://www.computerworld.com/s/article/print/347122/After_the_Ink_is_Dry?taxonomyName=Management&taxonomyId=14

II. Management (cont'd)

Related Article

Carnegie Mellon Spins Off IT Sourcing Certification Group

A set of standards developed at Carnegie Mellon University will be expanded in a certification program that establishes the proficiency of companies providing IT outsourcing services. The university has issued an exclusive license to a new spin-off company, ITSqc, founded by the same academics involved in setting up the standards in the first place. (http://campustechnology.com/articles/2010/01/11/carnegie-mellon-spins-off-it-sourcing-certification-group.aspx)

Related Article

Schmidt: Why You Should Outsource Your IT Security

Former White House security adviser Howard Schmidt told a room of Australian security experts that he believed companies should outsource their IT security.

At the Australian Information Security Association conference in Sydney on 3 December 2009, Schmidt said outsourcing IT security allowed outsourcers to see the "bigger picture" of the organisation's IT set-up. (http://www.securecomputing.net.au/News/161961,schmidt-why-you-should-outsource-your-it-security.aspx)

IT Outsourcing Contract

A formal contract between the university and the outsourcer shall exist to protect both parties.

To prepare the contract, operational staff and function owners should be involved to help create performance metrics and statements of work so as to measure what is restricted to the university operations. The requirements and expectations of end users and affected functions should be considered in developing the contract.

For information security, the types of information exchanged and the purpose for information exchange should be clearly defined in the contract. A binding confidentiality agreement shall be in place if the information being exchanged is sensitive.

Based on the risk assessment result, additional controls should be referenced in the contract, for example:

- Legal, regulatory and other third party obligations, such as:
  - Data protection or privacy laws for Hong Kong.
- Information security obligations and controls, such as:
  - Information security policies, procedures, standards and guidelines;
  - Background checks on employees or third parties working on the outsourcing contract;
  - Access controls to prevent unauthorised disclosure, restrict modification or destruction of information;
  - Information security incident management procedures;
  - Return or destroy all of the university's information assets by the outsourcer after completion;
  - Protection of intellectual property shared with the outsourcer, e.g. copyright and patents own by the university;
  - Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls associated with IT systems;
  - Anti-malware, anti-spam and similar controls; and
  - IT change and configuration management practices and controls.

References:
http://www.iso27001security.com/ISO27k_model_policy_on_outsourcing.doc
http://www.computerworld.com/s/article/print/347122/After_the_Ink_is_Dry?taxonomyName=Management&taxonomyId=14

III. General Users (Function Owners)

Roles and Responsibilities

Designated owners of outsourced functions are responsible for assessing and managing the business and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

Risk Assessment

The function owner shall assess the risks before the function or process is outsourced. The risk assessment shall include the following considerations:

- nature of logical and physical access to university's information assets and facilities required by the outsourcer to fulfil the contract;
- sensitivity, volume and value of any information assets involved;
- commercial risks, such as the possibility of the break down of outsourcer's business, the failure to meet agreed service levels; and
- outsourcer's security and commercial controls currently in place.

After the completion of the risk assessment, the results shall be presented to management for reviewing and approval of the risk and benefit for outsourcing.

Change in Operation

The outsourcing of a function changes the work of hands-on operational staff radically. In turn, the staff has to manage and monitor the work of outsourcer and develop metrics to measure the performance of the outsourcer accurately.

Function owners work as the communication medium between the outsourcer and management. They have to maintain open lines of communication, and ensure that the objectives of the management are achieved.

Related Article

An Outsourcing Service Model: Outsource Operations, But Not Responsibility

The internal service management team or retained layer consists of the people who own the relationship with the service provider. This team is responsible for ensuring that the service provider delivers the service as contracted and, more importantly, that the service delivered meets the requirements of the end users.

The team measures the performance of the service provider on an ongoing basis. Service measures should be in place from day one to measure actual performance against promised performance. In addition, the team should also take measures regularly (at least once a year) to benchmark the service levels the organization is receiving against industry best practices. (http://www.sourcingmag.com/content/c060621a.asp.)

References:
.http://www.iso27001security.com/ISO27k_model_policy_on_outsourcing.doc.
.http://www.computerworld.com/s/article/print/347122/After_the_Ink_is_Dry?taxonomyName=Management&taxonomyId=14