GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Outsourcing Security Management

The need for outsourcing

The security of Information is a key management concern in the modern, electronic business world. In order for companies to maintain their competitive edge, business decisions must be based on accurate, complete and accessible information.

According to BS 7799, Security of information refers to the preservation of

- Confidentiality - Ensuring that information is accessible only to those authorized to have access.
- Integrity - Safeguarding the accuracy and completeness of information and processing methods.
- Availability – Ensuring that authorized users have access to information and associated assets when required.

The degree to which these aspects are preserved must be based on the business requirements for security. This can be properly understood through accurate risk and impact analysis.

Security management is concerned with addressing activities that are required to maintain risks at a manageable level.

According to Information Security Forum,
A project to upgrade software to a business critical system containing extremely sensitive information was incorrectly implemented.
As a result the mission critical data within this system was unavailable for two days. This affected the business in the following ways:

- Sensitive information could not be retrieved, creating a safety risk.
- $105 million in revenue could not be recovered.
- 1 000 departmental users and 10 business partners could not use the system as intended
- 5 000 queries from customers went unanswered
- 500 data entries were delayed

Source: It could happen to you – A profile of major incidents, Information Security Forum

The challenge to meet security requirements, to prevent such disastrous impacts, is becoming more overbearing to organizations. Outsourcing security management could offer the solutions - The key questions faced by any organization is

- Should they keep the responsibilities of information security in-house;
- Should they develop and train their own IT staff,
- Should they develop their own security policies

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Or

- Should they contract such services to an outsourcing specialist who is using the latest available technology, tools and expertise to offer the most efficient service?

The decision to outsource security management needs to be weighed carefully as this highly debatable decision has both pros and cons. This purpose of this paper is to highlight some high-level security issues, faced by organizations when outsourcing security management. Some key factors regarding preparation and management of the outsourcing partnership are also included.

Range of services

The number of outsourcers offering security services is fast growing to meet the demand for security management. Outsourcers can offer complete or partial solutions to companies. The services offered vary from high - level security e.g. developing policies to detailed technical solutions e.g. Router configuration standards. Organisations need to exercise caution with whom they select to partner with. If they do not properly understand their need for security, these services may exceed or fall short of the requirements necessary to preserve security.

Security monitoring and auditing services

Outsourcers are also providing clients with security monitoring and auditing services. These essential functions provide feedback. For example:

- Logging & reporting failed and successful attempts to gain access.
- Using Auditing tools to ensure best practices are applied to policy or standard settings.
- Implementing intrusion detection to recognize unauthorized and suspicious activity.

Any service level agreement must specify the responsibility for monitoring and reporting.

Specialized knowledge and experience

Security outsourcers claim to have specialized knowledge and experience. The expectation is that they are trained on new technologies, techniques, and are aware of the latest vulnerabilities and security updates. The difficulty facing organisations is the measurement of this claimed expertise and knowledge and actually benefiting from it.

Team of specialists

Outsourcers can afford to retain highly skilled security professionals. Outsourcing security gives an organisation access to a team of specialists who focus on securing their clients networks and information. There is very little knowledge transfer to the organisations staff. Thus the organisation becomes totally dependent on these teams of specialists. A mitigating factor is that as trained security professionals depart, the responsibility to continue providing specialist security personnel rests with the outsourcers.

Security Philosophy, Polices & Practices may differ

The outsourcer's security policies and practices may differ from those of the organization. This may result in the organizations needs for security not being met. The

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

organization must ensure that the outsourcer complies with the organisations policy. For example, the Change Control policy must be adhered to before any testing or maintenance service is performed, on networks or critical application systems.

Critical Access

Outsourcing security management allows critical access to the company's private and sensitive information. This could lead to the outsourcer gaining unfair advantage or becoming a competitor of the company. Service level agreements must include legal clauses, which will prevent unnecessary risks to the company. Once information is leaked, there is very little a company can do. Non-disclosure agreements which prevent outsourcers from using an organizations architectures and strategies must also be drawn up, perhaps with penalties for violations.

The seriousness of this type of outsourcing threat was highlighted, when a Chinese programmer working on a large Air Force computer contract, broke into a database that detailed combat readiness. He posted on the Internet passwords to the database, which contained unclassified information on aircraft, communications and missiles. The programmer worked for the contractor the Air Force hired to work on the computer system.

Unaware of the culture and people

Organisations are often unaware of the culture and type of people working for the outsourcer. The likelihood of misunderstanding is increased if the level of information security knowledge between the organisation and the outsourcer is vastly different. This could lead to frustrations, which drive people to behave dishonestly. Differences in the business environments in terms of hours of business, organizational politics, business practices and culture could also lead to communication weaknesses and the failure to deliver services.

Sub-contracts

Due to the demand for fast and efficient services, outsourcers who lack the expertise or technical skills must look elsewhere. This often results in the outsourcer sub-contracting parts of their work to smaller unfamiliar companies. These sub-contracts also increase the risks of inappropriate programming practices, virus infection, poor communication, and generally low-quality service being delivered. Given the subcontractor relationship, there is little the organisation can do directly and often has to work indirectly through the chief outsourcer.

Ownership

Many people are under the misconception that "outsourcing is handing over control"- An organisation can assign responsibilities to the outsourcer but the ownership and control of the information must be dictated by the organization. It is therefore imperative that an internal management team is dedicated to this function.

Latest Technology

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The outsourcer may be keen on implementing the latest (potentially unstable, bleeding edge) security technology and tools. This could create unnecessary complex procedures to the existing processes if the business need is not initially considered. Internal staff aggravated by new procedures, which increase their workloads, will be tempted to bypass procedures and breach security. The particular flaws associated with the release of technologies may not be identified and pose problems, which would have been identified by other users.

People aspects

Most outsourcers focus primarily on perimeter and host security i.e. the technical solutions. The people aspects of security are often ignored yet most security related incidents occur from within the organistion.
These security compromises can take many forms:

- Sharing of passwords with co-works and strangers.
- Using company resources for personal and other non-related business purposes.
- Inserting incorrect and falsified information to the information system and computer programs.

User awareness

Security management must address end-user security awareness and education.
Adequate information security and computer usage policies must be developed, implemented and communicated to users. Using outsiders to develop policies and procedures raises the risk that these policies may not consider the existing culture of the organisation. Many employees would perceive these policies as obstacles to getting their tasks completed.

Getting it right from start

- Service Level Agreement (SLA)
- Internal Management Team
- Security Policies and procedures

Service Level Agreement (SLA)

The first step to ensuring a successful alliance is to prepare a well-developed Service level agreement. This agreement will set the boundaries, levels of quality of service, penalties and deliverables that the organisation requires. Legal issues regarding data protection acts, national and international security laws should also be included to protect both parties.

A suitable method of accurately measuring performance must be agreed upon and complied with on a regular basis. Determining the quality of service is subjective.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Contract negotiators should identify factors that are indicative of the quality of service required. The outsourcer should provide evidence to support the objective measurement of these factors.

Outsourcing agreements can exist for several year's, the SLA must continuously be evaluated, improved and adjusted. Regular reviews of procedures for measuring the SLA factors and the factors themselves must be reviewed. As the business needs grow, the security requirements need to be re-addressed within the SLA.

Internal Management Team

An internal management team comprising of senior executives and existing security professionals should be formed within the organisation to manage and measure the performance of the outsourcer. Failure to recognize and create these vital functions has led to organistions losing control of or simply not managing their agreements. This team needs to be intimately involved with the outsourcers to ensure due diligence is being performed and to provide adequate stewardship of critical information resources. The levels of adequacy determined in the SLA should guide the criteria for measurement.

Security Policies and Procedures

Before any security service is outsourced, the organization should ensure that security needs are understood and compensating mechanisms, such as policies are created and implemented throughout the organization. Security services are driven by security policies. The absence and weakness of a security policy can prevent an organization from taking necessary action against attackers or employees. If the governing policy does not define what is acceptable or unacceptable, the legal avenues available to the organisation, will be limited. Security policies are also extremely useful in raising security awareness.

The policies that have been developed must be adequate; they must be clear, concise and effectively cover all security layers i.e. from the Governing security policy of the organistion, which provides high-level guidelines to the detailed standards implemented at lower levels. The value of the policy is only achieved when policies are complied with. Policies must be periodically monitored to test their effectiveness and appropriately adjusted for inadequacies.

Conclusion

Within the last few years Security Management outsourcing has grown and matured. There are old and new players in the market. As the need for security services amplifies, organisations will establish criteria to evaluate security management outsourcers and partner with them. Will this interdependency ever provide an acceptable level of assurance?

Based on the above discussion, it can be concluded, that apart from the technical solutions, adequate management and complex scenarios, assurance is primarily

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

determined by trust and people fulfilling their responsibilities. Even though all the precautions and best practices are followed, the potential still exists for an outsourcer to exploit an organistion.

Skip Kemerer of NASA has precisely stated that any person with unscrupulous motives and with access to sensitive information has the potential to cause damage. "Security is tied to the person. If I had access to government secrets and wanted to sell them, no one could stop me from doing that. It still comes down to the individual."

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References and Resources

1. Harreld, H. "Outsourcing opens security risks". 5 January 1998. URL: http://208.201.97.5/pubs/fcw/1998/0105/fcw-risks-1-5-1998.html (20 March)

2. Reid, W. S. "Outsourcing: The 20 steps to success". 1996.URL: http://www.wsrcg.com/outsourc.htm (20 March)

3. Vijayan, J. "Outsourcers rush to meet security demand". February 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57980,00.html (20 March)

4. Levine, D. E. "The ins and out of outsourced security". November 1999. URL: http://www.planetit.com/techcenters/docs/security- (20 March)

5. Microsoft Enterprise Services White Paper. September 2000. "Security management for ASPs". URL: http://www.microsoft.com/technet/ecommerce/aspsec.asp (21 March)

6. Raikow, D. "Keys to the Kingdom" November 2000. URL: http://www.zdnetasia.com/biztech/security/story/0,2000010816,20153974-1,00.htm (21 March)

7. Cardwell, B; Violino B and M.K McGee. "Hidden partners, Hidden dangers—Security and service quality may be at risk when your outsourcing vendors use sub-contracts". January 1997. URL: http://www.techweb.com/se/directlink.cgi?IWK19970120S0039 (22 March)

8. Pankowska, M. "Outsourcing impact on security issues" 1998. URL: http://figaro.ae.katowice.pl/~pank/secout2.htm (22 March)

9. BS 7799- British Standard, Part1 – Information security management. 1999

10. Information security Forum, It could happen to you- A profile of major incidents, February 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: April 24th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor