Security Service Level Agreements: Quantifiable Security for the Enterprise?

Ronda R. Henning
Harris Corporation
Rhenning@harris.com

Abstract

A popular business paradigm for information systems treats the information infrastructure as a corporate utility. In this model, a fixed Total Cost of Ownership (TCO) is associated with a given workstation, the network infrastructure, user applications, and personnel required for operational support. Related to the TCO model is the Seat Management model, which exploits the economies of standardization and scale to reduce information technology expenses. In both of these models, a defined, measurable, service level is applied as a cost metric. For example, seven days per week, twenty-four hour help desk support is more costly than five days per week, business hours support. These measurable service levels are defined as Service Level Agreements. Few security services have been specified in terms that are amenable to Service Level Agreements. This raises the question -- can security be adequately expressed in a Service Level Agreement context. This paper looks at a derivation of security related service level agreements for a large enterprise. The possible applications of this approach are presented, as is a discussion of the caveats an information technology organization should consider prior to adopting security service level agreements.

1.0 Introduction

To minimize the costs associated with information technology, corporate enterprises have been migrating to a business case oriented support models. In these models, platform standardization and economies of quantity are applied. The rapid pace of technology advancement makes leasing an information infrastructure a more cost-effective solution. When weighed against the alternative of purchasing individual components, integrating the pieces into an infrastructure, and having an obsolete architecture within six months, leasing is a much more attractive option. Two analysis methodologies support these business models:

1. Total cost of ownership (TCO), which seeks to quantify an organization's cost per employee for infrastructure, help desk support, upgrades, and ongoing maintenance. TCO is usually characterized by on-site interviews followed by a recommendation report on cost saving measures. These recommendations include standardization of hardware and software suites, centralization of network management functions, and consolidation of help desk support.

1999 New Security Paradigm Workshop 9/99 Ontario, Canada

2. Seat Management, whereby an organization is benchmarked against best practices in similar organizations. Seat Management may include TCO analysis, and focuses on life cycle managed support services. Seat Management focuses on savings that can result from outsourcing entire processes such as enterprise management and network infrastructure.

While standardization of the enterprise's computing infrastructure is a desirable economic goal, it may not be an appropriate strategy from an information survivability perspective. Current thought in information survivability favors a diversity of hardware and software within an organization. An organization's ability to survive an intrusion is increased when a diverse information infrastructure is in place as opposed to a homogeneous one.

If an organization's network infrastructure has been privatized or leased from a vendor, the tenant organization may have minimal assurance that security is being correctly managed and little recourse in the event of possible compromise. The contracting organization is dependent on the security services that the service provider has in effect. There may be shared storage media with other customers, a lack of protection for network connections, or no cohesive incident response capability. An important, and often missed aspect of outsourced services, is the concept of shared risks and vulnerabilities. For example, if a site's connectivity is through a leased private network but an outsourced infrastructure is used to centralize enterprise management, the outsourced infrastructure is a potential vulnerability to the private network.

TCO and Seat Management are not new paradigms, and the use of Service Level Agreements to contractually specify gradients of service and capability are not new concepts. However, to date security services have not been consciously incorporated into this model. The paper presents the results of an attempt to derive Service Level Agreements (SLAs) for

security services. These SLAs are validated against both the users' formal security policies and his practical security policy as embodied in his system concept of operations and architecture. The arguments for and against security SLAs are presented, and we conclude with a discussion on whether the SLA concept can be meaningfully applied to security services.

2.0 A Caveat

The reader should be forewarned -- this paper presents a practical approach that can potentially improve security services. It is based in the reality of mission critical information and applications, a shortage of qualified information technology staff, and a need to reduce costs while maintaining a current information infrastructure.

3.0 Enterprise Economic Models

Both Seat Management and Total Cost of Ownership have security implications for an enterprise's information infrastructure. . Understanding the security implications is simplified through the examination of both the seat management and the total cost of ownership models.

3.1 Total Cost of Ownership

In the total cost of ownership assessment, an organization is audited against a proprietary cost model.[1] A series of on-site interviews with various members of the information systems staff seeks to answer a fundamental question:

"How much does a single user cost an organization?"

On the surface, a user's conventional costs may appear quite simple: the cost of the hardware on the desktop and the software application suite used. In reality, the physical cost of the workstation and its software does not include the cost of the network infrastructure, any long haul communications media, help desk software, or information systems personnel that staff the enterprise's network operations center. All of these costs are aggregated and categorized.

The raw information is then analyzed to determine if an organization has maximized its investment. For example, if multiple word processors or office suites are used, a study recommendation may include standardization on a single software suite. The recommendation is usually substantiated with cost analysis information that illustrates how licensing, training, and support costs are reduced through standardization.

During the on-site interviews, the analysis team substantiates the interview findings with cursory audits of system configurations and the network operations center. The preliminary results are usually briefed to the organization at the conclusion of the interview process.

[1] Total cost of ownership analytical models are considered highly proprietary. Among the more widely used models is that of the Gartner Group.

3.2 Seat Management

Seat Management differs slightly from Total Cost of Ownership analysis. In the Seat Management context, the emphasis is extended beyond economies of standardization and scale. Recommendations for consolidation of functions and personnel are more commonplace. Consolidation of services allows the seat management environment to highlight potential outsourcing opportunities within an enterprise.

For example, a seat management analysis may recommend an organization replace all hardware over N-years old, and equipment leasing instead of purchase. In this analysis, a case would be made for the obsolescence and increased maintenance costs associated with older hardware. Leasing would be recommended over purchase to ensure an organization would have a standard architecture component, and to avoid the costs associated with technology refreshment. In a leased enterprise, the platforms and/or applications are replaced every N-years, when the term of the lease expires.

Seat management emphasizes the various life cycle support services that can be performed on a commodity oriented, fixed price basis. In this context, an enterprise might outsource all configuration management functions for a given amount per seat.

3.3 The Relevance to Security Services

Total cost of ownership and seat management services have a disconcerting flaw -- they do not effectively consider information assurance mechanisms as a critical portion of their analysis. One of the most attractive and cost effective recommendations of seat management is the consolidation of network services into a single Network Operations Center (NOC). This results in manpower reductions as well as greatly simplified operating environments, features that are highly desirable in enterprise management. However, these features also make this environment highly vulnerable to undetected misuse and improper configuration. For example:

- An incorrectly installed Windows NT™ patch may impact thousands of users and make their systems vulnerable to a malicious code attack.
- One system administrator may inadvertently turn off auditing of security relevant events for an entire location's infrastructure, eliminating valuable evidence in cases of intrusion or misuse.
- Monitoring of critical vendor or Computer Emergency Response Team security alerts may not occur, leaving an organization vulnerable to potential compromise.

This is not meant to dismiss seat management as a detriment to good security practices. It simply illustrates that with a standard environment and centralized administration, it is much easier to impact the security posture of many more users. Therefore, correct and diligent security administration becomes much more significant to a larger population of users. The possibility of propagating much broader vulnerabilities, over a larger span of control, in a homogeneous environment,

is significantly larger. It becomes necessary to completely define an organization's security policy and practices and to verify their correct implementation in the corporate infrastructure.

4.0 Security Management within the Context of the Enterprise

Within an enterprise, security management is often an ill-defined function, often defined as password management and virus protection. Most enterprises have one or more security policy directives that define security relevant operations. In some industries, such as healthcare, security policy requirements may exist as governmental directives. For example, the NSA INFOSEC Assessment Methodology considers the following areas to be representative security relevant activities[2]:

- INFOSEC Documentation
- Identification and Authentication
- Account Management (establishment, deletion, expiration)
- Session Control Management (access control lists, files, directories, servers, remote dial-up, internet services)
- External Connectivity
- Telecommunications
- System Security Administration
- Auditing
- Virus Protection
- Contingency Planning
- System Maintenance Procedures
- Configuration Management
- Backup Policies
- Labeling
- Media Sanitization/Disposal
- Physical/Environmental Controls
- Personnel Security
- Training and Awareness

A traditional comprehensive security management program addresses each of these areas. The mission context of the information processed in a given system provides the context of information criticality. This criticality, in turn, can be used to determine the security management mechanisms that are most appropriate for a given application.

5.0 The Service Level Agreement

One approach to the integration of security management services into enterprise information services and their economic models is through the definition of Service Level Agreements (SLAs). SLAs are applied throughout the seat management and telecommunications services domains to define quantifiable standards of service. If a vendor does not meet the SLA metrics, cost penalties may be assessed against the vendor. Classic SLA areas include:

- the response time to trouble calls,
- mean time between failures (MTBF), and
- average time to service help desk requests.

To date, security management activities have not been quantified or expressed as Service Level Agreements. This does not mean that security management is not a quantifiable, measurable service. To date, except in some experimental metrics programs, security management practices have not been explicitly categorized and defined. The state of security technology has only recently matured to the point that centralized security administration may be realized. Technology and administration practices may not be sufficiently mature to be reliably quantifiable.

To determine if meaningful security relevant service level agreements could be generated, a trial project was undertaken. This project enterprise resembled most other global enterprise applications: geographically disbursed, large quantities of data, relatively robust data integrity requirements. The enterprise had recently completed a Total Cost of Ownership assessment, and was in the process of defining a Seat Management environment. In the course of this process, a random security audit highlighted the need for improved security management practices. Service Level Agreements were already being defined for other aspects of the enterprise architecture, resulting in a high degree of comfort with the concept.

5.1 Derivation of Preliminary Service Level Agreements

Unlike traditional service level agreements, there was very little available material for derivation of security relevant service level agreements. While a single security audit type approach may define the state of security within an enterprise, it does not necessarily provide any confidence in the state of the future security posture. Because service level agreements are enforceable contract performance clauses, it was important that the service level agreements be based as much as possible on a factual basis. To ensure the service level agreements were appropriate, a three-step process was applied to generate a preliminary group of service level agreements.

5.1.1 Policy Analysis

Because there was very little data available to support generation of security service level agreements, the first step was to explore all relevant policy, guidance, and operating instructions. These included various U.S. Government regulations and standards, such as:

- Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources
- Computer Security Act of 1987
- CCIB-98-028, Common Criteria for Information Technology Security Evaluation
- DoD 5200.28, Security Requirements for Automated Information Systems

[2] National Security Agency, INFOSEC Assessment Methodology Student Handbook, Module 3, p. 14, 1999.

- Federal Information Processing Standards Publication (FIPS Pub) 181 - Standard for Automatic Password Generation

Analysis of over fifteen such regulations and operating instructions allowed a preliminary set of categories for SLAs to be generated. These categories covered the following topic areas:

- Security documentation
- Security Auditing
- Contingency Planning
- User Security Training
- Network Infrastructure Management
- Physical Security
- User Discretionary Access Control (DAC) Management
- Password Management
- Electronic Audit Trail Management
- Security Perimeter or Boundary Services
- Intrusion Detection and Monitoring
- Web Server Security
- Database Server Security
- Encryption Services
- Configuration Management

With the basic categories in place, further refinement activities were initiated. The policy and guidance documentation was used to define minimum services that were mandatory for policy compliance. As such, mandatory requirements defined the minimum required service level agreements.

5.1.2 Architecture Analysis

The results of the preliminary service level agreement definition task were applied in an architecture analysis activity. Where possible, the mandatory security requirements as specified in operating instructions and policy were validated against the customer's network maps and architecture diagrams. This approach validated those mandatory requirements that could be traced to specific topology elements (i.e., web servers, firewalls, etc.). It also assisted in formulation of questions for the next phase, on site interviews.

5.1.3 On-site Interviews

The last phase in the service level agreement formulation process was a series of on-site interviews at selected customer sites. Sites were selected because they were representative of a given architecture configuration in terms of size, network topology, or technologies deployed.

To prepare for the on-site interviews, a series of questions were generated. These questions traced to specific service level agreement topics, and were designed to solicit additional details about representative site implementations.

In conjunction with these interviews, site documentation was reviewed to determine if policies and procedures were correctly implemented. Interview subjects often volunteered additional information, which was also useful in discovering the operational user's security concerns.

5.1.3 Results of the Process

The results of the service level agreement generation analysis were somewhat mixed. The initial categories defined during the document analysis phase were an excellent starting point for the architecture analysis and interview process.

Four major categories of security metrics were defined, addressing the different measurement aspects of the service level agreements. The major categories of measurement criteria were:

- Performance Criteria - encompassing metrics for a tangible, deliverable material, such as the generation of documentation, audit logs or reports.
- Temporal Criteria - related to objectives to be met within a specified period. These include retention of back-ups and audit logs, return-to-service time, and responsiveness to attack.
- Functional Criteria - pertaining to the activities that arise in making adjustments to systems or networks as a normal part of adding new features, users, applications, methods, or processes.
- Process Criteria - pertaining to recurring tasks, such as those performed as part of a daily or monthly routine. These include performing back-ups, monitoring system events, and intrusion reporting.

In most cases, a single service level agreement category incorporated multiple criteria areas. For example, the service level agreement for documentation incorporated functional, process, and performance criteria. This reflected the documentation function, the fact that it was used to document processes such as daily system back-up, and the tangible nature of the end product, namely, the document itself.

Table 1 illustrates a representative group of service level agreements for the generic areas of contingency planning and security training.

6.0 The Organizational Balance Sheet

No one approach to security management has a completely positive impact. In this section the potential benefits and liabilities of service level agreement based information services is presented.

6.1 Potential Benefits

The use of service level agreements for security services has the potential to provide some very tangible benefits to an enterprise. The largest benefits are associated with improved security administration and management practices. The definition of service level agreements forces an organization to think about security. User roles and privilege groups are

SECURITY SERVICE BANDS AND PERFORMANCE METRICS					
Service Measurements	**Level 1 Service**	**Level 2 Service**	**Level 3 Service**	**Level 4 Service**	**Performance Metrics**
Contingency Planning					
Contingency Plan for Local Sites. Contingency plans include security related contingency scenarios such as intrusion and virus attacks that compromise resources (hardware, software, and data) and restoration of resources.	Generate plan for all systems	Generate plan for all servers	Contribute to Plan	Review Plan	Quality of Plan, For SEC1 &2; >95% of systems have plan in place
Contingency Plan for Contractor Site	Generate	Generate	Generate	No	Quality of Plan
Rehearse contingency plans to ensure operability.	Monthly	Quarterly	Annually	Optional	> 5 issues found during rehearsal 30 days to resolve issues.
Back up data from network servers and security components.	Daily	Daily	Daily	Daily	99% data availability
Archive backed up data	Off Site	Off Site	Off Site	On Site	99% data availability
Restore backed up data	30 minutes	1 hour	4 hours	8 hours	Restored 95% of time within response time.
User Security Training					
Train users in proper use of security features (e.g., Password Format, Incident Reporting)	On Site Training, Annually	CBT, Annually	CBT, Annually	Optional	100% Users Certified
Train customer administrators in proper use of security features (e.g., Password Administration, Desktop Configuration)	On Site Training, Annually	Off Site Training, Annually	CBT, Annually	Optional	80% Administrators Certified
Perform social engineering attacks on systems.	Every 1 mo. 95% of attempts thwarted.	Every 3 mos. 90% of attempts thwarted.	Every 12 mos. 85% of attempts thwarted.	Every 18 mos. 75% of attempts thwarted.	Every audit met and average is >95% of target.
Security violations introduced by individuals due to oversight or intentional introduction to the systems (from help-desk reports, security audit reports or incident reporting reports).	Less than 2% of systems every 1 mo.	Less than 7% of systems every 3 mos.	Less than 15% of systems every 12 mos.	Optional	% of Security incidents introduced by users within target.

Table 1. - Representative Service Levels for Contingency Planning and User Training.[3]

defined and standardized in terms of access rights to data and connectivity to various networks. In essence, the security policy of the enterprise is defined in an enforceable, uniform manner that accurately reflects the information access needs of the organization.

System standardization also usually results in more effectively managed systems. Service level agreements are cost effective when they allow an organization to reduce operations and administrative manpower required to operate an infrastructure. One technique to accomplish the manpower reduction is the use of centralized enterprise and/or network management environments. This approach provides "single seat" monitoring of critical enterprise services, such as fault isolation and account administration.

The net result of a service level agreement based architecture is a more effective enterprise information infrastructure, with consolidated control of critical security relevant functions. Standardization of hardware and software suites makes users more effective in the long term, and simplifies maintenance and technology refreshment activities. Financially, the potential reduction in manpower, coupled with quantity licensing cost reductions, allow a service level agreement based architecture to decrease information technology expenses.

7.2 The Potential Liabilities

The very standardization that results in the economic and administrative benefits of service level agreement based infrastructure services also defines the greatest source of liability. A diverse, robust infrastructure, reflecting a heterogeneous collection of systems, maximizes an organization's information survivability.

In general purpose N-tiered client-server architectures, clients tend to be Microsoft Windows™/Intel based platforms, while servers and data warehouses execute on Unix variants. The trend towards standardization of platforms tends to move both clients and servers to Windows/Intel platforms. In this environment, not only are the clients susceptible to malicious code compromises, but the servers are equally as susceptible. Not only can desktop systems be readily compromised, but an enterprise's data warehouses and corporate knowledge base could also be compromised at the same time. What was once characterized as a minor nuisance virus attack can easily

[3] Source: Information Assurance Benchmark Analysis Study, Final Report (draft), 21 October 1999.

become a plague like event requiring implementation of a comprehensive incident response capability.

Finally, the level of sophistication required to execute a successful penetration attempt against any given platform in the enterprise drops dramatically. The proliferation of bulletin boards with representative sample code of viruses and trap doors makes a "compromise by example" scenario quite possible in a homogeneous environment.

It should also be noted that security service level agreements might be most applicable to large enterprises. In these environments, there can be economies of quantity that make it feasible to invest the time required to generate meaningful service level agreements for an enterprise. For smaller organizations, or organizations at a single location with relatively small communications expenses, the effort involved in defining service level agreements may outweigh the potential savings.

7.0 Remaining Issues

The initial analysis of security services in the context of a managed service level agreement environment has left some issues unresolved and in need of additional research.

7.1 Quantifying Security

The initial group of security relevant service level agreements was circulated to several seat management service vendors for comment. The primary comments received were a lack of tangible, measurable services. In the telecommunications arena, service level agreements are used to specify service parameters such as the amount of bandwidth, number of dropped packets, and duration of outages. Security services have historically not been quantifiable in such concrete terms. The issue is whether it is possible to define operationally viable metrics that provide some indication of the relative quality of an enterprises security posture. For example, does timeliness of incident response or percent of system patches correctly implemented provide any insight into an organization's security posture? Representative areas to investigate for potential metrics may include:

- Availability of an incident response team.
- Time to detection of intrusions
- Response to intrusion
- Defined access control policy implemented on N% of the platforms.
- Correct firewall configurations
- Defined user roles
- Detection of denial of service attacks
- Response time for forgotten/reset passwords

The trial service level agreements attempted to provide threshold values for some of these services as part of the service level definitions. The commenting services vendors had few comments on the feasibility of attaining the specified service thresholds.

7.2 Process Oriented Security Management

The use of security service level agreements to define expected security management services has been characterized as security by process specification. The nature of several of the areas in the trial set of security service level agreements is process oriented. Security service level agreements must address operational and administrative security management activities. They do not address the electronic assurance mechanisms that enforce security policy on the information system users.

Security service level agreements do not replace system assurance mechanisms. What they can provide is process-oriented assurance that operational and administrative processes are in place and correctly executed in an organization. They do not replace assurance mechanisms integrated into the products used by the vendors.

7.3 Insurance vs. Assurance

Using security service level agreements has been compared to purchasing insurance. In this scenario, the service level defines the relative comfort level or insurance that the enterprise has some degree of protection. Assurance, on the other hand, ensures that mechanisms properly enforce a specified security policy and nothing more.

The insurance analogy is applicable and extends to necessary operational and administrative procedures that are needed to maintain secure operations. In this scenario the service level agreement specifies the operational level of services required to maintain the assurance mechanisms in a secure state.

It should be noted that, unlike the insurance industry, which can predict its level of exposure to a particular class of threat, the assurance industry can not quantify the potential exposure of a given system to a given class of threats. Rather, security risks tend to behave and propagate more like infectious epidemics, (i.e., on an exponential scale) as opposed to a controllable, predictable manner.

7.4 The Cost of Security Services

Within a total cost of ownership model, the cost of a given service or group of services must be definable and divisible. The costs associated with each trial area in a given service level must be identified and aggregated to develop a total cost of security services.

It is a straightforward task to define the costs associated with the configuration, maintenance, and eventual replacement of a single mechanism. It is not as simple to address the costs of federated services such as intrusion detection or audit analysis capabilities. When the costs associated with compromise recovery to a secure state are incorporated, the total cost associated with security services becomes a more difficult calculation.

When traditional commercial service level agreements address security services, the service thresholds are defined in terms of number of hours of assistance when an intrusion is detected, or a recovery to a secure state is required. Specification of additional security services, or administration of services such as intrusion detection, firewall management, access management, etc., are not normally calculated into defined service level agreements.

8.0 Conclusion

In conclusion, we have presented the concept of security service level agreements as a mechanism to specify the security services required for an effective enterprise. The context surrounding service level agreements has been introduced, and a technique for deriving security service level agreements has been presented.

Security service level agreements do not replace assurance mechanisms, however, they do promote a well-defined set of security oriented operating procedures. As such, they can be a valuable component of a comprehensive enterprise security program.

Service level agreements may impact information survivability. They have an adverse impact from the perspective of a robust, diverse infrastructure. However, potential improvement gains from centralized administration may allow early detection of security incidents and more rapid containment strategies.

The user of security service level agreements must understand the costs and benefits associated with this service model. The user must also be aware that the service level agreement provides process based assurance for the operational, administrative procedures needed for secure operations. Security service level agreements do not replace electronic assurance mechanisms for security policy enforcement.

9.0 Acknowledgements

The author wishes to acknowledge the information assurance benchmarking program team, and the participants in the New Security Paradigms Workshop, for their comments and input to this paper.

10. Bibliography

[1] Esten, Deborah, "TCO finds the Strike Zone", DATAMATION, December 1997.

[2] GartnerGroup, TCO Distributed Computing Assessment, 1997-1998, available at http://www.gartner.com/measurement

[3] General Services Administration, "Seat Management Overview," 1998, available at http://www.gsa.gov/fedcac/seat.htm.

[4] Harris Corporation, "Information Assurance Benchmark Analysis Study Final Report (draft)," 21 October 1999.

[5] National Security Agency "INFOSEC Assessment Methdolody (IAM) Student Manual, Version 1.0, September 1999.

[6] Phillips, Jeffrey R., Ph.D., "Total Cost of Ownership (TCO) Best Practices and Seat Management", Proceedings of AIMC'98 Annual Information Management Conference, 23 October 1998.