25

Security when outsourcing: concepts, constructs, compliance

E. Roos Lindgreen, H.R.D. Janus,
A. Shahim, G. Hulst, I.S. Herschberg

The authors can be reached at KPMG EDP Auditors, Burgemeester Rijnderslaan 10, 1185 MC Amstelveen, The Netherlands. Telephone: +3120-6567429. E-mail: roos.edo@kpmg.nl.

Abstract

As the ownership and management of information technology (IT) is increasingly put out at contract, information security turns out to be an essential issue to address in any outsourcing process. The authors analyse present concepts for both the demand side and the supply side of the market for external facilities management. They propose a cyclic approach related to British Standard 7799 allowing the service provider and his client clearly to define respective responsibilities in the construct of a formal security agreement, part of the general agreement between the service provider and his client. Such a security agreement stems from an assessment of the client's IT environment; compliance with the security agreement is tested by a formal review to be conducted by an impartial evaluator.

Keywords

Information security, outsourcing, security agreements

1 INTRODUCTION

It is a sad fact that many organisations are ill aware of the cost of ownership and the quality of service of information technology (IT), despite its many evident blessings.

According to recent surveys (see, for example, (Paans and Gianotten, 1994)), outsourcing some activities in owning and managing IT environments to a specialised third party, henceforward called the *service provider*, is believed to lower the cost and improve the quality, especially if the service provider has been chosen as one of several competitors. Acting in this manner, many organisations, henceforward called *clients*, are currently outsourcing their IT-related activities.

© IFIP 1997. Published by Chapman & Hall

Typically, the client and the service provider unite to agree on the *quality* of the service to be delivered. In practice, the intangible notion of quality of service is carved up into disparate quality aspects, such as response times, throughput times and availability windows. Such individual aspects are usually specified in an overall *service level agreement*, part of the comprehensive agreement between the client and the service provider.

The present paper focuses on quality requirements to be imposed on information security in outsourcing, where information security is defined, in the present paper, as *the preservation of confidentiality, integrity and availability of information systems in the face of adversaries with malicious intent.*

As will be proved below, stipulating security requirements is beneficial to both the client and the service provider.

First, let us consider the benefits to the *service provider*. Typically, the service provider is under a contractual obligation to deliver a specified level of service. To the client, the obligation persists even when the service provider is confronted with inadvertent or intentional actions endangering compliance with the service level agreement. It follows that, to the service provider, taking proper security measures is a prerequisite for safeguarding any agreed quality of service.

There is another important reason for the service provider to take adequate security measures: the client relies on due care by the service provider, who has, in a manner of speaking, been entrusted with the client's vital organs. Note that, in the outsourcing market, reliability is seen as critical to success, and security incidents attributed to the service provider's negligence will dissuade customers from the service, rightly or not. Information security is thus essential to any outsourcing service.

Technical analysis shows that the security measures taken by the service provider ultimately depend on some minimal discipline by the client, ranging from the use of strong passwords to the proper reporting of security incidents. Only by explicitly agreeing on their mutual responsibilities, the client and the service provider can eliminate the vagueness threatening the effectiveness of the measures taken. Also, an explicitly worded agreement provides a framework for solving disputes on liability such as may arise after an incident.

In summary: to the service provider, taking appropriate security measures is necessary for risk management, which, in turn, requires the stipulation of security requirements in an explicitly worded agreement on the parties' mutual responsibilities.

Such an approach furnishes definite advantages to the client. First, security is set at a mutually acceptable level; and secondly, that level is visible to both contracting parties. An additional benefit is that, typically, the degree of security will be higher than it was before outsourcing, since the degree of security required by the service provider may well be higher than the degree of security achieved by the client beforehand. For a typical client, outsourcing will thus compensate for some part of a known security deficit.

Despite its evident importance, information security turns out to be an underrated item in many service level agreements. We propose a structural yet simple approach to remedy such underrating. Our approach has been applied successfully in a number of outsourcing projects. It is characteristic to our approach that conflicts between requirements are resolved, in the sense that the interests between opposing parties are agreed to have been uniformly victorious.

To quote one instance, business costs will be perceived to have prevailed whenever they are opposed to information security agreements; an objective discrimination is thus promoted.

The outline of the paper is as follows. Section 2 describes the basic requirements to be met by an information-security agreement between client and service provider. Section 3 describes the proposed approach for arriving at such an agreement. Section 4 discusses the practical applicability of the proposed approach. In section 5, conclusions and directions for future research are given.

2 BASIC REQUIREMENTS

In section 1, we have made our case that an *explicit* agreement on the mutual responsibilities for security is advantageous, both to the client and the service provider. The next step is to list the requirements to be met by such an agreement, without pretence to completeness.

Requirement 1 - Stipulation of mutual requirements and responsibilities

Above all, an approach should allow for a clear and unambiguous definition of mutual requirements and responsibilities. They must be able to identify which measures should be taken by whom or, at worst, be capable of inferring their mutual obligations.

Requirement 2 - Clarity

A security agreement should be worded so as to be necessary and sufficient for the goal envisaged; in other words, it should be clear. One important aspect of clarity is the *level of detail* of the agreement. A delicate balancing act must be performed. If stated in abstract terms only, the agreement will be ambiguous, leaving room for various interpretations when it is disputed. Yet, if overly detailed, it will be resented as rigid, confining and bureaucratic.

The ensuing optimisation problem is complicated by the fact that security requirements differ in kind from other quality requirements usually found in service level agreements. All other quality requirements have familiar schemata and are quantifiable. Typical examples could be performance requirements (e.g. *Performance of communication link: 2 Mbps sustained*), response times (e.g. *Response times for common commands: 95% within 2 seconds*) or availability requirements (e.g. *Availability of the system: 7 days, 24 hours, except for the second Wednesday of each month, when the system is unavailable from 17:00 to 19:00*). In contrast, there is no agreed way to quantify security requirements, and no agreed formalism for expressing them. Fortunately, it is proposed that the difference can be smoothed out by specifying security requirements in operational terms, viz. in terms of the measures to be taken. This brings security requirements in line with other conventional, customary quality requirements.

Requirement 3 - Completeness of measures

For want of a better approach, security requirements, we assume, have been stated in operational terms rather than in their ideal formulation, which would be in terms of business requirements. Granted this, completeness of those requirements is found to be essential. As an instance, the security part of the overall service level agreement should not only address

technical security measures, but organisational security measures as well. Moreover, it should address *all* relevant technical and organisational measures.

The completeness requirement shows up the essentially negative character of information security. Moreover, it suffers from the defect that absence of security is provable experimentally, whereas positive security can never be proved: the tiniest flaw may leave an entire system wide-open to all potential adversaries (Herschberg and Paans, 1984). In this respect, security requirements are in the same unfortunate position as is testing of programs: flawedness is provable, correctness is not.

The completeness requirement is at odds with the clarity requirement. As above, we see that stipulating security requirements is an optimisation problem, and a non-trivial one at that.

Requirement 4 - Adherence to standards

If possible, an approach to information security should adhere to existing standards in order to improve efficiency and provide a sound basis for mutual confidence. A particularly appropriate standard is the Code of Practice for Information Security Management, promulgated as British Standard 7799 (BS 7799, 1995).

BS 7799 defines technical and organisational security measures, broken down as follows:

1. Security policy;
2. Security organisation;
3. Assets classification and control;
4. Personnel security;
5. Physical and environmental security;
6. Computer and network management;
7. System access control;
8. System development and maintenance;
9. Business continuity planning;
10. Compliance.

Although BS 7799 has been launched with much publicity, it has only met a moderate degree of acceptance. According to a recent survey in the United Kingdom (Bacon, 1996), about 2% of the organisations polled claimed to have fully implemented BS 7799, while another 11% stated to be seriously considering its implementation. Despite these mildly disappointing statistics, BS 7799 and its national adaptations emerge, at this writing, as the most widely accepted *de facto* standard.

Requirement 5 - Transparency

An approach to information security must be sufficiently transparent so as to be understandable to novices in the field of information security. Since any issue related to information security will constitute an interface between the client and the service provider, it will cross the paths of senior management, sales representatives, account managers and legal counsellors. It is most desirable that each party should be able to capture the essentials of the agreement without having to be an information-security expert.

Requirement 6 - Weighing by business value
Since different systems have different security requirements, no approach to information security should treat security requirements uniformly. Rather, those requirements should be weighed, whereas such differential weighing, it is widely accepted, is to be in harmony with the business value of the system under consideration.

Requirement 7 - Freedom of choice
The client, whenever outsourcing, must be the ultimate judge of the services he demands. It follows - as a complication to the service provider - that the client must be free to reject security measures, however much they may be desired by the service provider.

Requirement 8 - Flexibility
Information security is impacted by many external variables subject to continuous change, such as standards, legislation, the client's internal security policy and the state of the art in information technology. If it is to accommodate these external dynamics, any security agreement should have intrinsic flexibility, supple enough to adapt to any foreseeable changes.

Requirement 9 - Assessment of compliance
For mutual confidence, it is essential that an impartial evaluator should periodically assess to what degree the client and the service provider comply with the requirements agreed upon.

3 THE INFORMATION SECURITY CYCLE

In order to meet the requirements enumerated above, we propose a structured yet simple cyclically repetitive approach to the interaction between the client and the service provider when outsourcing.

This approach, termed the *information security cycle*, consists of six prescriptive consecutive phases as per table 1 and figure 1.

Table 1 Phases in the information security cycle

1	Classification	Classify IT environment based on business value.
2	Selection	Select proper security measures.
3	Quick security audit	Check which measures are in place.
4	Security agreement	Agree on security measures and mutual responsibilities.
5	Implementation	Implement unimplemented security measures.
6	Evaluation	Evaluate whether security agreement is complied with.

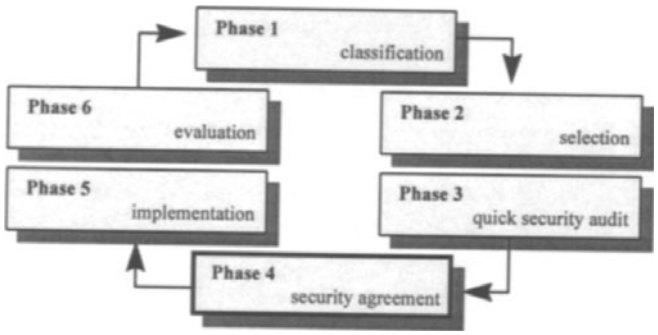

Figure 1 The information security cycle.

The phases above are to be traversed periodically. In the course of the cyclic traversal, there must be close co-operation between the client and the service provider. Since the security agreement will impact the service offered commercially, the information security cycle should be initiated as an essential part of pre-sales negotiations. Thereafter, a periodicity of a year is recommended, unless either party insists on a shorter time of traversal.

Below, the phases of the information security cycle are described in detail.

Phase 1 - Classification

In the classification phase, the client assesses the sensitivity of the IT environment to be outsourced, with due regard to the confidentiality, integrity and availability of the data and the applications.

Various methods for such a classification exist. There is a choice of a top-down approach and a bottom-up approach. In the top-down approach, the sensitivity of the IT environment is based on an inventory of business processes and applications. In the opposite approach,

known as bottom-up, it is the IT environment which is primary to the classification. Since the IT environment is the better understood, one does do well to adopt the bottom-up approach. For this purpose, two stages are followed: first, a classification team inventories the data and applications stored and processed within the IT environment; second, the classification team inventories the business processes using these data and applications.

The next step is to identify the relative importance of these business processes, applications and data in a top-down fashion, taking each of the quality aspects (confidentiality, integrity and availability) into account. The resulting classification is set according to a high water mark; the most important data and/or application determines the classification of the entire IT environment.

In addition, the IT environment is categorised as being highly sensitive to negative publicity, should an incident occur or otherwise.

Phase 2 - Selection

In the selection phase, the client selects a set of security measures from a standard catalog based on BS 7799. The catalog comprises two sets of security measures: (1) elementary security measures considered necessary by the service provider from the viewpoint of due care; these measures are henceforward collectively termed the *information security baseline*; (2) additional security measures, henceforward termed *information security services*.

1. The information security baseline

In section 2, it was argued that the information security baseline should be derived from existing standards, most notably BS 7799. Unfortunately, BS 7799 is not fully fit for the purposes stated (Roos Lindgreen, 1996). In order to enhance its practical applicability, we propose to use a derived version of BS 7799 by modifying it in the following ways:

- to remove the standard's inherent redundancy;
- to remove measures aimed at special environments, such as traditional mainframe-environments;
- to remove measures that are way beyond due care;
- to remove measures that are application-specific, as opposed to generic;
- to remove unnecessary details.

The result is a "cleaned-up" version of BS 7799, preserving the overall structure, content and spirit of the standard. For purposes of reviewability, each deviation from the standard should be carefully motivated.

The resulting baseline is considered mandatory - respecting, however, the client's freedom of choice. Some of the measures in the baseline are to be taken by the client (e.g. stating an information-security policy or defining ownership for all information systems); some measures are to be taken by the service provider (e.g. installing a central desk for reporting security incidents or configuring the access-control mechanisms within the IT environment); and some measures are to be taken by both (e.g. stating security requirements in contracts with third parties and observing due care when using IT equipment).

2. Additional information security services

Of course, the client can have security requirements that surpass the information security baseline sketched above. In that case, the client should be able to pick his choice of security measures from an additional catalogue. Such a catalogue could describe information security services for each of the quality aspects confidentiality, integrity and availability; these services could then be implemented by tangible measures such as encryption, extended access control, extended physical security, data encryption for mobile PCs, or TEMPEST.

In any case, the selection of security measures should be based on the outcome of the classification phase; see figure 2.

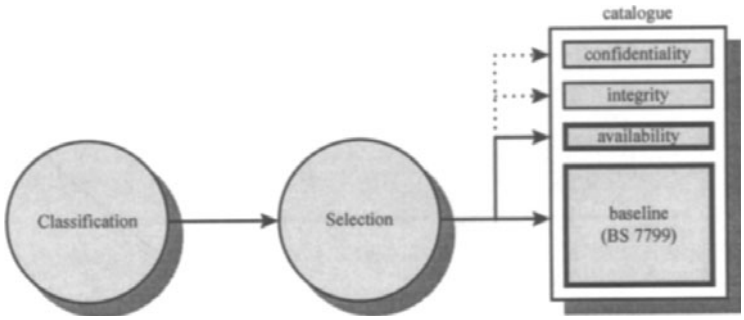

Figure 2 From classification to selection.

Phase 3 - Quick security audit

After a set of mandatory and additional security measures has been selected, the client and the service provider should perform an initial assessment in order to establish the degree to which the security measures selected have been put into place. This audit should be quick and clean; it should at least provide, to the client and the service provider, a first indication of information-security arrears. In order to speed up the audit process, an automated audit tool may be used.

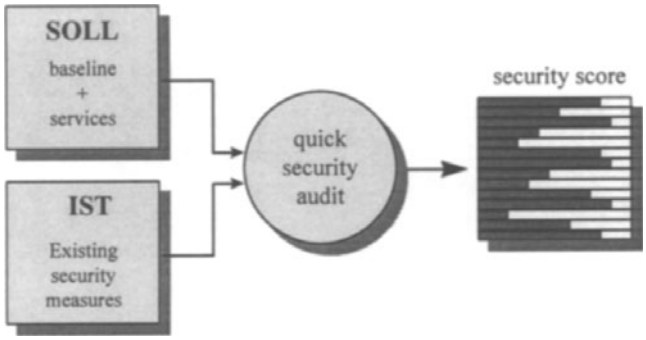

Figure 3 Quick security audit.

Phase 4 - Security agreement

The client and the service provider then formally agree upon which security measures are to be taken by whom. The resulting *security agreement* is self-contained, referring to the corresponding paragraph in the generic service level agreement and vice versa.

It makes sense to model the security agreement after the information security baseline, so that for each of the measures in the baseline, the client and the service provider agree on their mutual responsibilities. In the security agreement, the client and the service provider also agree on the realisation of additional security services.

Phase 5 - Implementation

In the implementation phase, the client and the service provider implement the security measures agreed upon, especially those not already in place. The implementation phase should be performed according to accepted project-management principles. Prior to implementation, the client and the service provider should at least agree on the measures to be implemented, the procedures to be followed in the course of implementation and the conditions for acceptance.

Phase 6 - Evaluation

In this phase, an impartial evaluator assesses to which degree the client and the service provider comply to the security agreement. This assessment should not be limited to the mere presence of the measures, but rather should be extended to ensuring that any measure installed in turn is conformable to its specification. The assessment, which may result in some sort of certificate (Veltman, 1995), will expose any deviation from the security agreement and so contribute to the mutual confidence between the client and the service provider.

4 DISCUSSION AND CONCLUDING REMARKS

Supported by standard forms, automated tools, model contracts and security catalogues, the approach described above has been implemented by a large outsourcing company. It has been applied in practice on several occasions. Based on simple theoretical foundations, the information security cycle has proved a suitable basis for working out the complex issue of information security in real-life outsourcing processes. Nevertheless, some critical remarks can be made.

The classification phase should be traversed with caution. First, since the classification is based on a high water mark, it is not inconceivable that a relatively large IT environment is highly classified, although only a minor part of this environment contains truly sensitive data. In that case, the service provider can propose to carve up the IT environment into disparate compartments, each of which can be secured to fit. Second, the classification phase can easily lead to intensive and time-consuming discussions on details that may be less relevant in the scope of the information security cycle. This may lengthen the entire cycle's traversal time, which, in turn, will lessen its degree of acceptance. An efficient classification thus requires sufficient experience and expertise.

We have found that a formal security agreement may be highly appreciated by some clients, but will be perceived as unnecessarily bureaucratic by others. We feel that the security agreement should not degenerate into a goal in itself. The service provider should keep in mind that maintaining continuous contact and an open discussion with the client is far more important - and often far more effective.

A last point of criticism may be that the information security cycle as described is insufficiently detailed. Our defence is threefold. First, we feel that the simplicity requirement poses an upper bound to the level of detail of any approach that has "practical applicability" as its stated purpose, especially if non-experts are involved. Second, it is our experience that every client is unique, defying any attempt at designing a method that is highly detailed, yet generally applicable. And third, we argue that any approach to information security should offer sufficient leeway in order to deal with the dynamics of present IT environments.

Perhaps the most challenging aspect of the proposed approach - or, indeed, of any approach to information security - is to convince of its necessity all parties involved, observing the possibly conflicting interests of these parties. We have found that, especially at senior management level, security awareness may be raised by arguing that information security is an essential ingredient of general risk management, the latter, in turn, being an essential ingredient of responsible management, rather than dishing up scary stories about high-tech hacking.

5 REFERENCES

Bacon, M. et. al. (1996) *National Computer Security Survey 1996*, KPMG report, publication no. 4937.

British Standards Institution (1995) BS 7799, *A code of practice for information security management*, BSI, ISBN 0 580 23642 0.

Herschberg, I.S. and Paans, R. (1984) The programmer's threat: cases and causes, *Proceedings of the NGI Section EDP Auditing workshop "Beheer en controle van en in besturingssystemen"*, Noordwijkerhout, NGI, ISBN 90 706 9004 7, May 15-16, pp. 125-136.

Paans, R. and Gianotten, M.H.E. (1994) Data center management, *Getting order out of chaos*, Giarte Publishing, Amsterdam / Minneapolis, ISBN 90 74712 04 5.

Roos Lindgreen, E. (1996) A Sense of Secureness, *Approaches to information security*, Ph.D. Thesis, Delft University of Technology, Delft, The Netherlands, ISBN 90 900 9320 6.

Veltman, P. (1995): Third party review en -mededeling bij uitbesteding van IT-services, Compact 95/3, KPMG EDP Auditors en Samsom Bedrijfsinformatie, ISSN 0920-1645, pp. 20-37.

6 BIOGRAPHY

Edo Roos Lindgreen is audit manager at KPMG EDP Auditors, Amstelveen, The Netherlands. His current professional and research interests include corporate information security and the design, implementation and assessment of complex IT environments.

Hans Janus is business development representative at Communication Solutions Nederland (CSN), Leidschendam, The Netherlands. His professional interests include cryptography, information security and marketing research.

Abbas Shahim is consultant at KPMG Management Consulting, Amstelveen, The Netherlands. His professional and research interests include data warehousing, logistics, system development and information security.

George Hulst is security manager at CSN. He is responsible for corporate information security, coordinating and supporting the Information Security Cycle in outsourcing projects. George is a member of the project group Internet of the NGI, the Dutch computer science association.

Bob Herschberg is professor of the chair of Operating Systems and Distributed Systems at Delft University of Technology. His research interests are the penetrability of systems reputedly secure and the securability of systems reputedly sensitive.