Security and Trust in IT Business Outsourcing: a Manifesto [6]

Y. Karabulut [1] F. Kerschbaum [2] P. Robinson [4]

SAP Research
Karlsruhe, Germany

F. Massacci [3] A. Yautsiukhin [5]

DIT, University of Trento
Trento, Italy

Abstract

Nowadays many companies understand the benefit of outsourcing. Yet, in current outsourcing practices, clients usually focus primarily on business objectives and security is negotiated only for communication links. It is however not determined how data must be protected after transmission. Strong protection of a communication link is of little value if data can be easily stolen or corrupted while on a supplier's server. The problem raises a number of related challenges such as: identification of metrics which are more suitable for security-level negotiation, client and contractor perspective and security guarantees in service composition scenarios. These challenges and some others are discussed in depth in the article.

Key words: Business Process Outsourcing, Security, Security Metrics, Protection Level Agreement.

1 Introduction

Today many companies prefer to delegate IT work packages to external or third-party organizations rather than fulfilling them themselves [4,11]. In this way a company can concentrate on its core business rather than on peripheral

[1] Email: yuecel.karabulut@sap.com
[2] Email: florian.kerschbaum@sap.com
[3] Email: Fabio.Massacci@unitn.it
[4] Email: philip.robinson@sap.com
[5] Contacting author. Email: evtiukhi@dit.unitn.it
[6] This work was partly supported by the project EU-IST-IP-SERENITY

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

tasks, especially if they differ too much from the company's primary activities. For example, Consolidated Freightways, a transportation company, outsources the upgrade and management of its IT infrastructure to IBM Global Services [11].

Definition 1.1 *Outsourcing* is the ongoing administration, management and possibly subcontracting by an external party, of specific client's (IT) processes to enhance their efficiency and effectiveness [25]

Often the outsourced company itself may further outsource its assignments to others. That is, a company may start as a contractor and by acquiring and handing out new assignments may become an orchestrator.

When a company plays an orchestration role it coordinates a business process to accomplish the work. The process can be static or dynamic. In traditional outsourcing contracts we envisage a static orchestration where the process is defined from the outset and partners and services do not change. For novel paradigms, such as virtual organizations, partners and services can be selected on the fly.

Before cooperation proceeds, participants negotiate a *Service Level Agreement* (SLA). The main part of the agreement is devoted to functional requirements and to some non-functional requirements such as performance. Not enough attention, if any, is devoted to security.

Example 1.2 Web Service security only focuses on the security parameters of communication links. It covers requirements for message encryption, signature, authentication, and server access control [2,23]. WS security standards do not mention how data is protected after transmission. Data can therefore be stored in a server without a properly configured antivirus or in a database without role base access control.

In this paper we identify the security and trust issues that underpin an outsourcing relationship and the notion of *Protection Level Agreement* (PLA) that is appropriate in this setting.

The paper is organized as follows. Section 2 is a short state of the art in security metrics. We introduce a notion of PLA in Section 3. Sections 4 and 5 are devoted to client's and contractor's view of PLA respectively. Section 6 describes how client's PLA can be achieved in service composition scenario. The issue that trust is not transitive is discussed in Section 7. Section 8 is dedicated to related works.

2 Security Metrics. A Primer

Unclear performance and benchmarking metrics are a cause of 56% of outsourcing relationship failure [31]. Therefore, the first step in the problem solution is security metrics identification, a task that so far remained elusive.

Loosely speaking all metrics can be classified into one or more of the following categories:

Organizational - evaluate the security management process.

Operational - assess the system and operating principles in place

Technical - evaluates the quality of software and hardware.

The most well known technical method are the Common Criteria [15]. A product is evaluated against a Protection Profile , a set of requirements for the corresponding product category. Evaluation Assurance Levels (from EAL0 to EAL7) show the level of satisfaction w.r.t. a Protection Profile.

SSE-CMM (System Security Engineering Capability Maturity Model) [27] evaluates a security management process. SSE-CMM assigns a level of maturity (from 1 to 5) to a security system engineering process. This appraisal denotes how well the organization fulfils all base practices.

These methods give a numerical (discrete) measures of security of management processes and products quality. There is no such evaluation method for operational security. Common Criteria can be used for this purpose, but "the interaction between variety of products (hardware and software) are such that detailed evaluation is very close to practical impossible" [19].

Some guidelines [29,8] suggest checking how well (percentage of compliance) the system fulfils best practices. The list of the best practices can be huge and it is very difficult to prove that it is complete, even if a well known standard (such as ISO17799) is used as a basis [10,16].

Risk analysis [28,1,6] is one of the prominent of security system assessment approaches. The most used metric for this analysis is annual monetary loss. If other dimensions (e.g. hours of downtime, reputation) are also used the losses of an organization can not be measured in currency. In this case some form of normalization must be used [6].

Several approaches tried to calculate metrics based on mean-time-to-security-failure [21,24]. Most of them are based on threat analysis of an attack graph. This metric is theoretically useful but so far a field test for its practical relevance is missing.

3 Security Issues in IT Outsourcing

Before proceeding, we identify the stake-holder entities in a typical outsourcing scenario. These entities are sketched in Figure 1.

Definition 3.1 A *Client* is an entity that interacts with of a completed, self-contained business process. A *Contractor* is an entity which agrees to execute the business process and satisfy the client's requirements for such execution. An *Orchestrator* is a contractor that manages a workflow, where some tasks are distributed to other entities. A *Subcontractor* is an entity that receives a task assignment, which is part of a higher-level business process, from another

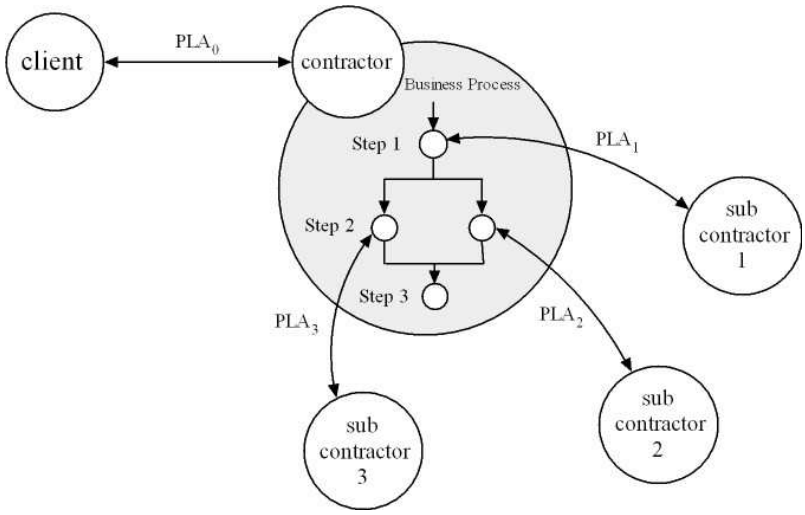

Fig. 1. General business outsourcing scheme of functional interaction

contractor.

In the Figure 1 the contractor plays an orchestrator role, suggesting that an orchestrator always plays a client role with subcontractors. Before investigating technology solutions, such as trusted computing platforms or multi-party computations, we consider what assumptions can be made about the nature of the business agreements and trust between the parties involved. A "contractual trust" relationship between client and contractor exists, in that they have agreed on binding terms and conditions in a *Service Level Agreement (SLA)*.The contractor is hence trusted because if it does not behave according to the contract it is obliged to pay penalties to the client.

The agreement between a contractor and a client normally contains guarantees that reflect the client's business objectives, devoted to functional requirements. These objectives determine the *Quality of Service (QoS)* which the contractor's system must portray.

The high level security goal of a client is to protect its data and make it available (always and only) to the entitled users. In the outsourcing scenario, a client shifts data processing to a contractor and, in doing so, relinquishes direct control of the way in which data is processed and protected. Hence, we return to our key problem: *defining the security equivalent notion of QoS and SLA*.

The contract must clearly describe how data is protected while under the contractor's control:

- protection in *transmission* is the protection of client's data while in transit from the client's host to the contractor's internal network.
- protection in *processing* is the protection of client's data when a contractor controls the way in which data is processed. That is, when stored on machines within the contractor's administrative domain.

Existing forms built around Web Services technology define means for specifying the parameters for a secure communications link. These include requirements for message encryption, signature, authentication and server access control [2,23].

Agreements about data processing and storage restrictions are absent in the Web Service contract. With this missing part, strong communications link only solves one dimension of the secure outsourcing problem (see example 1.2).

Proposal 1 *A client and a contractor must negotiate a data protection agreement including warrants that data is protected during processing by a contractor, as well as during its transmission. These warrants describe the* Quality of Protection *(QoP) required for outsourcing system.*

Challenge 1 *How do we guarantee that a certain QoP is achieved?*

We need some metrics to be sure that the promised level is achieved. Traditional SLA metrics measure some aspects of the process and represent the Quality of Service towards meeting the business objectives. The identification of the metrics is a core phase for agreement negotiation. The client must be sure that its objectives are completely reflected and chosen metrics are relevant for it. The Quality of Protection should be represented by metrics as well.

Proposal 2 Protection Level Agreement (PLA) *is proposed as the section of an agreement that contains security requirements.*

Challenge 2 *Which metrics are more appropriate for PLA?*

Solving Challenges 1 and 2 poses several issues:

(i) *Client vs. Contractor.* This is the client's view of the problem. It has to define which metrics and PLA satisfy its security business objectives. Another main issue is the monitoring of the actual protection mechanism to check whether PLA are actually met and not only declared.

(ii) *Contractor vs. Client.* It is the contractor's perspective. The contractor must determine the metric targets it can provide and how such metrics are related to achievement of the metrics negotiated with its client.

(iii) *Contractor vs. subcontractors.* Other issues arise if service composition takes place. The orchestrator must compose the PLAs of its subcontractors to meet the client's PLA.

(iv) *Intransibility of Trust.* A client may trust to a contractor but not trust its subcontractors. This point must be taken into an account by an orchestrator when a business process is created or a certain QoP is negotiated.

4 Client vs. Contractor

The following observation on the difference between SLA and PLA is useful to decide the appropriate representation for security requirements. SLA de-

scribes functional requirements: what the system must *at-least* do. On the other hand, the natural intuition behind a PLA is that it describes negative events and specifies things that the system should *at-most* allow. This point is represented in Figure 2.

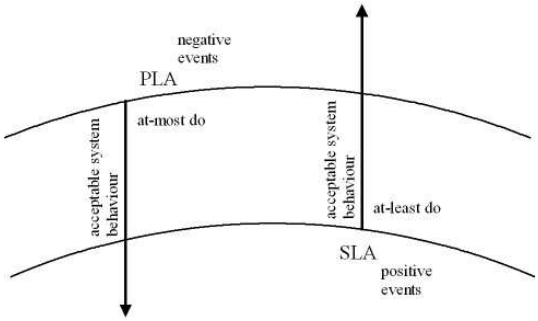

Fig. 2. Acceptable system behavior .

Example 4.1 For example, the speed of connection must be not less then 256 bits/s. Nobody will complain if the speed is higher. On the other hand, the number of successful virus attacks must not be higher then 10 per month (nobody will complain if the number of successful attacks is less).

Proposal 3 *A PLA represents "at-most" allow requirements on the behavior of the outsourcing system*

We want to highlight that if a primary goal of outsourcing is a functional service it is more convenient for a client to determine its security requirements as a PLA. In other words, the client should set a SLA to guarantee that it receives an appropriate level of QoS on its functional service and should accompany this agreement by setting also a PLA to guarantee that the data that it provides for the Functional service get an adequate level of QoP.

In contrast, if the primary goal of outsourcing is to shift security services then a SLA should be specified on those activities. Indeed in this case, the functional service that we are outsourcing is simply a service whose particular function is a security function. So we should be able to distinguish when security is the service itself (SLA needed) from the case in which security protects the object of the service (PLA needed). Indeed, the processing of the data which is used to deliver the security services should be subject to a PLA.

An example might clarify better the point: if we are outsourcing a key generation function for identity-based cryptography we should set up a SLA on the minimum key size (i.e. SLA on the function). In contrast a PLA should be set up to protect our identities or our private key (i.e. PLA on the data for and from the function).

The crucial point in PLA negotiation is identification of metrics which describe the level of protection. We have identified two types of metrics:

Definition 4.2 *Internal metrics* describe security qualities used by a contractor to achieve a high level of security.

Internal metrics help a contractor estimate the maturity of its security system. Some examples of these metrics are: time between updates [18], length of passwords, percentage of compliance with a standard [10,16].

Definition 4.3 *External metrics* are negotiated with the client to show that its security requirements are addressed.

External metrics are understandable for a client and show how security solutions affect it. Possible examples are number of successful attacks on client's data confidentiality [6], mean time to intrusion affecting client's data [24,21], time for system recovering after an undesirable event to restore the availability of client's data.

Mark Lutchen in [20] notes, *'What other mistakes are companies making? When they do outsource IT, they frequently use the wrong metrics - **metrics focused on processes, not outcomes...**'.*

Internal metrics are not informative enough for a client.

Example 4.4 A client may specify an external metric: at most 2 successful virus attacks every month; or an internal one: the antivirus system must be updated at least every 2 weeks, knowing that according to the statistical evidence the number of new virus attacks is expected to be similar. If the trend changes (i.e. wild viruses per month increase) more viruses will affect the client's data than before even if the contractor behaves according to the agreement. In the first case, it is the contractor's responsibility to cope with the problem (i.e. update antivirus system once a week) to keep the number of virus attacks as it is specified in the agreement.

Proposal 4 *External metrics should be used in PLA negotiations.*

So which external metrics are most fruitful for a QoP? We do not recommend metrics based on risk analysis and financial results. At first these metrics have a number of limitations and are not precise [9]. Further, qualitative analysis amplifies these limitations because it operates with relative values (e.g. high, medium, low). The second and foremost reason is that these values are not connected to the service provided and cannot be monitored by the contractor and the client in a shared and agreed way (loss expectancy is difficult to estimate). This does not mean that clients should not use risk analysis to identify the appropriate PLA but simply that the outcomes of the risk analysis such as Annualized Loss Expectancy (ALE) themselves should not be a PLA.

Here we propose the following metrics:

Undesirable events in the observed interval. This measure can be either a percentage or in an absolute value.

Free interval - the interval between the moment in which an undesirable

event took place and the moment in which the incident was tracked and recognized as such.

Time of recovery - the interval between the moment in which the incident has been tracked and the time in which it has been fixed.

We want to point to one more additional problem of trust which is beyond the identification of correct metrics: their monitoring, because in fact they may not be fulfilled by a contractor.

Challenge 3 *How can a client monitor requirement fulfilment?*

A monitor system which controls PLA fulfilments should be developed. Many requirements are very difficult to check by external audit, i.e. from the client's environment. So this monitor should be installed in the *untrustable* contractor's network where the contractor has physical access to it. Several techniques can be used to assure the client that it can trust to the received data: using cryptographic primitives [3], deploying a Trusted Computer Group's environment [26], involving a Trusted Third Party .

5 Contractor vs. Client

A PLA does not tell the contractor how it should configure its system to meet the requirements. The contractor must map the PLA to a functional SLA, to receive concrete requirements which defines what the contractor should install and how it should behave. The mapping may be based on industry statistical data trends, personal experience, stored history, etc. If a client has some particular security requirements or security is one of the main goals of outsourcing the requirements can be expressed in "at-least" way (SLA) directly.

To achieve the external metrics the contractor will have to put in place a number of security policies and mechanisms. This eventually means that a PLA will be transformed to a SLA from "at most one e-mail attachment virus per week steps through the company's centralized antivirus software" to "at-least one signature update per day to the centralized antivirus software". Once such transformation has been done we can use internal security metrics to evaluate the quality of protection achieved, represented by external metrics. A discussion of the idea can be found in [18]. But this idea has not been substantiated by experimental evidences, statistical studies, or formal reasoning. It is just an author's opinion. The author himself has pointed that it is difficult to take into account all factors (e.g. events are not independent, many countermeasures contribute somehow to overall reduction of event probability and so on).

Challenge 4 *How to correlate internal metrics to external metrics?*

Indeed, methods which estimate a security level are based on a set of questions to check compliance with standards [14]. The set is broken up into

protection domains (cryptography, audit, networking). The questionnaire can be redivided into threat domains (protection against viruses, password sniffing, DoS). After that we receive a complete set of parameters and corresponding internal metrics which contribute to a threat protection. Now if we can tell how each of the techniques contributes to mitigation of the threat (e.g presence of a firewall reduces the number of Trojan Horses by 30 percents) correct internal parameters can be chosen to achieve external metrics (e.g. number of Trojan Horses per month).

6 Contractor vs. Subcontractor

In most cases the contractor has to execute a business process (a workflow) to satisfy the client's needs. The workflow can be specified by a client or by a contractor. At one extreme, the client can specify a workflow and require that the contractor fulfils it as it is. On the other hand, the client can only define a set of high level requirements. In this case the contractor has to create the workflow itself in such a way as to fulfil all client's requirements.

Sometimes a contractor does not fulfil all workflow tasks itself but sends a part or several parts of the task to subcontractors which have various levels of protection (Figure 1).

Challenge 5 *How can the orchestrator assign outsourced tasks and PLAs to subcontractors to create a business process which not just accomplishes the client's SLA but satisfies the client's PLA as well?*

At the beginning the contractor has to identify how each subcontractor's PLA_i contributes to the client's PLA. It depends on the functional workflow and how undesirable events at the workflow level as a whole map into sub events.

The process can be made once before the execution: the contractor determines the entire process and then just follows it. In more dynamic environment, the contractor can make a decision during the process execution. This helps establishing the process to fulfil clients requirements in the most efficient way.

7 Trust is not transitive

When several participants come to play, trust issues emerge. As we said a client trusts a contractor to accomplish the task, because their relationship is sealed by a contract. At the same time a contractor trusts its subcontractors for the very same reasons. However there is no contractual trust between a client and the subcontractors. If a subcontractor misbehave the client will have to get back to the main contractor and for a variety of reasons he might decide not to get a proper compensation. The same is true for the contractor – subcontractor relationship. Hence there is the need to consider more

"subjective" notion of trust instead of contractual trust. The client may trust some subcontractors more than others. This decision may be based on previous experience or on statistics. Since the data is not under client's control after its transmission to the contractor, trust relationships must be specified beforehand. The challenge which arises is:

Challenge 6 *How can a client determine which subcontractors it trusts more than others and which less than others?*

One of the possible solutions can be taken from [22]. An orchestrator suggests several possible subcontractors for the business process. The client determines a level of trust (e.g. from 1 to 10) for each of them. A reasoning algorithm, similar to the one represented in [22], returns the most trustable set of subcontractors which can be used by the orchestrator to accomplish the client's goal.

8 Related works

Only a few works tackle the issue of security requirements in business outsourcing. In [17] it is claimed that security requirements must be reflected in the contract and their fulfilment must be somehow monitored. The authors consider security requirements as a part of SLA. *Trusted Virtual Domains (TVDs)* [12,5] are intended to connect a number of remote trustable virtual processing environments in one secure network. Security operational policy (accord of PLA/SLA), which are obligatory for every environment, are used. This technology can be applied to client-contractor interaction when one side (most likely, a contractor) allows another one to use its TVD. It is necessary to point to that TVD requires installation of special isolating software to operate.

In [26] a monitoring system for trusted computer platform is presented. The idea is to embed a trusted hardware component into the execution environment which verifies the compliance of the system with an operational policy (which can be considered as a PLA) at the beginning of interaction.

One of the first papers discussing security SLA in a large enterprise is [13]. The main idea is to check compliance the system with fifteen security domains split into best practices. For each best practice the security service level is determined and added to the SLA (yet it does not consider task outsourcing). [7] extends the security division to compare two SLAs or to find a security SLA which is the closest to the desired one. A similar idea of divide-and-conquer technique was applied to evaluation of Web Service security in [30].

9 Conclusion

In the article the problem of guaranteeing appropriate security during storing data on a contractor's server has been discussed in depth. We have introduced several important definitions and identified a number of challenges and issues.

We have argued that external metrics are more meaningful for a client and have proposed some of them which can be used for PLA. Internal metrics are more appropriate for a contractor. They help to estimate the quality of its security system and to choose the right configuration to achieve its client's requirements. Monitoring of security requirement fulfilment is another important issue which depends on metric types.

Additional issues emerge in a service composition scenario. Clients's security requirements must be inserted into a functional workflow, decomposed and distributed between subcontractors. In addition to these issues trust relationships must be taken into account.

References

[1] Alberts, C. J. and A. J. Dorofee, *OCTAVE Criteria*, Technical Report CMU/SEI-2001-TR-016, CERT (2001).

[2] Atkinson, B., et al. "Web Services Security," Microsoft, IBM, VeriSign, 1.0 edition (2002)

[3] Bellare, M. and B. Yee, *Forward integrity for secure audit logs*, Technical report, University of California at San Diego (1997).

[4] Bowles, J., *Outsourcing for competitive advantage*, available via http://www.vmc.com/articles/Forbes%20Advertorial.pdf (2004).

[5] Bussani, A., et al. *Trusted Virtual Domains: Secure Foundations for Business and IT Services*, Technical Report RC23792, IBM (2005).

[6] Butler, S. A., *Security attribute evaluation method*, Technical Report CMU-CS-03-132, Carnegie Mellon University (2003).

[7] Casola, V., A. Mazzeo, N. Mazzocca and M. Rak, *A SLA evaluation methodology in Service Oriented Architectures*, in: *Proc. of QoP.* (2005).

[8] CISWG, *Report of the best practices and metrics teams*, Technical Report CS1/05-0005, Government reform comittee (2004).

[9] Cohen, F., *Managing network security - part 5: Risk management or risk analysis*, Network Sec. **1997** (1997), pp. 15–19.

[10] Eloff, J. and M. Eloff, *Information Security Management - A New Paradigm*, in: *Proc. of SAICSIT*, 2003, pp. 130 – 136.

[11] Goth, G., *The ins and outs of it outsourcing*, IT Professional **1** (1999), pp. 11 – 14.

[12] Griffin, J. L., et al. *Trusted virtual domains: Toward secure distributed services*, in: *Proc. of HotDep*, Yokohama, Japan, 2005.

[13] Henning, R., *Security service level agreements: quantifiable security for the enterprise?*, in: *Proc. of NSPW* (2000), pp. 54–60.

[14] ISO/IEC, "Information technology Security techniques Evaluation criteria for IT security," (2001).

[15] ISO/IEC, "Common Criteria for Information Technology Security Evaluation," Common Criteria Project Sponsoring Organisations, 2.2 edition (2004).

[16] Johansson, E. and P. Johnson, *Assessment of enterprise information security - an architecture theory diagram definition*, in: *Proc. of CSER*, 2005.

[17] Karjoth, G., et al *Service-oriented assurance comprehensive security by explicit assurances*, in: *Proc. of QoP.* (2005).

[18] Leach, J., *TBSE - an engineering approach to the design of accurate and reliable security systems*, Comp. & Sec. **23** (2004), pp. 22–28.

[19] List, W., *The common criteria – good, bad or indifferent?*, Inform. Sec. Technical Report **2** (1997), pp. 19–23.

[20] Lutchen, M., *IT Outsourcing: The Importance of Retaining a Strong Management Capability, Part One (of Three)*, available via http://www.pwc.com 2005.

[21] Madan, B. B., et al. *A method for modeling and quantifying the security attributes of intrusion tolerant systems*, Performance evaluation journal **1-4** (2004), pp. 167–186.

[22] Massacci, F., J. Mylopoulos and N. Zannone, *Hierarchical hippocratic databases with minimal disclosure for virtual organizations*, The VLDB J. (2006), to appear.

[23] Naedele, M., *Standards for xml and web services security*, IEEE Comp. **36** (2003), pp. 96–98.

[24] Ortalo, R., Y. Deswarte and M. Kaaniche, *Experimenting with quantitative evaluation tools for monitoring operational security*, TSE **25** (1999), pp. 633–650.

[25] Pai, T. M., *Outsourcing for competitive advantage: Are you missing a business opportunity?*, available via http://www.infosys.com/events/MDPAI%20pres%5F5%20Nov%5FSpore.ppt (2001).

[26] Sadeghi, A.-R. and C. Stüble, *Property-based attestation for computing platforms: caring about properties, not mechanisms* (2005), pp. 67–77.

[27] SSE-CMM, "Systems Security Engineering Capability Maturity Model - SSE-CMM Model Document," Carnegie Mellon University, version 3.0 edition (2003).

[28] Stoneburner, G., A. Goguen and A. Feringa, *Risk management guide for information technology systems*, Technical Report 800-30, Nat. Institute of Standards and Technology (2001).

[29] Swanson, M., et al *Security metrics guide for information technology systems*, Technical Report 800-55, Nat. Institute of Standards and Technology (2003).

[30] Wang, Y. and P. K. Ray, *Evaluation methodology for the security of e-finance systems*, in: *Proc. of EEE* (2005).

[31] Yankelovich, P., *Global Top Decision-Makers Study on Business Process Outsourcing*, available via http://www.colthr.com/files/Business%5FProcess%5FOutsourcing.pdf (1999).