December 2003

A Business Process Engineering Based Approach Towards Incorporating Security in the Design of Global Information Systems

Gerald Quirchmayr
University of South Australia

Jill Slay
University of South Australia

Andy Koronios
University of South Australia

Kathy Darzano
University of South Australia

Recommended Citation
Quirchmayr, Gerald; Slay, Jill; Koronios, Andy; and Darzano, Kathy, "A Business Process Engineering Based Approach Towards Incorporating Security in the Design of Global Information Systems" (2003). *PACIS 2003 Proceedings*. 77.
http://aisel.aisnet.org/pacis2003/77

A Business Process Engineering Based Approach towards Incorporating Security in the Design of Global Information Systems

Gerald.Quirchmayr, Jill.Slay, Andy.Koronios and Kathy.Darzano

School of Computer and Information Science
University of South Australia, Mawson Lakes Campus
Mawson Lakes, South Australia.
Email: Gerald.Quirchmayr@unisa.edu.au
Jill.Slay@unisa.edu.au
Andy.Koronios@unisa.edu.au
Kathy.Darzanos@unisa.edu.au

Abstract

IT security has become one of the key issues in information systems and the more global an information system, the bigger the threats it becomes exposed to. The technology to make information systems safe exists, however organisational and design aspects of such systems still need to be addressed. Security is usually not dealt with at the level of business processes and so security policies are typically not linked to system design and implementation. Even at the system level, security features are generally regarded as add on, rather as a key design issue. For this reason we introduce an approach for increasing the security levels of global information systems through business engineering technology.

Keywords

IT security, business process security, security of global information systems.

Introduction

Despite system administrators’ attempts to make information systems secure, they face a series of very difficult circumstances, the worst of which is the lack of integration between business and system design. The recent focus on enterprise application integration in e-business and e-commerce contexts is thus self-explanatory. Systems are usually implemented before the security implications of the overall infrastructure are considered, and it is only after the first incidents have occurred that security policies are developed This tends to show that, in general, security is still considered as an overhead and not as an asset. As long as problems are not encountered, it is always difficult to argue the case for investment in a proper security infrastructure. It is symptomatic that it took the successful attacks on over 2500 websites during the first day of the 2003 Iraq war to finally create a common awareness of how vulnerable our systems have become on one side and how essential they are for operating businesses. Another very recent development is the attempted abuse of Internet banking by what seems to be money laundering schemes related to organized crime.

Traditionally, security is dealt with on a system level by administrators trying to harden the information systems in place against attacks. Rarely, if ever, is security considered while designing the business processes to be supported by the information systems. Security is usually introduced as add on to information systems, and is only part of the overall system design in very exceptional cases. For this reason, methods, such as OCTAVE, developed by CERT, have recently become so popular with government agencies, the financial sector and industry.

As two of the authors have already discussed (Quirchmayr and Slay 2001), the situation is declining with ubiquitous access through Internet-based browsers. It looks almost like an arms race between system defenders and attackers. As soon as a new form of attack is out, everything possible is done to quickly plug the identified hole. So called “white hacker teams” (Whitehacker 2003) have helped to improve the situation as they look at possible vulnerabilities and inform system vendors and affected users before a real attack takes place.

The key issue does, however, remain unsolved: security is generally not a key factor in business process design and, with very few exceptions, is not even considered in the architectural design of information systems. As problems magnify, corporate and end user confidence begin to decline. The first field dramatically feeling the impact is B2C e-commerce [7]. While consumers continue to consult web sites for product information, the number of purchases is far from the predictions made by leading analysts only a few years ago. The fear of security breaches, violations of privacy, and a lack of confidence in existing legal frameworks contribute to the downfall of what was once so proudly called the recession proof new economy. The lack of consumer trust is one of the central issues.

E-commerce now has new opportunities in the form of B2B e-commerce and back office integration, usually referred to as supply chain integration and enterprise application integration (Traunmüller 2002; Bauknecht, Tjoa and Quirchmayr 2002). It is important that the IT industry learns from its previous mistakes, and improves the bad reputation the sector gained in the early stages of e-commerce. This was partially acquired through wrong claims made by numerous consultants about the effectiveness and efficiency of technology. A current example of the difficulties faced due to poor reputation is outsourcing partners and consultants who suffer from the aftermath of the dot.com fallout. Traditional systems and service providers also find it more and more difficult to convince potential customers of the benefits their solutions have to offer.

Security as a Key Issue in Business Process Design

In early 2001, two of the authors started a research project at the University of South Australia that was looking into security design aspects of information systems. This work quickly led to the conclusion that the security infrastructures in place in today’s industry are a mere add on, and are hardly ever part of the overall system design. When the situation was investigated regarding business process design, the findings were even more disappointing. Although several design methodologies are available, such as BPMS (Karagiannis 1996 and http://www.boc-eu.com/english/bpms.shtml), offering the possibility to integrate security modules in the business process design, they are usually not adopted. The authors therefore decided that it was necessary to focus on a newly emerging paradigm, featuring security as overall design aspect, similar to usability design. The primary goal in our approach is to achieve *Secure Business Process Models* that will then provide the necessary security requirements for designing the supporting information (system) infrastructure.

The analysis approach suggested by the authors does therefore propose to extend the traditional BPR requirements analysis phase by a “module b”, comprising the following steps:

1. Requirements analysis for business process modelling
    a. “Traditional” business process modelling requirements (for a detail of a very advanced approach the reader is referred to the example of BPMS (Karagiannis 1996).
    b. Security requirements.
        i. Identification of stakeholders with security, privacy and confidentiality requirements.
        ii. Specification of the requirements of identified stakeholders.
        iii. Identification of the confidentiality/security level of the information entering and leaving a process.
        iv. Identification of the confidentiality/security level of the process itself.
        v. Security risk analysis and assessment.
        vi. Specification of required security levels and mechanisms following the risk assessment carried out in step V.

Together with a thorough analysis of the existing environment through the application of OCTAVE or a similar method, this approach should lead to a comprehensive set of security related requirements and will therefore deliver guidance for business (re-)design.

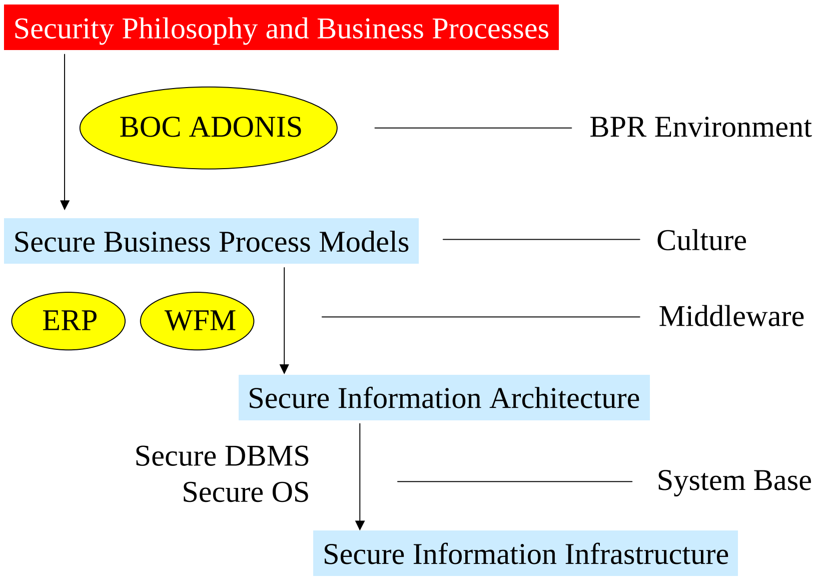
Security Philosophy and Business Processes
BOC ADONIS
BPR Environment
Secure Business Process Models
Culture
ERP
WFM
Middleware
Secure Information Architecture
Secure DBMS
Secure OS
System Base
Secure Information Infrastructure

Figure 1: Architecture of proposed development environment

As shown in the above figure, the introduction of an institutional / corporate security philosophy as one of the essential drivers of business process design helps to make security part of the business (process) culture. This has the effect of creating the necessary awareness and changing the attitude towards security, confidentiality and privacy on a level high enough to make it acceptable when later on imposing it on users through information system requirements. This will also help to identify those security procedures that interfere too strongly with the work to be carried out by staff members. Advanced business process modelling tools usually offer a simulation module that allows running the defined procedures through a theoretical evaluation before starting any real implementation. Thus not only the practicability, but also the proper functioning of envisaged security measures can be tested at a low cost level.

So once the business process model is set up, the security requirements for the information system are also identified too in the form of modules and can serve as input for system design or selection. It quickly becomes obvious whether a proposed system architecture can meet these requirements or not and if not, the additional cost for implementing these features can be estimated.

As is the case with IT governance in general, the full transparency of architectures, structures and events on system level is essential for assuring that decision makers really are in control. This goal is not achieved easily, but driving security design from the business (process) level is an enormous improvement. It helps with creating the necessary awareness of management and opens a window for the introduction of some core principles of good IT governance, such as putting the emphasis on (IT Governance Guides 2003):

- The potential of IT to leverage and influence intangible assets (information, knowledge, trust, etc.).
- The alignment of IT and business strategies.

- The review and approval of IT investments.
- The assurance of IT-related risk transparency.
- The measurement of IT performance.

A Process Oriented View on Security

In line with the overall approach presented in this paper, we now take the perspective that the management of security should itself be viewed as a business process. The two alternatives presented by two of the authors in an earlier paper , a framework and a repository oriented concept, are very well suited for centralized server based information systems as target platforms. Increasingly, global information systems do however come with a strong need for decentralisation. For this reason, this model is not sufficient in meeting this challenge and must therefore be extended. Distribution is not limited to the system architecture; it might be the basis of the whole corporate culture. A distributed approach to business process modelling must therefore be followed. A frame and repository approach do both work well in a centralized environment, but in a globally distributed information system, the repository approach has its advantages due to much easier replication and therefore higher performance.

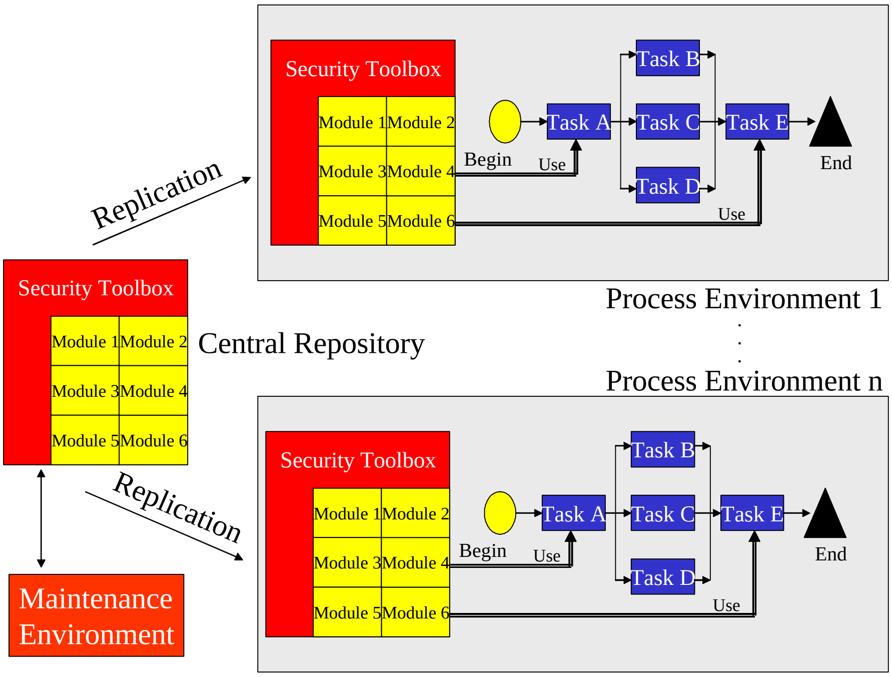

Figure 2: Distributed repository approach

To underline the full compatibility of the authors' approach with well established business process engineering concepts, the ADONIS standard notation (see http://www.boc-eu.com/english/adonis.shtml) was used in the above picture. Decomposing processes into tasks and linking security modules to these tasks in the style of a use case extension is an idea that can easily be implemented in advanced BPR tools, using either their sub-process or their resource representation features. In theory, provided that communication lines offer the necessary bandwidth, the replication can be replaced by loading the security toolbox from a central server. Even if this is possible, it is not recommended due to the increased vulnerability each loading process would introduce. A centralized management and update combined with local storage and execution is therefore preferable to a fully centralized system. The only exceptions are different types of handheld devices with low computational power. In this case it is better to limit their functionality to display and data entry and base all other functionally on the server. This trend is in fact backed by recent research results and industry strategies, such as DSTC'S ODSI and the trend towards server based computing, probably best represented by SUN Microsystems's pioneering slogan "The network is the computer" and IBM's e-server technology .

Practicability Check

An examination of the reality of global information systems gives a good impression of the large number of open issues when it comes to security. The source of most of the problems is that security was not an issue in the original design of most commercial systems. Most of the security technology available today is primarily an extension of existing architectures with some of it working very well at the system level. So it is therefore only the next generation of information systems that can afford to fully incorporate the business process oriented approach described in this paper. The logical consequence is that for the time being a compromise has to be sought: The proposed extension of the requirements analysis phase is already applicable now for the development of new business processes and applications, and for the re-engineering of existing ones. The suggested repository approach can only help in environments where a centralized security management system already is in place. In architectures where security is tied to single application packages, such a centralized security control and management approach has to be developed first. The authors are aware that their approach will in the first phase only be valuable for industry sectors that have always had a high appreciation of security, confidentiality, and privacy, such as financial institutions, of which banks are an excellent example. It is no coincidence that banks were the first outside the government sector to carry out a careful analysis of security requirements before providing Internet services to their customers and it is also no secret that banks are known for following extremely high standards. Over time, security will have to become a standard feature of all information system packages. In an ideal case, we will see a direct export of security models from business engineering environments into security components of information systems, similar to the integration already provided between business process engineering tools and workflow management systems.

Conclusion

This paper has investigated one of the most interesting open security questions in information systems design and has proposed a high level solution by introducing a way of integrating security design at the level of business process models. This approach should help to make key security aspects part of the overall process and architecture design and should contribute to raising the necessary awareness for security requirements at a corporate level. By clearly identifying security needs at a process rather than only at a system level, a more realistic appreciation of requirements from a purely functional angle becomes possible for management. This puts decision makers into a position where they have access to security requirements in a way that enables them to directly relate them to their needs.

References

ADONIS (2003). viewed 15th May 2003. <http://www.boc-eu.com/english/adonis.shtml>

Bauknecht, K, Tjoa, AM & Quirchmayr, G, (2002) (eds.), 'E-Commerce and Web Technologies,' Third International Conference, EC-Web 2002 Aix-en-Provence, France, September 2002, Proceedings published by Springer, 2002, LNCS 2455.

IT Governance Guides (2003) see publications of IT Governance Institute; 3701 Algonquin Road, Suite 1010; Rolling Meadows, IL 60008 USA; Web: www.ITgovernance.org.

Karagiannis, D, Junginger, S & Strobl R, (1996) Introduction to Business Process Management Systems Concepts, in Scholz-Reiter, B, Stickel, E. (Eds.), Business Process Modelling, Springer, ISBN 3-540-61707-8, pp. 81-106.

OCTAVE (2003) viewed January 3rd 2003. <http://www.cert.org/octave/>

Quirchmayr, G, & Slay, S, (2001). 'A BPR-Based Architecture for Changing Corporate Approaches to Security', in Proceedings of the 5th Australian Security Research Symposium, 11 July 2001, Perth.

Traunmüller, R, (2002). (ed.), 'Information Systems – The e-Business Challenge' IFIP 17th World Computer Congress – TC8 Stream on Information Systems: The e-Business Challenge, August 25-30, 2002, Montréal, Québec, Canada, Proceedings published by Kluwer Academic Publishers.

Whitehacker (2003), viewed January 3rd 2003. <http://www.thewhitehacker.com>