2004

# Business Process Re-engineering and Information Security Planning: Opportunities for integration

Omar F. El-Gayar
*Dakota State University*

Brian D. Fritz
*Dakota State University*

## Recommended Citation

El-Gayar, O. F., & Brian, F. (2004). Business Process Re-engineering and Information Security Planning: Opportunities for integration. 8th World Multi-Conference on Systemics, Cybernetics and Informatics.

# Business Process Re-engineering and Information Security Planning: Opportunities for integration

**Omar F. EL-GAYAR**
**College of Business and Information Systems, Dakota State University**
**Madison, SD 57042, U.S.A.**
**omar.el-gayar@dsu.edu**

**Brian D. FRITZ**
**College of Business and Information Systems, Dakota State University**
**Madison, SD 57042, U.S.A.**
**fritzb@pluto.dsu.edu**

## ABSTRACT

Business process re-engineering (BPR) has come to recognize a need for the adoption of socio-technical methodologies and capabilities for knowledge representation of qualitative concerns. Security planning and decision-making has a similar need, and furthermore socio-technical methods common to BPR can be usefully applied in this capacity.

The introduction of security models like Defense-in-Depth and similar efforts to recognize the organizational impact of security planning in operational security management serve as an initial step in educating security personnel and provide a more comprehensive view, but unfortunately, security decision-making has traditionally relied almost solely upon quantitative risk assessment, cost/benefit mechanisms, and related, functionalistic methodologies. This greatly limits the representational capacity of the decision process, and with it the possible dimensions of analysis in which to consider security issues.

Within this paper, we briefly examine security planning and the relevant techniques of BPR and Socio-technical design, and present a framework for their integration within the context of information security. It is our contention that such methodologies can be utilized in the security decision process to facilitate representation of subjective concerns and broadly-defined issues germane to security policy, within an organizational context.

**Keywords:** Security management, Security planning; Security processes; Business process reengineering; Socio-technical modeling

## 1. INTRODUCTION

The shift towards a more holistic view of information security as an organizational concern would necessitate security management methodologies capable of incorporating and representing a broader perspective than has been the case [1]. Such a shift, in essence necessitated by the rapid change of technology and the emergence of new organizational structures, has brought certain classical assumptions central to traditional security theory into question. Specifically, the phenomena of distributed systems and decentralization, such as that evidenced by the widespread Peer-to-peer (P2P) applications, facilitate radically different computing architectures than traditional security approaches are designed to account for [2]. Additionally, the changes represented by methodologies like business process re-engineering (BPR), which advocates transformational use of IT [3] and radical restructuring of the firm, have fundamentally altered the structures of many organizations. In essence, the majority of the assumptions underlying traditional security theory have been and are being substantially altered by new technologies and process-oriented orientations to business.

We note additionally that information systems implementation can cause deliberate or unintentional modification of business processes [4], and this can result in social and psychological repercussions within the organization. In the modern business environment, the need exists for access by as well as interaction with trusted intranet as well as extranet systems, a need which explicitly violates a more traditional closed-system conception assumed by the classic security paradigm [5]. The emerging perspective on such organizations and their information systems, operating within such a complex environment, must be one of open systems, as defined in [6].

These changes in our awareness of information security necessitate new approaches and revisions to our awareness of organizational security. If we truly recognize a view which goes beyond the functional problems of threat mitigation, we gain an expanded perspective for our analysis efforts, and lose nothing in return. Socio-technical methods which are capable of representing social context, motives, and emergent organizational concerns can be employed in business process redesign and reengineering efforts to mitigate the effects of radical change and decrease resistance [7]. It is our contention that similar methods can and should be utilized explicitly in the security decision process to facilitate a holistic representation of subjective concerns and broadly-defined issues germane to security management and planning, within an organizational context. Within this paper, we briefly examine security planning and the relevant techniques of BPR and socio-technical theory, and present a framework for their integration within the context of information security.

## 2. SECURITY PLANNING AND MANAGEMENT

Traditional security methodologies have been characterized as functionalistic and even technocratic [8]. The prevailing paradigm of information security evolved under radically different assumptions [5] about both the nature of organizations and technology than the modern IT environment presents – large, centralized, dedicated computing power (i.e. mainframes) and batch processing, strict task-oriented, hierarchal power structures, and closed systems. Early conceptions, inherently functionalistic in nature, [9] including the access control matrix [10] and [11] models, and the information security notions of the so-called "Orange Book" [12] – Confidentiality, Integrity, and Availability, constituted this paradigm [5], with "Confidentiality" as the historical focus for information security. Decentralization and web-based technologies, widespread use of redundant and fail-over systems, and the growing concern with business continuity planning (BCP) in information security suggest that Integrity and Availability are increasingly coming into greater focus.

Information security awareness is multi-dimensional, often non-technical in nature and trans-organizational in scope of importance [13]. The controlled governmental and business environment's managed information flow from "high" to "low" has historically been essential to the preservation of Confidentiality, [9] as the primary concern of information security. However, public awareness of security concerns and the publicity accorded by the media to potential vulnerabilities across organizational barriers to a certain extent violates this constraint, again resulting in an open system. Such concerns must inherently affect the security management of an organization.

The introduction of security models like Defense-in-Depth and related efforts by institutions like the International Standards Organization (ISO), and International Information Systems Security Certification Consortium (ISC)$^2$ to promote information security awareness serve as an initial step in educating security personnel and provide a more comprehensive and holistic view of organizational security. Unfortunately, security decision-making and risk assessment has traditionally relied almost solely upon the traditional managerial techniques of quantitative risk assessment, e.g., Actualized Loss Expectancy [14], cost/benefit mechanisms, and related methodologies. We have elsewhere argued that truly multi-dimensional security planning needs to incorporate qualitative concerns and multiple stakeholder perspectives, and to illustrate trade-offs explicitly in the security decision process [15].

## 3. RE-ENGINEERING AND SOCIO-TECHNICAL METHODS

### Business Process Reengineering

Business Process Reengineering (BPR), a methodology which achieved wide-scale popularity as a management tool in the 1990's [16, 17], is a process-oriented form of organizational redesign which aims at making radical changes to an organization to gain large-scale increases in productivity. The methodology involves a holistic analysis of the organization oriented around the customer processes' perspective, and the delineation of specific inputs and outputs to the various value-creating processes. BPR favors the elimination of bureaucracy as a natural consequence of reorganization and recombination of tasks and lends itself towards flattening power structures [18]. The combination of these qualities suggest that BPR techniques may possess high synergy with a multidimensional conceptualization of information security awareness.

BPR, at its inception, was never claimed by its authors to be an original technique, i.e., [16] nor a comprehensive methodology. The originators deliberately refrained from constraining the methodology to a systematic collection of techniques. It is thus not altogether surprising that BPR has been identified and criticized variously as being originally void of a methodology [19], a neo-Taylorist movement [17], and a management fad [20]. "Real" BPR has come to be characterized as essentially a top-down approach to organizational process restructuring intended to achieve measurable large-scale performance gains [21] by refocusing business processes around process customers and reintegrating task-based work into a process perspective.

Identified unique characteristics of the movement, common between various interpretations are:

- The consistent notion of its being focused on "radical" [22] changes, as opposed to incremental improvement methodologies like TQM [16, 23].
- The stance taken towards IT as a key enabler of the revolutionary change to be wrought through re-engineering [3].

BPR has been widely implemented, and in some cases used to great success, but high failure rates of 40 to 70 percent reported by organizations [24] seem to suggest that there are deep roots to this problem. Several BPR pioneers themselves hold the primary cause of organizational BPR failure to be the lack of accounting for the sociopolitical dimension [25, 26].

**Socio-technical Theory and BPR**

Socio-technical theory holds that there is inherent interdependent relation between people and technology [19]. Sociotechnical approaches to systems development were pioneered in the 1970's and 80's [27], as an incorporation of more organizational and behavioral approaches to change management. Conceptualizing an organization as a set of business processes bears great similarity to notions of a social organization as a collection of interacting open systems [7], common to Organizational Development (OD) theory.

Why should we concern ourselves with a socio-technical "soft-systems" approach at all? An organization which changes the logistics of workflow but fails to facilitate change to the organizational realities becomes highly susceptible to failure, unexpected delays, worker frustration, and even sabotage of the new process [18]. Resistance to change in general assuredly occurs when the resulting situation created by change is perceived as a threat to an individual's security or stability [28]. Additionally, installation and implementation of an information system can itself result in an unintentional or intentional "re-designing" of the business processes in which it is embedded [4] as well as reactionary behavior as the organization adapts to the change. Insofar as both people and technology are fundamental to the whole of an organization, the social and psychological impact of new technology and process redesign upon the existing sociopolitical climate and organizational roles must be taken into account. This is the fundamental insight which socio-technical design offers us.

The incorporation of socio-technical theory into BPR is based upon the realization that many of the ideas associated with the techniques of BPR – process-based thinking, radical change, and transformative use of IT – are compatible with socio-technical analysis, when divorced from a purely Taylorist bias, such as was espoused by some early BPR advocates [29]. Pairing these fundamental concepts with the recognition of a need for integration between human and technology issues in the changes to be wrought [7, 30], we can see how a dialogue for the consideration of socio-technical design ideas in BPR could be created. Unfortunately, early efforts in this direction minimized the organizational political issues or viewed them simply as problems standing in the way of implementing effective control structures [7]. Socio-technical modeling treats these "fuzzy" issues as design requirements not altogether different from more objective criteria and goals.

A fundamental need unique to socio-technical modeling is the representation of organizational concerns – not merely the concerns of engineering the design (*what* occurs in a process, and *how* can we make it occur), but also those of motive (*why* does it occur in the first place?). Processes, problems and concerns must be seen within their social and psychological contexts. These concerns are inherently different from those of engineering and design – they are predominantly qualitative and subjective issues and perceptions held by multiple people within a given organization. Relevant techniques for the explicit inclusion of goal hierarchies in business modeling for IS design have been explored, i.e., [31], as have social representation frameworks for modeling [18] but not specifically in relation to security management.

## 4. OPPORTUNITIES FOR INTEGRATION

Certain commonalities can be seen to exist between the areas discussed in the previous sections. We recognize that the commonality of a process-focused perspective exists between BPR and socio-technical design. It naturally follows that if it is possible to conceive of a security process at all, it should be equally possible to re-engineer the process thus conceived. Changing business processes requires mutual adaptation by structures, processes, people, and technology to accommodate one another [32] in the new environment. This insight suggests the possibility of an integrative framework for change.

The dilemma faced by information security is this: if we accept, a priori, a purely functionalist definition of security, we admit essentially that security consists of the ascertainment of threats, and the mitigation of these threats by the application of various control measures. This simplistic notion is not incompatible with socio-technical theory, nor with any expanded view of security. In fact, it illustrates a meta-problem in that by applying a control, we are actually changing the nature of the security environment, and if we do not take this explicitly into account, we simply create a vicious reactionary cycle through the process of control implementation. Figure 1 presents the basic framework of security management based on the key areas: People, Technology, and Process, derived from the Defense in Depth model standards for security management.

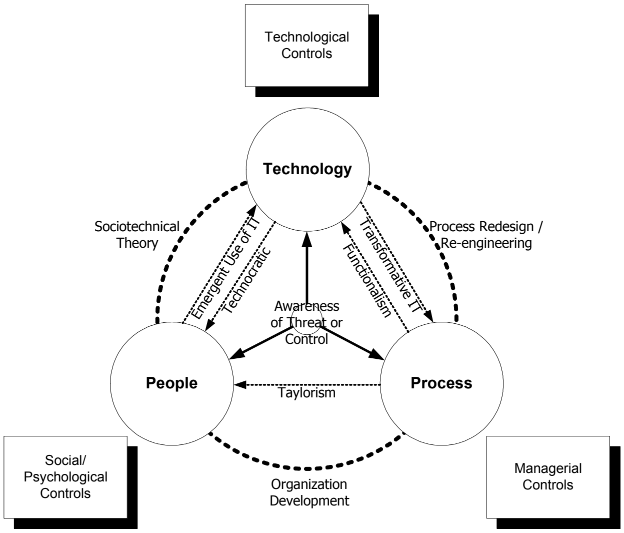

Figure 1. A framework of integrating BPR, socio-technical theory in information security.

We now briefly describe the various components of the framework presented.

The foundational components can be defined as follows:

- ***People***: Within the context of this framework, this refers to the individuals within the organization, and the formal as well as informal relationships and social hierarchies which exist within the organization.
- ***Technology***: We've used this broad term to refer to the whole of the organizational information technology infrastructure. In security terms, we are thus concerned with the IT infrastructure and computing environment.
- ***Process***: This refers to the business processes as well as formally-organized hierarchies which exist within the organization. It includes the whole corpus of organizational policy and legal agreements as well as formal literature, operations manuals, and the like.

At the center of the framework, "Awareness of Threat or Control" is a self-explanatory definition, but how it impacts the model must be explained. We are considering the perception, or awareness, of a threat (for example, a public warning of an upcoming worm, or news of an actual security breach within the organization), as eliciting a response from each of the base components (People, Technology, and Process). Similarly, the implementation of a control impacts organizational awareness and may have social/psychological as well as technical consequences, or provoke a managerial response.

We turn next to the three sets of controls: Technological, Managerial, and Social/Psychological.

- ***Technological controls*** are well-understood and the primary subject of traditional information security – physical controls which mitigate against physical threats (for example, a network firewall, or even a low-tech safe).
- ***Managerial controls*** are the policies and executive fiat which can alter the organization's formal political structure. These controls protect at the legal level, and may include, for example, a nondisclosure agreement, an access control policy, or a directive for a total shutdown.
- ***Social/Psychological controls*** are slightly more difficult to define – the idea of such a control originates from behavioral control theory. In essence, they comprise the social norms, organizational awareness and education, and incentive systems which shape and influence but do not necessarily compel desired behaviors.

We have included several one-way processes within the model that characterize several of the more narrowly focused methodologies discussed briefly within this paper, namely,

- ***Taylorism*** is a one-way flow from Process to People, such that organizational restructuring is simply imposed upon the existing social organization.
- ***Functionalism*** is next identified as a one-way relation, where organizational processes make demands on technology without regard for either the existing technological infrastructure or concern for the effect such implementations on the people within the organization.
- ***Technocratic*** bias is described as the imposition of technological constraints on the social order without concern for its potential repercussions.
- ***Transformational use of IT*** within an organization (the innovative utilization of IT as a key part of long-term strategy) can itself be the cause or inspiration for process redefinition based on inherent capabilities of the technology.
- ***Emergent use of IT*** is occasioned when social group interaction results in innovative use of IT which were outside the original intended purpose of that technology and expands its utility.

The applied knowledge of Process Re-engineering, Socio-technical Theory and Organizational Development are represented as bidirectional relationships between the foundational components. Process Re-engineering relates Process and Technology, Socio-technical Theory connects People and Technology, and Organizational Development relates People and Process. These three disciplines form a larger body of knowledge which forms the integral framework for security management.

Within this framework, then, knowledge of business process re-engineering, socio-technical theory, and organizational development become amenable to security management as mediators between the three fundamental components of People, Technology, and Process. Ideally, this presents a more holistic perspective and broadly suggests developed fields of study within the literature which can facilitate adherence to this framework. This is certainly not to suggest that any individual might have mastery of these various subject matter, only that basic concepts and techniques from these areas of knowledge could be adapted to facilitate a broader understanding of security management in relation to an organization.

## 5. CONCLUSION

This paper takes a preliminary step towards a truly integrated conceptualization of information security awareness as a multidimensional concern. We broadly sketch the relevant areas of knowledge which seem appropriate and even natural to such an integration and discuss briefly the limitations of more specialized and focused approaches. We then present a conceptual framework for integration that visually demonstrates the relationships implicit between the elements from a perspective of security awareness.

## 6. REFERENCES

1. Eloff, J. and M. Eloff. *Information security management - a new paradigm*. in *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*. 2003.
2. Lipson, H.F. and D.A. Fisher. *Survivability - A new technical and business perspective on security*. in *Proceedings of the 1999 New Security Paradigms Workshop, New York*. 1999.
3. Hammer, M., *Reengineering work: Don't automate, obliterate.* Harvard Business Review, 1990(July-August): p. 104-112.
4. Orlikowski, W.J., *Improvising organization transformation over time: A situated change perspective.* Information Systems Research, 1996. **7**(1): p. 63-92.
5. Greenwald, S.J. *Discussion Topic: What is the old security paradigm?* in *Proceedings of the New Security Paradigms Workshop, Charlottesville, Virginia*. 1998.
6. Ashby, W.R., *Introduction to Cybernetics*. 1964: Routledge Kegan & Paul.
7. Biazzo, S., *Process mapping techniques and organisational analysis: lessons from sociotechnical system theory.* Business Process Management Journal, 2002. **8**(1): p. 42-52.
8. Willison, R. and J. Backhouse. *Understanding Criminal Opportunity in the IS Context*. in *IRIS*. 2003. Finland.
9. Nelson, R. *What is a secret—and—what does that have to do with computer security?* in *Proceedings of the 1994 workshop on New security paradigms*. 1994. Little Compton, Rhode Island, United States.
10. Lampson, B.W. *Protection*. in *Proceedings of the 5th Princeton Symposium on Information Sciences and Systems*. 1971. Princeton, New Jersey.
11. Bell, D.E. and L.J. LaPadula, *Secure computer system: Unified exposition and multics interpretation*. 1976, Technical Report MTR-2997, The MITRE Corporation, Bedford, Massachusetts.
12. *Department of Defense Trusted Computer System Evaluation Criteria*. DoD 5200.28-STD. National Computer Security Center, Department of Defense Computer Security Center ed. 1985: Department of Defense.
13. Siponen, M.T., *Five dimensions of information security awareness.* ACM SIGCAS Computers and Society, 2001. **31**(2): p. 24-29.
14. Courtney, R. *Security risk assessment in electronic data processing*. in *AFIPS Conference Proceedings of the National Computer Conference*. 1977. Arlington, VA.
15. El-Gayar, O.F. and B.D. Fritz. *A framework for decision support in information systems security*. in *Proceedings of the Tenth Americas Conference on Information Systems*. 2004. New York.
16. Hammer, M. and J. Champy, *Reengineering the Corporation*. 1993: Harper Business, New York.
17. Davenport, T., *Process innovation*. 1993: Harvard Business School Press, Boston, MA.
18. Katzenstein, G. and F.J. Lerch, *Beneath the surface of organizational processes: a social representation framework for business process redesign.* ACM Transactions on Information Systems (TOIS), 2000. **18**(4): p. 383-422.
19. Mumford, E. and R. Hendricks, *Reengineering Rhetoric and Reality: the rise and fall of a management fashion*. 1996.
20. Mumford, E., *Systems Design: Ethical tools for ethical change*. 1996: Macmillar Basingstoke.
21. Tinaikar, R., A. Hartman, and e. al., *Rethinking business process re-engineering: a social constructionist perspective.* Examining business process re-engineering : current perspectives and research directions, London, Kogan, 1995: p. 107-116.
22. Dixon, J., et al., *Business Process Reengineering: improving in new strategic directions.* California Management Review, Summer, 1994: p. 93-108.

23. Davenport, T. and J. Short, *The new industrial engineering information technology and business process redesign.* Sloan Management Review, Summer, 1990: p. 11-27.
24. Hammer, M. and S.A. Stanton, *The Reengineering Revolution*. 1995: Harper Business, New York.
25. Davenport, T., *The fad that forgot people.* Fast Company, 1995. **1**(1): p. 70.
26. Hammer, M., *Beyond Reengineering: How the process-centered organization is changing our work and our lives*. 1996: London: Harper Collins (paperback version London: Harper Collins Business).
27. Lin, A. and T. Cornford, *Sociotechnical Perspectives on Emergence Phenomena*. 2000, Department of Information Systems London School of Economics and Political Science.
28. Watson, G., *Resistance to change*. 1969: In W. G. Bennis, K. D. Benne, and R. Chan (Eds.), In the planning of change. New York: Holt, Rinehart & Winston.
29. Scarbrough, H., *BPRC Focus Group: The Relevance and Contribution of Socio technical Systems*. 1997.
30. Ahmed, P.K. and A.C. Simintiras, *Conceptualizing business process re-engineering.* Business Process Re-engineering and Management Journal, 1996. **2**(2): p. 73-92.
31. Jacobs, S. and R. Holten. *Goal driven business modelling: supporting decision making within information systems development*. in *Proceedings of conference on Organizational computing systems*. 1995. Milpitas, California, United States.
32. Leavitt, H.J., *Applied organizational change in industry: structural, technological and humanistic approaches.* Handbook of Organizations, Rand McNally, Chicago, IL, 1965: p. 1144-70.