Secure Business Process Management: A Roadmap

Thomas Neubauer, Markus Klemen, Stefan Biffl
Institute of Software Technology and Interactive Systems
Vienna University of Technology, Austria
Email: {neubauer, klemen}@securityresearch.at, biffl@ifs.tuwien.ac.at

***Abstract*— The security of corporate business processes is crucial for the business success of companies. Existing Business Process Management methodologies barely consider security and dependability objectives. Business processes and security issues are developed separately and often do not follow the same strategy. Growing business integration and legal requirements raise the need for secure business processes as security problems negatively affect profit and reputation of companies and their stakeholders. In this paper we summarize the state of the art of business process management and security and identify shortcomings of existing approaches. Based on that we identify research challenges and present a roadmap for Secure Business Process Management (SBPM) that allows an integrated view on business process management and security. This approach provides top management in process oriented enterprises with a stepwise methodology for the parallel and continuous development and improvement of business processes along with security issues over the whole business process life cycle.**

I. Introduction

In many domains companies model and optimize their business processes to better manage the external value that comes from these business processes [1]. While business process management (BPM) aims at efficiently creating business value there is a number of threats that process managers need to consider. Security hazards such as viruses, hacker attacks or data theft pose major threats to the reliable execution of business processes and may have negative effects on company value, e.g. on profit, shareholder value or reputation [2], [3]. This effect is enforced with the growing integration between companies through interorganizational business processes and the resulting openness and distribution as security breaches of one company negatively affect company value of all stakeholders. In the last years BPM became a fixed part and success factor of enterprises [4]. The reasons for this development are manifold:

- The success of B2B and B2C that lead to integrated processes between companies.
- The growing cost pressure on companies especially after the financial crisis of year 2000.
- The change in customer behavior resulting in demand for more individual products (mass customization) and therefore shorter product life cycles.
- The need for transparent processes and continuous monitoring to fulfill the demands made by regulations such as the Sarbanes-Oxley or Gramm-Leach-Bliley Act.

As a result of the growing support of core businesses with IT-Systems the significance of security aspects especially in e-business applications is ever increasing. Most companies (80%: [1], [5]) already support the majority of their processes with IT-Systems. Thus, the security of business processes is crucial for the business success of an enterprise. Skepticism of customers about the security of business processes of a company would nullify the potential advantages of BPM such as the realization of faster or cheaper services. Therefore companies are continously increasing their resources to protect their business processes against security threats. Companies generally spend a lot of money on security - the worldwide total revenue for security product and service vendors should increase to $21,1 billion by 2005 - but neglect the definition of holistic security safeguards [6]. Recent virus attacks showed the vulnerability of professional e-business environments, e.g. the economic impact of the Love Bug virus is estimated to amount $8.7 billion [7]. Additionally the attacks of hackers may have major economic impact on companies. On the one hand because of costs for theft, for recovery and for loss of business value. On the other side because of loss of reputation and confidence. However, many companies are not aware of their spending on security and even more important if the investments into security are effective. Costs for hardware and software can normally be identified quite easily because they are tied to the IT department. The identification of security costs is more difficult when processes or people must be considered in the cost-benefit calculation [5]. Costs for the recovery after a security breach or for the downtime of a system or a value chain due to security problems are often not considered because the data is not available or the costs for providing this information would be too high. The definition of security safeguards is often a result of current needs or influenced by security problems that may go public. In addition decision makers are often driven by fear when defining security safeguards. As a consequence security decisions provide only punctual solutions and are made without considering the costs and benefits of introducing theses measures.

Process managers have to model and assess processes to assure these processes fit the security need of the company or value chain. Their challenge is the elicitation of optimal business processes according to the given business strategy. Generally process managers are not security experts and neglect the integration of security safeguards to the process models. Analyzing, planning and implementing security environments are subject to the security departments or the CSO, because security is an area that demands specialist knowledge [8]. As

Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)
0-7695-2567-9/06 $20.00 © 2006 IEEE

a result security departments are rather isolated from other corporate core areas [9]. Therefore integrated methodologies for supporting companies in defining security safeguards over the whole business process life cycle are also rare. Existing approaches focus on parts of the life cycle and focus either solely on BPM or security.

In this paper we extend existing business process life cycle methodologies to allow the parallel definition and continuous improvement of business processes along with security objectives. Therefore we define Secure Business Process Management that integrates security objectives in the BPM life cycle. Surprisingly existing BPM methodologies neglect the connection of business processes and security issues. The proposed framework allows the integrated Planning, Valuation, Selection and Continuous Improvement of security safeguards along with business processes. Therefore we present methods that allow the valuation and selection of an optimal set of security safeguards based on corporate business processes according to multiple objectives and under resource constraints. The definition of a procedure model for the integration of security safeguards to business process methodologies allows reducing the gap between IT security and business. It allows improving transparency and security awareness of employees. One of the main aspects when defining security safeguards is the definition of an optimal security level according to the requirements given by the business processes (e.g. the potential loss of business value when the execution of a process is stopped due to security problems) and the costs for security safeguards. Security per se does not provide business value but investment in higher security levels typically reduces the risk of loss of business value.

II. Overview of Research in Security and Business Process Management

In the last ten years several methodologies [10], [11], [12], [13], [14], [15], [42] for BPM have been proposed. These models support users in managing business processes over their whole life cycle. Generally this life cycle comprises analyzing, optimizing and modeling business processes, executing them with workflow tools and monitoring operational data during the execution. Some methodologies also consider the corporate strategy for defining business processes and deriving operational goals. Most of these models focus on the continuous improvement of business processes. Although the procedures and components of BPM methodologies are quite similar, the definitions of BPM are still quite inconsistent [16]. Some of the reasons can be found in the shift from business reengineering to BPM. The 90ies were dominated by Hammer and Champy [17] and their fundamental reengineering approach. In the last years the focus lies on continuous BPM that supports the whole business process life cycle. This includes the improvement of agility to allow a fast reaction to changing markets as well as interorganizational process management. As a result of inconsistent definitions tools for supporting BPM provide different spectrums of functionality [46]. Still many tools labeled as BPM tools consider only single phases of the business process life cycle such as business process modeling.

However, existing methodologies have in common that they neglect security objectives. Efficient business processes are a major reason for business success. As the acceptance and therefore the success of business processes heavily depend on their security the integration of security objectives to BPM methodologies is crucial. Although security is considered being on of the most important issues in corporate environments [1], work on integrating security objectives to BPM is very rare [18]. Some attempts of integrating security into BPM have been made but the proposed approaches provide partial solutions. Existing literature mainly concentrates only on parts of the business process life cycle. First attempts of integrating IT security and business were made by Thorne [19]. He describes the relationship between business and security as following: *"...business managers are not interested in IT security and tend to pay lip service to it, IT security is seen as an expense that brings little tangible benefit, IT security obliges employees to spend time and money on activities that add no value to the business, IT security is about technical issues, not mainstream business activities, IT security people are seen as apart of the management team, the concepts of IT security are not expressed in ways business people can relate to."* Although potential security threats have multiplied with the rise of the Internet and E-Commerce the value of implementing security safeguards is still not transparent to many decision makers. On reason is the lack of appropriate methods for the valuation of IT security. Existing methods - described later on - neglect the realistic connection of security costs and business value. As a result of the gap between business and IT-security the development of holistic methodologies - that e.g. integrate security to the business process life cycle - is at the beginning of its development. The lack of transparency is a result of missing methods that business people understand. The integration of security safeguards to business process methodologies is a first step towards reducing the gap between IT security and business. It allows improving transparency and security awareness of employees because people are in contact with security requirements while executing their business processes.

Herrmann [18] proposes reengineering of businesses processes according to security and integrity. This approach focuses on the description of security safeguards at a high abstraction level. Other publications by Herrmann, Pernul and Roehm [20], [21], [22] concentrate on modeling security semantics of business processes. They argue that security requirements vary with the view taken and therefore define four different perspectives. With ALMOST they presented a framework for modeling secure business transactions using a specification language. Knorr and Roehrig [23] present the framework POSeM for analyzing security requirements of business processes in e-commerce. They use business process descriptions for deriving appropriate security safeguards. Therefore security levels are assigned to the components of a business process e.g. actors, artifacts or activities. A specific description language allows mapping security objectives to safeguards.

Backes [24] presents an approach for integrating security requirements to the development of business processes. This methodology emphasizes on incorporating cryptography in the development process of business processes. The main focus of literature lies on integrating security objectives to workflow management. Many approaches are trying to adapt existing access control and authorization from operating or database systems to the need of business process and especially workflow management. These approaches show that security is mainly a technical issue. Atluri [25] points out that most commercial workflow systems neglect security features such as authentication. He describes security requirements that have to be considered for building secure workflow systems. Kindler [26] describes access control in workflow management systems and focuses on integrating security safeguards to existing workflow systems. Karagiannis and Heidenfeld [27] propose "security workflows". Security workflows are a combination of business processes and security processes that implement security functionality. By reusing the security processes work for modeling can be reduced. Knorr [28] presents a prototype for graphical modeling and analyzing separation of duties in workflow environments. He uses Petri net workflows to specify different kinds of access control mechanisms. This tool can be used by security officers for designing and analyzing security rules of workflow specifications. Ribeiro [29] presents an analyzer for automatically verifying the consistency between workflow specifications and organizational security policies. Workflow processes are described with the Workflow Process Description Language (WPDL), security policies with the use of a specific Security Policy Language (SPL) that allows expressing permission, prohibition or special forms of obligation. This approach focuses on the formal definition of an access control policy. A detailed overview of current research regarding security of workflow systems is given by Barthelmess [5].

Definitions for security and dependability are provided by Avizienis [40]. Existing security frameworks (such as Cobit [44], the German IT Baseline Protection Manual (GITBPM) [36], ISO 17799:2000 [45]) offer requirements and guidelines for defined security levels. They allow an assessment of security deficits and the identification of appropriate security safeguards. Cobit generally considers business objectives but does not provide specific methods for parallel development of business and security issues. Other frameworks for the assessment and improvement of security are maturity models defined in analogy to the Capability Maturity Model (CMM) and ISO Spice: Systems security engineering-capability maturity model (SSE-CMM); Information security program maturity grid (ISPMG) [30]; Software security metrics (SSM) [31]; Fraunhofer Security Maturity Model (SMM) [32]. Some methods for the valuation of security investments have been proposed. One of the first methods for performing risk analysis was Annual Loss Expectancy (ALE) [33]. Limitations of ALE are the "lack of empirical data on frequency of occurrence of impacts and the related consequences" [43] but also the assumption that all security breaches have the same cost implications. Another technique for measuring the net social value of measures or programs is Cost-Benefit analysis (CBA) [34]. A short evaluation of current methods including ICAMP (Incident Cost Analysis Modeling Project), internal rate of return (IRR) and maximum net present value (NPV) can be found in Mercuri [35]. All these frameworks do not consider the external business value of reaching a defined security level. The valuation models need a framework for defining security levels as context for their application. In the field of security some methods and frameworks for the definition and improvement of security have been proposed. However, many companies do not use these methods although most companies are of the opinion that security is of major importance [[1]. The main reasons for this attitude are the following:

- The benefits of preventive investments into security are not transparent and cannot be measured. Therefore security investments are often a first approach to cost cutting because they do not directly improve the net profit. Investments are mostly made after security breaches but then in a precipitant and punctual way.
- Existing security frameworks such as the German IT Baseline Protection Manual [36] with more than 1700 pages are too large for a fast implementation and too inflexible for fast changes. This is especially true for small and medium enterprises (SME) [41].
- With the introduction of security frameworks new methods and models have to be implemented. Beside direct costs for implementation this results in additional costs for staff or maintenance. In addition employees but also decision makers are mostly skeptical against new methods.

III. Definition of a Roadmap for Secure Business Process Management

Many different and inconsistent definitions of BPM have been proposed so far. Most of the current definitions have in common that they support the whole life cycle of a businesses process and enable continuous improvement. Based on existing definitions for BPM [37], [38], [39] and security [40] we define the term "Secure Business Process Management" (SBPM) as following: The management of the whole business process life cycle in conformity with security and dependability objectives: Confidentiality, Integrity, Availability, Reliability, Safety and Maintainability. The business process life cycle comprises analyzing, optimizing and designing the business process in accordance with the business strategy, allocating applications and employees, implementing and executing the processes to support information exchange, monitoring and aggregating operational data for the purpose of decision making and continuous improvement. Based on this definition we define a roadmap for Secure Business Process Management.

Figure 1 shows the roadmap, its intermediate outcomes and the dependencies between these outcomes. The most important outcomes are described in detail in the following sections. The major goal of this roadmap is the definition of methods that are combined to a methodology for supporting process oriented

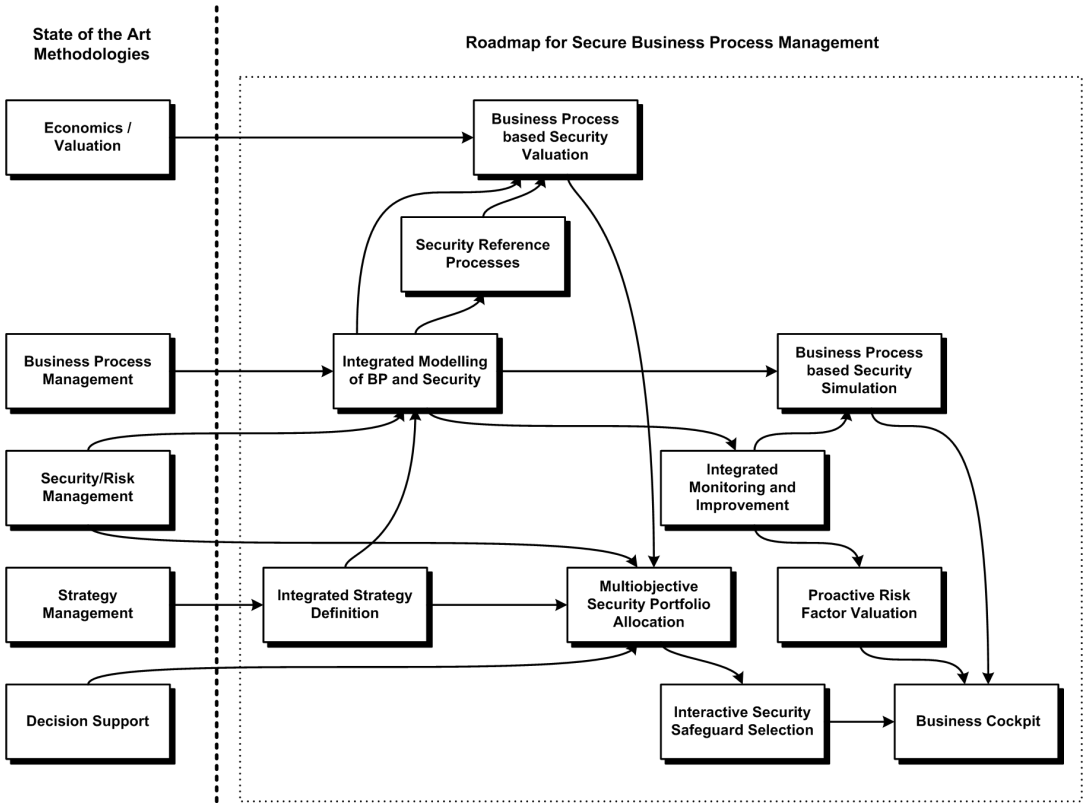

Fig. 1. Roadmap for Secure Business Process Management

companies in defining optimal security safeguards according to the security needs of their business processes. Concentrating on the security needs of business processes means a reduction of complexity and allows a more specific definition of security safeguards. The proposed approach extends existing BPM methodologies regarding the following aspects:

- Parallel development of business processes and security safeguards over the whole life cycle of a process.
- Valuation and allocation of security safeguards according to the need defined by the existing business processes. In this context we define security safeguards as specific actions for reaching security objectives. Security safeguards can be hardware (e.g. firewall), software (e.g. virus scan), organizational aspects or processes to implement or maintain the security environment (e.g. server installation, server maintenance, log file analysis).
- Consideration of interdependencies between business processes and security safeguards, e.g. regarding the potential reduction of process performance due to the implementation of multiple security safeguards.
- Continuous monitoring, optimization and improvement of business processes along with security safeguards, e.g. rates of occurrence of security breaches are monitored and used as a basis for re-valuation.

A. Strategy Definition

Current literature in the field of security as well as conference schedules show that security continues being dominated by technical issues [39]. Most companies today make security investments decision in an economic-independent way. This is also shown by the fact that investments into security are part of the IT budget. In today's companies security is too important to reduce it to a technical issue. Thus, security investment decision can not be regarded independently from corporate business, its strategic alignment, business processes and people; its consideration has to start at a strategic level.

Strategic considerations play a major role in creating and identifying the value of security investments. Thus, the implementation of a holistic approach is demanded. Therefore, the first step is the definition of a strategy regarding business processes and security based on the corporate strategy. Business processes allow the transformation of the corporate strategy and its specific goals on the operational level. The definition of a security strategy according to the corporate strategy supports the frictionless execution of the corporate business processes. In this way, the benefit of security can be defined as the creation of value by granting the operational execution of the corporate strategy by the use of business processes.

Such as the corporate strategy security measures have to optimally fit the unique corporate needs. The use e.g. of

"established" approaches of other companies can only serve as a guideline. Therefore security measures have to be tailored to the company-specific set of threats, risks and assets worth protecting. Depending on the decision if the corporate strategy explicitly comprises security goals, e.g. we are/want to be the most secure bank, two approaches are differentiated:

- Security as its own strategic goal influences the definition of the business processes.
- Security is not an explicit strategic goal. Therefore business processes are generally fixed and security measures are defined according to the given business processes.

Security strategy especially comprises the definition of a security policy and a security culture. Employees are still the weakest link in the security model e.g. due to gullibility [55] but also due to bad intentions. Thus, a major focus of the corporate security policy has to lie on the people. The improvement of security awareness of employees has to be at least as important as the definition of technical security safeguards. Moreover core business processes and support processes as well as candidates for outsourcing are identified. Core business processes providing additional business value have to be selected according to the core competencies of the enterprise. Depending on the goals defined in the corporate strategy business processes that have to be optimized are selected and goals for measuring process performance are defined.

B. Security-enhanced Business Process Definition

Security measures are modeled in the same diagrams as business processes to extend the advantages of businesses process models to the field of security. Modeling of security measures allows an improvement of documentation and therefore transparency. A higher level of transparency has also influence on the security awareness because employees are directly in contact with the corporate security policy when executing their business processes. Additionally workflow systems can be aligned according to the given security requirements. This phase comprises the analysis, modeling, simulation and optimization of business processes. Existing business processes are analyzed and optimized if the efficiency of the processes can be improved. The result of this phase is a set of business processes that are optimal according to the given business strategy. As stated above, only strategic security requirements are generally considered in the first step of business process modeling. Otherwise, security measures are defined in dependence of a fixed set of business processes. In the second step after optimizing and modeling the business processes the need for implementing security measures is analyzed. Business processes have priority over the definition of security measures because they allow the realization of the strategic goals. Of course, interdependencies between business processes and security measures must be considered, especially if security measures influence the performance of the business processes and therefore affect the degree of reaching a strategic goal. For an optimal allocation of the security measures according to the needed security level of the business processes and to economic issues we propose a framework for the valuation of security measures and business processes.

After modeling the business processes the definition of an organizational structure and the allocation of employees to activities is conducted. This comprises the organizational realization of security policies and training for the employees that are in contact with the defined security measures. The use of process models for the design of the IT-processes as well as the core processes allows a common basis and therefore a better comparability of the data. We differentiate between:

- Secure Business Processes are security-enhanced business processes. Security measures and business processes are modeled in an integrated view. These models are the basis for the execution of the business processes e.g. with workflow systems.
- Security Reference Processes are based on established security frameworks such as Cobit [44] or ISO 17799 [45]. These processes describe how to reach and keep a defined security level according to the used security framework. Security Reference Processes serve as a basis for valuating the costs of implementing security measures.

The combination of these process variants with the methods defined in sections III-C and III-D supports top management, process officers (CPO) and security officers (CSO) regarding the following scenarios:

- The optimal allocation of IT-Security investments based on the given corporate business processes and resource constraints such as the security budget.
- The identification of costs of implementing a defined level of security. The basis for this calculation are the given corporate business processes and reference processes. Using reference processes we define the activities needed for implementing and maintaining a defined level of security. The reference processes can be defined according to security frameworks such as Cobit or ISO.
- The optimal allocation of security reference processes based on a defined set of given corporate business processes and reference processes.

C. Business Process based Security Valuation

Companies generally measure value in monetary value in the marketplace. The major goal of management is to maximize present value. A company creates value when it achieves an equivalent benefit with fewer dollars or creates greater benefit for comparable cost [48]. However, security is not a product; it does not generate direct profit or provide benefit to the society. Even though security generates additional business benefit, it is hard to measure the value of additional investments into security. What is the benefit of installing two firewalls of different vendors instead of installing two firewalls of the same vendor or just a single one? What are the costs of not doing? Schneier [47] stated that security is a process, not a product. If security is a process it should be handled and especially valuated in a process oriented way.

We proposed a method [49] that allows the valuation of security in combination with the given business processes. We use Security Reference Processes for measuring the costs needed for implementing and keeping a defined level of security. With these reference processes we define the processes needed e.g. for installing a server or making a backup. Each of these processes is assigned with time and cost needed for executing a specific activity of the process. Depending on the type of the process (e.g. making a backup might be a daily process) different kinds of security costs are considered:

- Investment costs for implementing a defined level of security.
- Operating costs for keeping a defined level of security.
- Recovery costs that include the time and expenses (e.g. for spare parts) needed to recover the system after a security breach.

By aggregating the costs of the needed reference processes the total costs for implementing, keeping or recovering a defined level of security. We differentiate between three security levels for defining the degree of protection that results from the application of the reference processes. A low security level increases the risk of loss of business (downtime costs) but results in lower security costs. Security incidents (e.g downtime) decline with the improvement of the security level. The sum of security costs and downtime costs (lost business value) should be minimized.

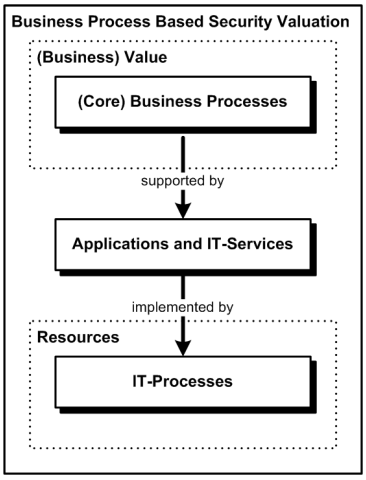

Fig. 2. Business process based Security Valuation [49]

On the other hand the value of implementing certain security safeguards or keeping a defined level of security is measured. We are using corporate business processes for measuring the potential loss of business value due to security breaches. Typical costs that we measure based on core business processes that are affected by security breaches are the following:

- Loss of profit resulting from the stop of a business process.
- Employee costs.
- Other indirect costs such as intangible costs resulting from lost customers or the loss of reputation.

The value of implementing security safeguards can be measured by using the simple method of subtracting the security investment from the prevented loss of business value. If the resulting number is positive, the Return on Security Investment (ROSI) is positive. This aggregated number may provide a guideline for judging the effectiveness of corporate security, but the use of a single aggregated number for deciding on the "optimal" security portfolio may not suffice any longer as economic and legal requirements force top management to pay more attention to security issues. Therefore, we us methods from multiobjective decision support to support decision makers in finding the trade off between security investments and the potential loss of business value when security is neglected.

D. Workshop-based Security Safeguard Selection

Traditionally project evaluation aims at characterizing security safeguard candidates with one aggregated value criterion such as the return on investment. However, (a) it is not always possible to aggregate measures from different dimensions and (b) stakeholders may vary strongly in their utility functions, i.e. their view on how much a unit of criterion A is "worth" compared to one unit of criterion B. In this situation stakeholders need better support to deal with the more complex data. Existing approaches mainly consider local problems and are not prepared in a way business people can relate to. Decision makers have to cope with a great spectrum of potential risks and the decision of selecting the most appropriate set of security safeguards. Moreover they are challenged by legal and economic requirements. The complexity of finding an optimal security level according to the given business processes is enhanced because decision makers have to deal with multiple - often opposing - objectives, the optimal allocation of given resources and different and changing preferences of multiple stakeholders.

Workshop approaches have proven to efficiently support stakeholders in decision making [52], [53]. We propose an approach [50] for combining the advantages of workshops with those of multiobjective decision support and supporting decision makers in identifying the optimal set of security safeguards according to their preferences and the given security strategy. In the context of SBPM the Workshop environment supports decision makers in assessing and valuating the corporate security environment. Existing corporate data provided by the following sources serves as the basis for the workshop:

- Analysis of the security environment by experts
- Data collected through monitoring
- Given business processes and security environment

The workshop serves as a platform for the refinement of this data. This includes the identification of assets, vulnerabilities, threats and potential safeguards. Moreover annual rates of occurrence and exposure factors are assigned to the threats and decision makers negotiate their preferences.

Compared to traditional approaches used for the selection of security safeguards our approach provides decision makers with a stepwise methodology for the assessment of security safeguards. The moderated workshop environment provides a

method for cooperatively selecting an optimal set of safeguards according to company specific objectives. The proposed approach takes into account interdependencies between security safeguards as well as resource and benefit constraints given by the stakeholders. The environment for multiple users allows the reduction of a strong influence of single opinions on the whole decision. Moreover a moderator provides advice and professional support during the workshop and therefore contributes to improving the security awareness of the participants. The clear structure and repeatability of the approach allows the application whenever decisions concerning security have to be made and money should be spent on security issues.

The final selection of an optimal portfolio is supported by an interactive graphical interface that allows the elaboration of the cost and benefits categories. The interactive selection allows decision makers to 'playfully' explore the solution space of all efficient portfolios until the decision makers find one that matches their preferences provides.

E. Monitoring and Business Cockpit

Growing integration along value chains and the execution of business processes with Workflow Systems raises the speed of execution but also demands faster detection of business or security problems. Security breaches must be identified when they occur in order to allow optimal counter measures. Newspapers are full of articles about companies being surprised of their business loss due to security breaches. Just as severe financial loss normally does not appear from one day to another, security problems mostly do not appear without any signs. Therefore monitoring serves the following purpose:

- Identification of business and security problems (in real-time) to allow an immediate definition of countermeasures (e.g. the attempt of credit card fraud should be identified in the moment it occurs and therefore demands adequate security systems).
- Continuous data collection as a basis for decision making and security safeguard selection.
- Optimization of security measures along with business processes by using data mining methods.

Operational data collected during the execution of the business processes serves as input for improving and optimizing strategy and business processes along with security measures. Business processes can be executed using Workflow Management tools or current standards such as BPEL [54]. For this purpose the business process diagram must be extended with specifications that are needed for the automated execution, e.g. the orchestration of needed applications with web services. Additionally the specified security requirements must be integrated in the workflows, e.g. role based access control, authentication or separation of duties but also classical security aspects such as securing the network against viruses. If specific applications that require software development are needed business processes along with the definition of needed security measures can serve as requirements definition.

Real-time business demands real time security. Therefore business processes as well as security measures have to fulfill the requirements of real-time concepts. Processes and methods allowing real-time processing of the available data must be available. Data (e.g. Information updates; Security messages) must be aggregated and made available to the decision makers. The aggregation and the visualization of operational data e.g by using a business cockpit allows the proactive valuation of risk factors. This enables the early identification of potential risks and the timely definition of counter measures.

IV. Conclusion

This paper defined Secure Business Process Management and presented a research roadmap for this field. This analysis is based on shortcomings of existing approaches that neglect the integration of security objectives to BPM. Based on existing shortcomings we proposed SBPM as a methodology for supporting process-oriented companies in implementing Secure Business Process Management. Therefore we provided a holistic methodology that considers all phases of the business process life cycle and extends these with methods for aligning business processes and security measures. Compared to existing approaches this allows the alignment and integrated design of business processes and security objectives over the whole life cycle of a business process. Further we extended existing approaches with methods for the valuation and allocation of security safeguards according to the given business processes. The emphasize of valuation methods lies on showing the benefits of implementing security safeguards. The presented methods for the allocation of security measures provide support for decision makers in finding the optimal selection of safeguards. Additionally the presented workshop for the assessment of security data enables the improvement of security awareness of stakeholders. The extension of existing BPM methodologies allows reducing the gap between IT-security and business activities using a combined business driven top down approach. Business processes and security issues are developed parallel and therefore synergy effects compared to an independent view on security and business processes can be realized. The integrated view on business process and the security measures enables an optimal allocation of security safeguards according to the security needs of the given business processes. Security must be as agile and flexible as the business process environment and may not lag behind. The parallel improvement allows a fast and agile adaptation of security measures to changes in the corporate strategy and the corresponding business processes.

References

[1] H. Loeffler, M. Oman, "IT-Survey 2004; KPMG Austria (Innsbruck-Linz)," 2004.

[2] K. Campbell, L. A. Gordon, M. P. Loeb, L. Zhou, "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market," *Journal of Computer Security*, vol. 11, pp. 431–448, 03 2003.

[3] M. Ettredge, V. J. Richardson, "Assessing the risk in e-commerce," *HICSS*, p. 194, 05 2002.

[4] A. Gadatsch, S. Schnaegelberger, and T. Knuppertz, "Geschaeftsprozessmanagement - Umfrage zur aktuellen Situation in Deutschland," *Schriftenreihe des Fachbereiches Wirtschaft Sankt Augustin*, vol. 9, 2004.

[5] R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. Malik, J. Pescatore, M. Reynolds, K. Russell, A. Weintraub, V. Wheatman, "The price of information security," *Gartner Strategic Analysis Report*, 2001.

[6] CSO Magazine, "E-Crime Watch Survey 2004," 2004. [Online]. Available: www.cert.org

[7] Computer Economics. [Online]. Available: www.computereconomics.com

[8] C. P. Pfleeger, "The fundamentals of information security," *IEEE Software*, vol. 14, no. 1, 1997.

[9] H. A. Gartner, P. Konrad, "Nutzung von Methoden und Instrumenten - Details zur KES-Sicherheitsstudie 1994," *KES - Zeitschrift fuer Kommunikations- und EDV Sicherheit*, vol. 2, 1995.

[10] M. Amberg, *Prozessorientierte betriebliche Informationssysteme*. Springer, 1999.

[11] D. Karagiannis, "BPMS: Business Process Management Systems," *SIGOIS Bulletin*, vol. 16, no. 1, pp. 10-13, 1995.

[12] G. Krallmann, H. Derszteler, *Workflow Management Cycle - An Integrated Approach to the Modelling, Execution and Monitoring of Workflow-Based Processes*, E. Scholz-Reiter, B.; Stickel, Ed. Springer, 1996.

[13] H. Oesterle, *Business in the Information Age. Heading for New Processes.* Springer, 1995.

[14] A.-W. Scheer, *ARIS - Vom Geschaeftsprozess zum Anwendungssystem*. Springer, 1998.

[15] A. Gadatsch, *Management von Geschaeftsprozessen*, 2nd ed. F. Vieweg&Sohn, 2002.

[16] A. Lindsay, D. Downs, K. Lunn, "Business processesattempts to find a definition," *Information and Software Technology*, vol. 45, p. 10151019, 2003.

[17] M. Hammer, J. Champy, *Reengineering the Corporation - A Manifesto for Business Revolution*. Harper, 1994.

[18] G. Herrmann, "Security and integrity requirements of business processes - analysis and approach to support their realisation," *Consortium on Advanced Information Systems Engineering*, pp. 36–47, 1999.

[19] S. Thorne, "A new vision for IT security in the 90s," *In. Bauknecht, Kurt; Teufel, Stephanie (Hrsg.): Sicherheit in Informationssystemen; Proceedings der Fachtagung SIS*, 1994.

[20] G. Herrmann, G. Pernul, "Towards security semantics in workflow management," *IEEE*, vol. 32, pp. 766-767, 1998.

[21] G. Herrmann, "Viewing business process security from different perspectives," *International Journal of Electronic Commerce*, vol. 3, no. 3, p. 89, 1999.

[22] A. W. Roehm, G. Herrmann, G. Pernul, "A language for modeling secure business transactions," *ACSAC*, vol. 15, p. 22, 1999.

[23] K. Knorr, S. Roehrig, "Security requirements of e-business processes," *IFIP Conference Proceedings*, vol. 202, pp. 73-86, 2001.

[24] M. Backes, B. Pfitzmann, M. Waidner, "Security in business process engineering," *Springer-Verlag*, p. 168183, 2003.

[25] V. Atluri, "Security for Workflow Systems," *Elsevier Science Ltd. , Information Security Technical Report*, vol. 6, no. 2, pp. 59-68, 2001.

[26] T. Kindler, T. A. Soyez, "Modelling security for integrated enterprise Workflow and Telecooperation Systems," *IEEE Fifth Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 96)*, 06 1996.

[27] D. Karagiannis, M. Heidenfeld, *Sicherheit in Informationssystemen - SIS98*. vdf Hochschulverlag AG, 1998, ch. Modellierung, Analyse und Evaluation sicherer Geschaeftsprozesse: Ein Implementierungsansatz fuer Security Workflows, pp. 223–246.

[28] K. Knorr, "Security in Petri Net Workflows," *PhD Thesis, Mathematisch-naturwissenschaftliche Fakultaet der Universitaet Zuerich*, 2001.

[29] C. Ribeiro, P. Guedes, "Verifying workflow processes against organization security policies," *IEEE*, pp. 1–2, 1999.

[30] T. Stacey, "Information security program maturity grid," *Information Systems Security*, vol. 5, no. 2, 1996.

[31] G. Murine, C. Carpenter, *Computer Security: A Global Challenge*. Elsevier Science Publisher, 1994, ch. Measuring computer system security using software security metrics.

[32] H. Kurrek, "SMM Assessing a Companys IT-Security," *ERCIM News*, vol. 49, 2002.

[33] National Institute of Standards and Technologies, "FIPS Publication (65)," 1979.

[34] M. Thompson, *Benefit-Cost Analysis for Program Evaluation*. Sage, 1980.

[35] R. T. Mercuri, "Analyzing Security Costs," *ACM*, vol. 46, no. 6, pp. 15–18, June 2003.

[36] Federal Office for Information Security (BSI), "German IT Baseline Protection Manual." [Online]. Available: www.bsi.de/english/index.htm

[37] W. M. van der Aalst, A. H. ter Hofstede, and M. Weske, "Business process management: A survey," *Springer-Verlag*, pp. 1-12, 2003.

[38] Business Process Management Initiative.[Online]. Available: www.bpmi.org

[39] Business Process Management Group. [Online]. Available: www.bpmg.org

[40] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, 2004.

[41] E. Weippl, M. Klemen, *accepted for publication: Practice and Experience in Applied Enterprise Information Assurance and Computer Security*. Idea Group, 2005, ch. Implementing IT Security for Small and Medium-Sized Enterprises.

[42] M. zur Muehlen, M. Rosemann: "Multi-Paradigm Process Management," *In: Proceedings of CAiSE'04 Workshops - 5th Workshop on Business Process Modeling, Development and Support (BPMDS 2004). Eds.: Janis Grundspenkis, Marite Kirikova, Riga, Latvia*, pp. 169-175, 2004.

[43] National Institute of Standards and Technology, "Federal information processing standards: Guideline for the analysis of local area network security; FIPS Pub 191, Nov. 1994." 1994.

[44] IACSA, "Cobit," Cobit has been developed and is maintained by the Information Systems Audit and Control Association (IACSA). [Online]. Available: www.iacsa.org

[45] "ISO 17799." [Online]. Available: www.iso-17799.com

[46] D. Kopperger, R. Naegele, and P. Schreiner, *Business Process Management Tools: Eine evaluierende Marktstudie ueber aktuelle Werkzeuge*, H.-J. Bullinger and P. Schreiner, Eds. Fraunhofer-Institut fuer Arbeitswirtschaft und Organisation IAO, Stuttgart, 2002.

[47] B. Schneier, Secrets and Lies: Digital Security in a Networked World, Wiley, 2000.

[48] M. E. Porter and M. Kramer, "Philanthropys New Agenda: Creating Value", *Harvard Business Review*, November-December, 1999.

[49] T. Neubauer, M. Klemen, and S. Biffl, "Business Process-based Valuation of IT-Security." *International Conference on Software Engineering, Proceedings of the seventh international workshop on economics-driven software engineering research, EDSER'05*, ACM, 2005.

[50] T. Neubauer, C. Stummer, and E. Weippl, "Workshop-based Multiobjective Security Safeguard Selection," *Proceedings of the First International Conference on Availability, Reliability and Security ARES 2006*, IEEE CS, 2006.

[51] F. Curbera, Y. Goland, J. Klein, F. Leymann, D. Roller, S. Thatte, S. Weerawarana: Business Process Execution Language for Web Services, Version 1.0. BEA, IBM, Microsoft, (2002)

[52] P. Gruenbacher, "EasyWinWin: Eine groupware-unterstuetzte Methode zur Erhebung und Verhandlung von Anforderungen." *Softwaretechnik-Trends*, vol. 23, no. 1, 2003.

[53] P. Gruenbacher, "Collaborative requirements negotiation with EasyWinWin", *IEEE*, pp. 954-985, 2000.

[54] "Business Process Execution Language for Web Services Version 1.1." [Online]. Available: http://www-128.ibm.com/developerworks/library/specification/ws-bpel/

[55] IBM, "Security Threats and Attack Trends Report 2005" [Online]. Available: www.ibm.com