Business Process-based Valuation of IT-Security

Thomas Neubauer, Markus Klemen, Stefan Biffl
Institute of Software Technology and Interactive Systems
Vienna University of Technology, Karlsplatz 13, A-1040, Austria
{neubauer, klemen, biffl}@ifs.tuwien.ac.at

Abstract

Growing business integration raises the need for secure business processes as security problems can affect the profit and the reputation of a company. However, decisions regarding a reasonable level of security in a business environment are often made in a value-neutral way.
This paper presents a framework for the valuation of cost-benefit of various security levels with business processes. The framework can be used for planning security levels in software development and allows further continuous monitoring and improvement of cost-benefit of security measures along with operative business processes.

Keywords: Value-Based Security; Business Process Management; Valuation of Secure Business Processes.

1. Introduction

In many domains companies model their core business processes to better manage the external value that comes from these business processes [12]. While business process modelling 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 the business processes and may have negative effects on company value, e.g. on profit, stock price, or reputation [4],[7].
Process managers (and often the CFO or CSO) have to model and assess security processes to assure these processes fit the security need of the company. Their challenge is the elicitation of the right security level according to their business processes and budget limits.

EDSER'05, May 15, 2005, St. Louis, Missouri, USA.

Security problems that may go public typically make top management react with fast decisions, often without firm data for decision support. As part of the IT-infrastructure investment into security hardware and processes is typically isolated from the development of core business processes: such a value-neutral planning neglects the value contribution of security investments.
Figure 1 shows the connection between core business processes of a company that actually generate income and IT-processes: IT-processes implement IT-applications and IT-services that in turn support execution of the core business processes.

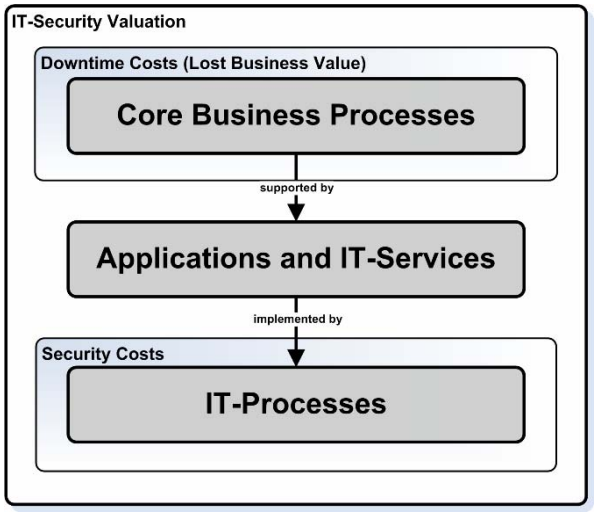

Figure 1: IT-Security valuation based on Core Business Processes and IT-Processes

Security per se does not provide business value. Investment in an appropriate security level typically reduces the risk of loss of business value. Thus the connection with business processes provides a common basis for the cost-benefit valuation of security.

In this position paper we propose to connect core business processes with IT-processes and subsequently security levels using an "IT-Security Valuation Framework". Current models and standards that define secu-

rity levels are surprisingly mostly value-neutral. This Framework allows a cost-benefit analysis based on external value of core business processes and is compatible with models that define security levels. The Framework can define value with a range of economic models such as Net Present Value, Value Chain Analysis or Return on Investment to value costs of IT-infrastructure, processes and benefit of business processes. The simplicity of this approach allows the integration to existing business process management methodologies [16]. This enables continuous optimization of security systems regarding cost-benefit along with the corresponding business processes.

2. Security models

There are several models and frameworks for the implementation and valuation of security. Important criteria for these models in the context of value-based security are:

1) Consideration of the core business processes for valuation;
2) Integration of methods for cost-benefit valuation;
3) Management view on security in comparison to a pure technical view;
4) Assessment and definition of security levels.

There are three groups of frameworks and models: Security frameworks aim at optimizing the effort needed to introduce security. Maturity models provide methods for the assessment and definition of security levels. Valuation models mainly focus on the valuation of security measure cost and neglect value issues.

Criteria	1)	2)	3)	4)
Security Frameworks				
Cobit[6]	-	-	+	+
GITBPM[9]	-	-	-	+
ISO 17799:2000[20]	-	-	+	+
Maturity Models				
SSE-CMM[18]	-	-	-	+
ISPMG[19]	-	-	-	+
SSM[14]	-	-	-	+
SMM[11]	-	-	-	+
Valuation Models				
ALE[15]	-	+	-	-
SooHoo[17]	-	+	-	-
CBA[8]	-	+	-	-

Table 1: Comparison of security models and frameworks.

Existing security frameworks (such as Cobit, the German IT Baseline Protection Manual (GITBPM), ISO 17799:2000) offer requirements and guidelines for defined security levels. They allow an assessment of security deficits and the identification of appropriate security measures. 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)
- Software security metrics (SSM)
- Security Maturity Model (SMM) Fraunhofer

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). Limitations of ALE are the "lack of empirical data on frequency of occurrence of impacts and the related consequences" [8] but also the assumption that all security breaches have the same cost implications. Another technique for measuring the net value of measures or programs is Cost-Benefit analysis (CBA) [21]. A short evaluation of current methods including ICAMP (Incident Cost Analysis Modelling Project), internal rate of return (IRR) and maximum net present value (NPV) can be found in [13]. Butler [3] uses a cost-benefit analysis method SAEM (Security Attribute Evaluation Method) to compare alternative security designs. The benefits of countermeasures and ways for risk reduction are estimated by security specialists. Multi-attribute risk assessment is used for prioritizing risks and optimizing countermeasures.

Current models have in common that they do not consider the external business value of reaching a defined security level. Valuation models need a framework for defining security levels as context for their application. Our approach uses businesses processes and IT processes as driver for cost benefit analysis: Firstly, business processes are used for measuring the potential loss of business value resulting from security breaches. With the use of IT processes the costs for implementing and maintaining a defined security level are measured. Secondly, data generated during the execution of the business processes can be used for a more accurate and company specific estimation of risk. Real time monitoring of operational data allows an immediate reaction to risk changes. Moreover, security measures are allocated based on the need of protection of the corresponding business.

3. IT-security valuation framework

The reliability of core business processes is crucial for the business success of an enterprise. These processes provide additional value to the company and the cus-

tomer who is willing to pay for that service and must be protected against security threats [1].

We suggest an "IT-Security Valuation Framework" for the valuation of security measures based on the external value of core business processes. This approach allows integrating:

- corporate (core) business processes that should be protected,
- security frameworks that allow the definition of security levels and IT-Processes,
- methods for the valuation of security.

We use the IT-processes for measuring the costs needed for implementing and keeping a defined level of security. There are different kinds of security costs that have to be 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.

On the other side downtime costs (lost business value) of a system due to unavailability must be considered (indirect/opportunity costs). These costs can be measured based on core business processes that are affected by the unavailability of the system.

- 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 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. Business process modeling tools such as Aris[10] or Adonis[2] can be used for the design, the assignment of data and the simulation of the process models.
Based on the data from the core processes and the IT-processes valuation models such as ALE can be used for calculating the expected loss and defining the optimal level of security.
In the next chapter we provide an example that shows the valuation of an optimal level of security based on a core process and the IT-processes of a call center. The optimal spending is calculated with the use of ALE. A low security level increases the risk of loss of business (downtime costs) but results in lower security costs. Downtime costs decline with the improvement of the security level. The sum of security costs and downtime costs (lost business value) achieves a minimum (grey curve) at the intersection of both dark curves (see Figure 2).

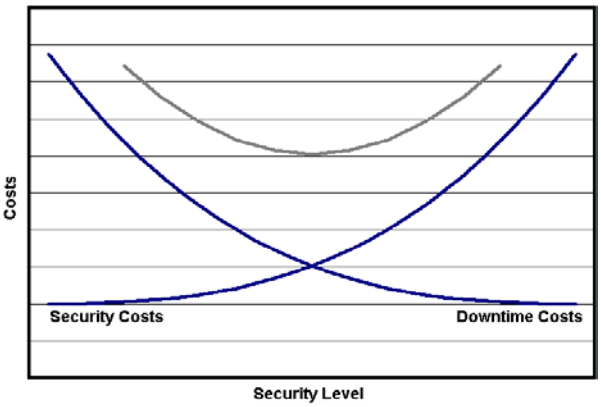

Figure 2: Relationship between Downtime Costs and Security Costs

4. Example of security valuation

In this section we illustrate the proposed framework with a simple example to show the benefit of connecting IT-Security planning with core business processes. The example describes a Call Center with Voice over IP that heavily depends on the availability of IT infrastructure. Using a very basic calculation model for brevity we show how the investment in security may reduce the risks of security breaches. The remaining risk is expressed using ALE (annual loss expectancy).

Figure 3 shows a simplified core business process.. It illustrates the first level support of a call center. In our example we assume that one employee can handle 10 cases/hour on average and that the call center has on average about 100 employees. Assuming that the costs for one employee are 18.75€/hour, the employee costs for on hour of downtime total 1,875€/hour.
In addition the loss of profit that would have been generated during downtime must be calculated. We assume that one downtime hour results on a loss of profit of 4,000€. Therefore the total downtime costs amount 5,875€/hour.
Figure 4 shows the simplified IT-processes that are used for the maintenance of the IT-Security Infrastructure of the call center. The figure shows three different levels that are processed cumulatively. Processes on higher levels include the processes on lower levels. This connection is visualized with subprocesses. The security levels have an impact on threat/risk frequency and/or expected loss (of internal benefits and external value contribution). Level 1 requires less effort than the processes on the other levels but improves security only by applying the most important patches and up-

dates. Additional tasks on Levels 2 and 3 further improve security but also require additional resources and cause higher costs. On the other side investment in higher security levels typically reduces the risk of loss of business value.
For reasons of simplicity this example only considers the operating costs needed for keeping a defined security level. We assume that the call center has two administrators that are responsible for executing the defined processes daily. The costs for both administrators are 62.50€/hour. The effort for keeping the defined security level and the corresponding costs are shown in the following table.

	Level 1	Level 2	Level 3
hours/day	3	5	8
Costs/year	56,250	93,750	150,000

Table 2: Security Costs

A security breach would result in a total or at least partly halt of the business process and associated downtime costs of 5,875€/hour. This amount is multiplied with the duration of the downtime and the probability of loss to determine the expected loss/year (ALE). The data for three scenarios is summarized in Table 3. After summing up IT-Security costs and downtime costs the optimal security level would be level two. Based on the assumed core business process the implementation of security level two would provide the optimal cost-benefit scenario.

	Level 1	Level 2	Level 3
Threat: Hardware Failure			
Freq.	0.50	0.50	0.50
ALE	44,063	14,688	14,688
Threat: Hacker			
Freq.	1.00	0.25	0.25
ALE	176,250	14,688	14,688
Threat: Worm			
Freq.	1.00	0.5	0.25
ALE	117,500	20,563	10,281
IT Operating Costs			
	56,250	*93,750*	*150,000*
Total ALE (cost from loss of benefit)			
	337,813	*49,938*	*39,656*
Total (sum of operation cost and exp. lost benefit)			
	394,063	**143,688**	**189,656**

Table 3: Cost-benefit calculation of the example.

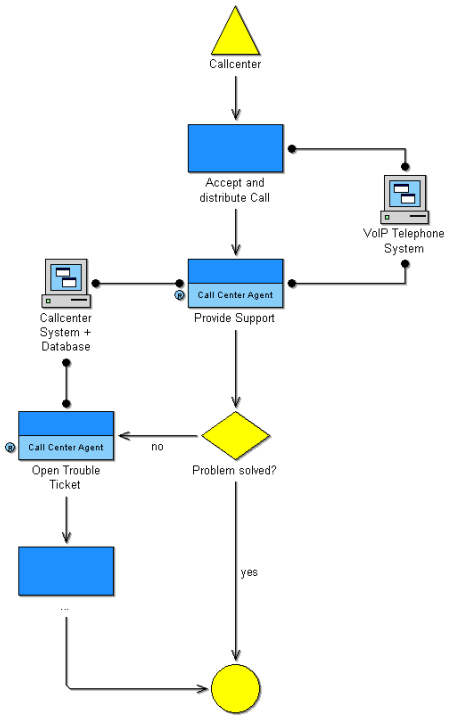

Figure 3: Core Business Process of a Call Center (Simplified).

5. Summary and Open Issues

This paper suggests a framework for a more realistic measurement of cost-benefit based on the external value of core business processes. This value-based framework aims at closing the gap between numerous security frameworks in literature that have specific merit but are neutral to external value.
The proposed approach provides the following advantages:

- The use of existing business processes allows the use of operational data produced during the execution of the business processes that is readily available. Thus data collection and analysis are easier, faster, and enable continuous monitoring, valuation and improvement of security parallel to the improvement and according to changing requirements of the corporate business processes.
- The advantages of existing cost-benefit models and security frameworks are integrated in one framework.
- Using company-specific business processes allows a more accurate collection of data needed for valuation of security cost-benefit.

Some aspects are not considered in this paper and remain open issues for further research:

- Valuation of a loss of customers and reputation resulting from security problems.
- There are differences between the security frameworks that are hard to reconcile. The effort for reaching a defined level varies significantly across frameworks. As a result the differences between costs and the achieved risk are an issue for further research.

6. References

[1] Avizienis, Algirdas; et.al.: Basic Concepts and Taxonomy of Dependable and Secure Computing; IEEE Transactions on dependable and secure computing, Vol. 1, No.1; 2004.

[2] BOC: www.boc-eu.com

[3] Butler, Shawn A.: Security Attribute Evaluation Method; ACM ICSE; 2002.

[4] Campbell, Katherine; Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market," Journal of Computer Security, vol. 11, issue 3, 2003, pp. 431-448.

[5] Clarke, R. Computer matching by government agencies: The failure of cost/benefit analysis as a control mechanism. Information Infrastructure and Policy 4; 1995.

[6] Cobit has been developed and is maintained by the Information Systems Audit and Control Association (IACSA) – http://www.iacsa.org.

[7] Ettredge, Michael; Vernon J. Richardson: Assessing the Risk in E-Commerce; Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

[8] Federal Information Processing Standards. Guideline for the Analysis of Local Area Network Security. National Institute of Standards and Technology, FIPS PUB 191, Nov. 1994.

[9] Federal Office for Information Security (Germany) (BSI) http://www.bsi.de/english/index.htm.

[10] IDS Scheer: www.ids-scheer.de

[11] Kurrek, H.: SMM – Assessing a Company's IT-Security In: ERCIM News, 2002, Nr. 49.

[12] Löffler, Helge; Markus Oman: IT-Survey 2004; KPMG Austria (Innsbruck-Linz).

[13] Mercuri, Rebecca T.: Analyzing Security Costs; Communications of the ACM; June 2003/Vol. 46, No. 6.

[14] Murine, G.E. and Carpenter, C.L. (1984), ``Measuring computer system security using software security metrics'', in Finch, J.H. and Dougall, E.G. (Eds), Computer Security: A Global Challenge, Elsevier Science Publisher, Barking.

[15] National Institute of Standards and Technologies; 1979 FIPS publication (#65).

[16] Oesterle, H.: Business in the Information Age. Heading for New Processes. Springer, Berlin/Heidelberg; 1995.

[17] SooHoo, K., How Much is enough? A Risk-Management Approach to Computer Security, Consortium for Research on Information Security and Policy (CRISP), June 2000.

[18] SSE-CMM (1998), The Model, v2.0, www.sse-cmm.org.

[19] Stacey, T.R. (1996), Information security program maturity grid, Information Systems Security, Vol. 5 No. 2.

[20] The ISO 17799 directory can be found at http://www.iso-17799.com.

[21] Thompson M.: Benefit-Cost Analysis for Program Evaluation; Sage, 1980.

Appendix

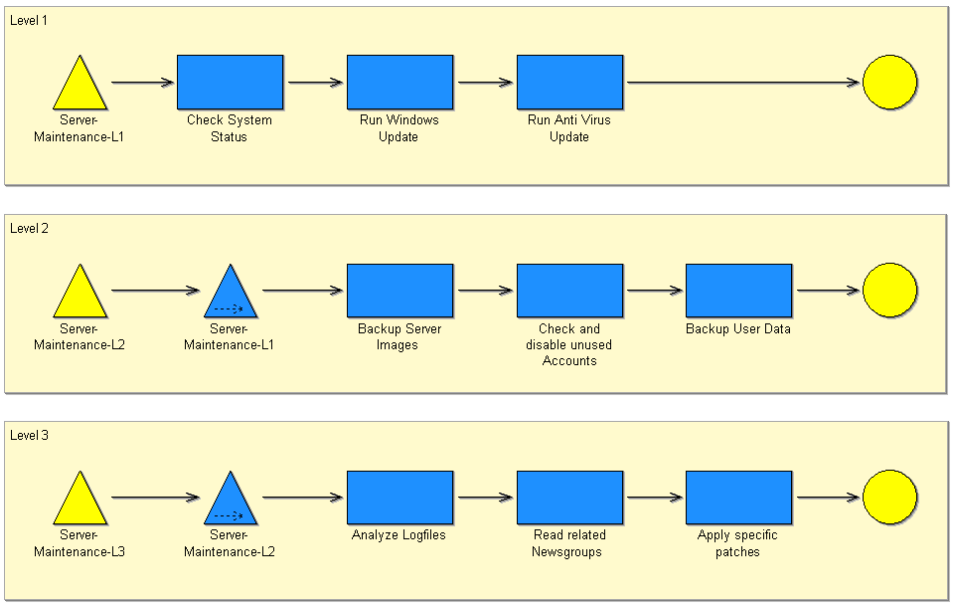

Figure 4: 3 levels of IT-Security Service Processes for the Maintenance of a Server.