2011 Third International Workshop on Security Measurements and Metrics

Performance Measurement in Cross-Organizational Security Settings

Lukas Demetz, Stefan Thalmann, Daniel Bachlechner, and Ronald Maier
University of Innsbruck School of Management
Information Systems
Innsbruck, Austria
{firstname.lastname}@uibk.ac.at

***Abstract*—Measuring IT security management performance is different and usually more difficult than other kinds of measurement. Quantifying IT security in general is difficult, additionally IT infrastructures differ strongly from each other, consist of heterogeneous components and change permanently. However, IT security needs the attention not only from specialized IT security staff, but also from general management. The critical point thus is the development of a set of suitable key performance indicators. This paper describes the creation of a set of performance indicators to be used in cross-organizational security settings on the basis of two qualitative empirical studies. Indicators were developed for organizations acting either as service providers or as service consumers.**

Keywords: security, performance, KPI, cloud computing

I. INTRODUCTION

The quote *"If you can't measure it, you can't manage it",* attributed to Robert Kaplan [1], claims that to manage systems or processes effectively, indicators are needed to draw conclusions with respect to their performance. To manage an organization's IT in general or IT-related security in particular, indicators that allow drawing conclusions with respect to the performance of IT security are needed. Metrics used in the context of IT security are referred to as security metrics [2].

Finding suitable metrics for performance measurement in general and for IT security in particular is not easy [3]. With respect to IT security, standards such as ISO/IEC 27002 [4] and PCI DSS [5] provide specific security metrics. Most security metrics proposed so far, however, focus on settings in which the IT infrastructure is run internally and do not take the peculiarities of outsourced services into account (e.g., [6-7]). As soon as parts of the IT are outsourced, finding appropriate metrics becomes even more difficult due to the fact that multiple organizations with more diverse requirements and a more complex IT infrastructure are involved. This is also accompanied by new challenges with respect to the identification of suitable performance indicators (PIs). Goal of this paper is to develop a list of PIs that is specifically suitable for cross-organizational security settings. Figure 1. visualizes the relationships between organizations participating in a cross-organizational security setting.

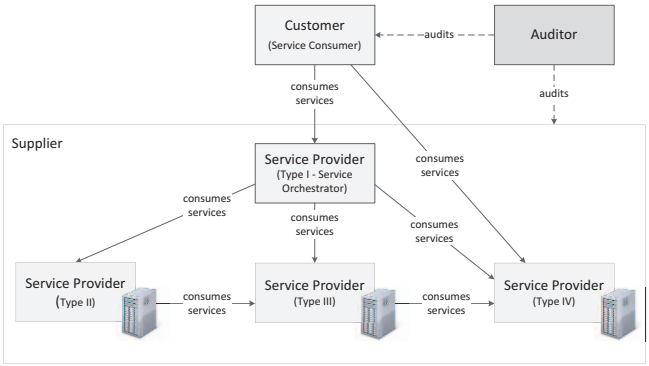

Figure 1. The investigated cross-organizational security setting [8].

In this paper, we present the findings of two independent empirical studies. The designs of both studies and their key results are described in section II. Based on the reasons for the limited use of PIs in IT security management given in the interviews (section II) and a comprehensive review of PI-related literature, a list of key performance indicators (KPIs) are sketched (section III). In section IV the findings and their relevance are discussed. Finally, we summarize the key contribution of this work in section V.

II. FOUNDATION

A. Study I – focussing on intra-organisational settings

The data of the first study was collected by means of a series of interviews with information security professionals. In the period from June 2009 to February 2010, we conducted 12 oral semi-structured interviews with information security professionals. All interviews but one telephone interview, were conducted face-to-face. Additionally, one pre-test interview was conducted. Two organizations were medium-sized, the others were large[1].

We interviewed organizations in Austria, Germany and Italy. The interviews took between 49 and 97 minutes, were recorded and transcribed. An interview guideline was sent to all participants. Once the collection of data was completed, we analyzed the data by means of a qualitative content analysis [9].

[1] http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm

978-0-7695-4680-3/12 $26.00 © 2012 IEEE
DOI 10.1109/Metrisec.2011.21

In the following, we present a summary of statements from the interviews, structured according to performance-related topics.

IT security management is no classic process: A major problem of IT security performance measurement is that IT security management is not a routinized, clearly defined process. This means the IT security management and the relevant variables vary a lot.

Incomparability of criticality of findings: One interviewee remarked that the incomparability of findings exacerbates the problem of finding appropriate metrics. For instance, consider an organization experienced two security incidents: a data leakage of customer data in which the credit card information of thousands were disclosed and the unavailability of the company's website due to a denial of service attack. Even though the organization suffered two security incidents, these two incidents are not comparable because they have completely different ramifications. In the former, the organization's public image and the customers' loyalty are damaged. Hence, a metric should take such reflection into consideration.

Financial metrics demanded, yet difficult to assess: Several interviewees concluded that management is mostly interested in monetary or financial metrics. Determining the monetary value of security incidents, however, is often possible only to a limited extent. For instance, should lost sales be taken into consideration when determining the monetary value of an incident? How to take insurances that cover a financial loss in case of an incident into account? Because of such questions, finding appropriate financial metrics is difficult.

Metrics provide look in rearview mirror: As one interviewee noted, metrics mostly provide a look in a rearview mirror. Thus, they only give insight about the performance in the past, but not about future performance.

Experience and gut feeling prevails: Multiple interviewees reported that IT security performance measurement does not only rely on quantifiable measures, but involves experience and gut feeling. That is, an experienced security professional is sometimes able to detect bad performance just based on a bad gut feeling. However, a bad gut feeling can seldom be quantified.

Probabilities instead of exact numbers: One problem of finding appropriate security metrics is that in several cases probabilities are used instead of exact numbers. For instance, possible amount of loss or the likelihood of an individual security incident is based on probabilities. However, probabilities may be wrong and provide a wrong picture.

B. Study II – focussing on cross-organisational settings

In the second study we relied on a series of semi-structured interviews conducted with professionals involved in cross-organizational security management. In total, we conducted 16 interviews with 7 organizations assuming one of the roles presented in Figure 1. in the first quarter of 2011. The interviewees were from Australia (1), Austria (1), France (4), Germany (7), Switzerland (1) and the US (2). All organizations are considered as large based on the definition of the EU commission.

Before the interviews were carried out, the interview guideline was pre-tested and slightly adapted after one pre-test interview. The interview guideline was sent to the interviewees prior to the interviews. The interview took between one and two hours. The collected data was analyzed by means of a qualitative content analysis [9].

The interviewees were asked about their involvement in activities regarding cross-organizational security management and how well performed they deemed their activities. Additionally, they were asked to give metrics, which they use to determine the performance.

All interviewees were able to answer the question about how well performed they think their IT security processes are. Although when we asked them to name metrics they use or would use to determine their processes' performance, scattered metrics, primarily time and costs, were stated. Here again the difficulty of finding appropriate metrics can be seen. However, all interviewees were able to name issues they encounter when measuring performance of their IT security. These issues are summarized in the following:

Difficult to quantify security: Some interviewees named a general problem of IT security performance measurement which is that security is in general difficult to quantify. For instance, you cannot, or only limited show the number of data leakages that are prevented by deploying a data loss prevention system.

Diversity of projects: Several interviewees working at a service supplier reported that service providers have difficulties finding appropriate measures because of the high number of service consumers and thus the high number of projects they host. This means, since every project is unique regarding the security requirements, each project would require own, or at least adapted metrics.

Getting the right information: Due to the fact that the IT infrastructure is distributed in cloud computing, the information needed for determining the performance of IT security is scattered. That is, each system resembles a silo only having local information, i.e., information about the system itself, and no further information of other systems. Hence, an overarching system coordinating the information of each system would be needed for performance measurement.

As a consequence, only incomplete information, or due to incompatibility between the systems incorrect information may be available for measuring performance.

Different systems used and compatibility issues: Another problem that arises from a distributed IT landscape is that systems from different vendors are operated that are not compatible or do not provide appropriate interfaces. That is, to measure the performance of the IT security, the systems need to communicate with each other, however, because of lacking interfaces this cannot happen. In return, performance measurement is not possible, or only to a certain extent.

Complexity of systems: Since the technology is moving fast, stay trained and master complexity of current

technologies is hard. Therefore, metrics may soon be outdated since a new technology is deployed

Missing expertise/skills: One interviewee reported that since their customers are highly specialized they have problems understanding the processes. Because of the high specialization, the interviewee simply does not have the required expertise and skills to measure the performance.

III. EXAMPLARY KPIS FOR CROSS-ORGANIZATIONAL SECURITY SETTINGS

In this section exemplary KPIs for organizations involved in cross-organizational security settings are described. The set of KPIs was developed on the basis of the two interview studies mentioned above as well as a comprehensive review of literature in which about 500 PIs could be identified. The indicators were developed for organizations acting either as service providers or as service consumers.

A. Service Consumer

In the following, we present potential exemplary KPIs for organizations involved in cross-organizational security settings with emphasis on the service customer perspective.

Quality of service provider: The monitoring and the quality control can be considered important for service customers having several service providers. Violations of security and compliance requirements should be avoided and minimized. Interviewees mentioned the difficulty to detect service and compliance violations. However, only detected violations can be measured. Hence, measuring the number of security and compliance issues as proposed in COBIT 4.1 seems to be a suitable KPI targeting on this aspect.

- no of security and compliance violations per service provider

Integration into existing landscape: One result from the interviews was that the extension and the modification of the existing landscape should be addressed. KPIs focusing on this aspect should consider efforts addressed with changes or modifications and efforts addressed with extensions of the existing landscape. In cases time to realize changes is considered critical, time is the aspect to be measured, like average time to plan for changes proposed by APM. Otherwise, estimating costs is more comprehensive, like the average costs of changes in the implementation proposed by ITIL and MOF. Surveying the effort needed to realize changes of parts of the IT landscape or even for outsourced services seems very beneficial as well. Thus, a comparison of different service providers in regard of the estimated integration efforts becomes feasible.

- avg. time to realize changes of the existing IT landscape
- avg. costs to realize changes of the existing IT landscape

Monitoring suppliers: Organizations have to monitor their suppliers in regard of fulfilling their requirements. Due to regulations, main parts of this task are performed by auditors. As frequently mentioned in the interviews, time and costs of such audits should not be underestimated. Hence, it seems valuable to measure time and costs needed for audit activities as proposed by COBIT for each service provider or for each outsourced service. Measuring fulfillment of defined security and compliance requirements by service suppliers through contracts could be very valuable as well. Weak points can be detected in this way and a quality measure for supplier networks can be created, like % of major suppliers meeting defined requirements and service levels proposed by COBIT.

- avg. time needed for auditing an (outsourced) service
- avg. costs needed for auditing an (outsourced) service
- % of service providers meeting defined security and compliance requirements and service level agreements (SLAs)

Skilled employees: Nonexistent or too few employees having substantial technical knowledge to understand complex service landscapes is frequently mentioned during the interviews. The lack of qualified staff was primarily mentioned for the service consumer and secondarily for the auditors. The interaction and especially the monitoring of service providers and also the ability to modify and to adapt the current IT landscape to changing requirements is affected. Hence, the measurement of employees having a well-defined set of skills, e.g., skills which qualify to monitor a service provider or skills which enable an employee to integrate outsourced services seem beneficial.

- no. of employees able to integrate outsourced services
- no. of employees able to negotiate technical details
- no. of employees being able to monitor service provider

Trust for service providers: Many interviewees mentioned the difficulty to measure the quality of relationships to service providers using hard facts. Personal contacts to employees of the service provider and experience are considered most important for estimating the trust in a service provider. Due to difficulties to measure these aspects independently from human beings, questioning employees seems an appropriate approach.

- avg. probability of security incidents per supplier

B. Service Provider

Taking changes in technology into account: As one interviewee remarked, the fast moving technology exacerbates the problem of finding appropriate KPIs, since existing KPIs may not be applicable to newly introduced technology. Additionally, to provide an IT service portfolio based on state-of-the-art technology, service providers need to integrate new technology into. These changes need to be planned properly beforehand and their implementation is often costly. Therefore, it seems useful to have information about changes of technology on hand.

- avg. time to plan for changes (APM)
- avg. costs of change implementation (ITL, MOF)

Providing audit compliance: For service providers, compliance with certain regulations or standards is very important. A service provider can be audited to show compliance resulting in a report. These audit reports can then be provided to customers or prospects showing the compliance and adherence to standards and regulations and thus increase the trust in a service provider.

- time/costs spent on audit activities (COBIT)

- no. of audits successfully completed (COBIT)
- % of systems with security certifications (COBIT)

SLAs covering provided services: Consumers of outsourced services want to be sure that the services they consume satisfy certain quality criteria. Therefore, SLAs specifying the requirements a service needs to fulfill are added to each service. This means, SLAs give insight about a service provider's ability to satisfy quality requirements. Having too many SLAs attached to a service, however, may become problematic since a service provider may get lost in the myriad of SLAs and does not know on which SLA he should focus. Moreover, in case SLAs are measured manually, assessing too many SLAs would take a considerable amount of time. Additionally, besides having SLAs, a service provider should also know who the person in charge of a certain SLA is.

- no. of SLAs per service
- % of service levels that are measured (COBIT)
- % of SLAs with assigned account manager (ITIL, MOF, ASL)

Costs of missing security: Providing a secure system is crucial for service providers. Providing a 100% secure system, however, is not possible, as the odds always favor the attacker [10]. This means, no matter how hard a service provider tries to prevent security incidents, there will always be a possibility of attacks. Hence, knowledge about possible costs that may occur following a security incident is crucial. Knowing the costs of possible security incidents also helps them to look for appropriate counter measures.

- cost of security incidents (ITIL, MOF) per service

Customer satisfaction: Having satisfied customers is crucial. In case of a service provider this is even more important as he has not only "end consumers", who directly use his services, but other service providers, who consume his services and orchestrate them. Therefore, service providers should know how many of their customers are satisfied with the quality of his services.

- % of stakeholders satisfied with quality of IT security (COBIT)

IV. Discussion

The analysis of the data collected within the two studies revealed that even though companies are able to judge whether their processes are well performed, they struggle when asked to name specific KPIs for determining their organization's security performance. This is true in case the IT infrastructure, and thus the security management, is operated internally, as well as for the outsourced case. However, the interviewees seem to face several challenges as soon as they try to find appropriate KPIs. We provided additional KPIs focusing on performance measurement in a cross-organizational security setting and we assigned the KPIs to a service customer and a service provider.

Concerning limitations, our paper is limited by the number of interviews we conducted. In total, we collected and analyzed data of 28 interviews. Therefore, it would be necessary to first increase the number of interviewees and second to possibly get a more diverse set of interview partners. Additionally, we focused on large companies, with the exception of two medium-sized ones. To get a more complete picture, however, it would be beneficial to consider small-sized companies as well.

V. Conclusion

This paper presented the results of a qualitative empirical study on issues in measuring IT security management performance. It turned out, that organizations intending to develop a performance measurement system for IT security need to select a number of efficiently assessable KPIs from a myriad of proposals that can be found in the literature. This paper helps in this selection process by proposing a set of KPIs for parties involved in cross-organizational security settings. The presented preliminary results represent a useful artifact for a more specific empirical investigation of the measurement of performance in cross-organizational security settings that the authors will engage in the future.

Acknowledgments

The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129) and through the COSEMA project which is sponsored by the Tyrolean business development agency.

References

[1] R. Kaplan and D. Norton, The Balanced Scorecard: Translating Strategy into Action. Boston: Harvard Business Press, 1996.

[2] K. Julisch, "A Unifying Theory of Security Metrics with Applications," IBM Research – Zurich 2009.

[3] S. M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," IEEE Security & Privacy, vol. 4, pp. 96-96, 2006.

[4] ISO/IEC, Information technology - Security techniques - Code of practice for information security management, 2008.

[5] Payment Card Industry Security Standards Council, PCI DSS Handbook. Wakefield, MA: PCI Security Standards Council,, 2008.

[6] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt. Upper Saddle River, NJ: Addison-Wesley Professional, 2007.

[7] D. S. Herrmann, Complete Guide to Security and Privacy Metrics, 1st ed. Bolca Raton, FL: Auerbach Publications, 2007.

[8] S. Thalmann, D. Bachlechner, R. Maier, M. Manhart, and L. Demetz, "Key roles in cross-organisational security settings," in Proceedings of the 2nd European Security Conference, Örebro, Sweden, 2011.

[9] M. Q. Patton, Qualitative Research & Evaluation Methods, 3th ed. Thousand Oaks: Sage, 2002.

[10] B. Schneier, "Inside risks: Cryptography, security, and the future," Communications of the ACM, vol. 40, p. 138, 1997.