# Towards Process Centered Information Security Management
## *A Common View for Federated Business Processes and Personal Data Usage Processes*

Erik Neitzel[1,2] and Andreas Witt[1,2]
[1]*Faculty of Computer Science, Otto-von-Guericke University, Magdeburg, Germany*
[2]*Department of Business and Management, University of Applied Sciences Brandenburg, Brandenburg, Germany*

Keywords: Security, Privacy, Federated Business Processes, Social Networks, Information Security (IS), Information Security Management Systems (ISMS).

Abstract: While comparing the progress of our two research projects of developing an information security management system (ISMS) for federated business process landscapes and the enhancement of security of social networks, we discovered a fundamental view congruency concerning the way information security can be handled. This paper deals with a conceptual framework which uses the ISO 27001 and the German BSI IT-Grundschutz Framework as a base for determining a methodology for a process based point of view towards information security management for both federated business processes within business applications and personal data usage processes within social networks. The proposed layers are (1) process layer, (2) application layer, (3) network layer, (4) IT systems layer and (5) infrastructure layer.

## 1 SITUATION

Todays organisations depend on IT systems which support their business processes in various ways. Those processes, however, have evolved from a single-organisation based support net into inter-organisation based business processes, see figure 1.

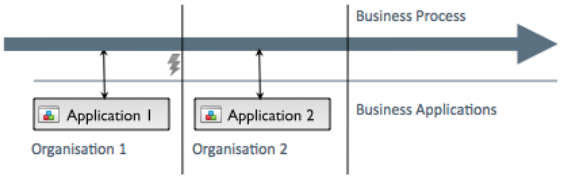


Figure 1: Federated business processes.

Generally, every organisation has to ensure the value contribution of their IT along the goals of the organisation. At the same time, the quality of application systems has to be guaranteed. There are economic criteria like costs and functional/non-functional criteria (features, usability, security). Some of those criteria are complementary. A distinguished position takes information security, as it is not just a quality criterion, but serves the organisations drive of reaching its goals at the same time.

For the assurance of the above mentioned value contributions there are both vendor independent (ITIL, COBIT) as well as proprietary (MOF, ITSM, ITPM) reference models. They describe goals, tasks, organisational aspects and concrete results of IT controls (Goeken, 2006). Hence, there are procedures for implementing general IT governance for organisations – often security aspects are adressed as well.

There are also information security management systems (ISMS) like the ISO 2700x (ISO/IEC, 2009) and the German BSI IT-Grundschutz 100-x (BSI, 2009) for the introduction and sustaining support of the quality criterion and business enhancer information security within an organisation. These frameworks are based on the Demming cycle, which suggests the phases Plan, Do, Check, Act (Walton, 1988).

Within the limits of one organisation there are first approaches for systematic procedure models as presented by Nowey (Nowey and Sitzberger, 2006), as well as suggestions for measuring security quality within business application systems (Dorrhauer and Röckle, 2011). A generic web-based federation of business application systems (Gaedke and Turowski, 1999) and approaches for their security are proposed (Armando et al., 2006) (Arsac et al., 2011).

However, none of the mentioned frameworks adresses the emerging need for governing business processes across multiple organisations – neither for

Neitzel E. and Witt A..
Towards Process Centered Information Security Management - A Common View for Federated Business Processes and Personal Data Usage Processes.
DOI: 10.5220/0004050301890192
In *Proceedings of the International Conference on Data Technologies and Applications* (DATA-2012), pages 189-192
ISBN: 978-989-8565-18-1

the general purpose of implementing a consistent cross-organisation IT governance nor for supporting information security management.

Analogously to the situation of single-organisation business processes evolving into inter-organisation based processes, social networks experience a similar trend by means of inter-organisational security issues, see figure 2. Within the realm of huge social networks like Facebook, a common business model is the selling of personal data to other organisations for advertising. For example, Facebooks ad revenues reaches $4.27 Billion in 2011 (Fredricksen, 2011).

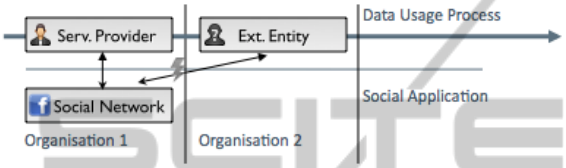


Figure 2: Social networks third party interests.

There are ideas regarding a re-invention of the social network using semantic P2P systems as presented in (Schwotzer, 2011). As long as those concepts are not turned into products, personal data will remain to be processed by third parties as presented here.

Those personal data usage processes are quite similar to business processes, as both of them are spread across multiple IT systems, being carried by various IT infrastructure components within different organisations as many businesses are supported by cloud based services.

## 2 PROBLEM

Generally, information security management deals with the process of sustaining risk reduction regarding various threats against the three main information security criteria. Those criteria are confidentiality, integrity and availability of information (ISO/IEC, 2009). Those criteria do not change when expanding processes to multiple organisations – and nor do the threats against them. The risk, however, rises significantly – and so does the need to implement effective safeguards. As discussed earlier, there is no current framework supporting information security management across multiple organisations.

Regarding social networks, the mentioned risk is similar. Data protection and privacy is compromised by the joint network operation itself. In terms of information security management, that means an extensive risk against confidentiality (here the confidentiality of personal data). Hence, the sustaining need for transparency increases – and so does the need for reporting on technical and organisatory safeguards being implemented by organisations.

In case of social networks, there are different points of view regarding security and privacy. The social network itself has to protect its network against hackers (Mirror, 2011). At the same time it has to offer personal data of its users for selling. For that, most social networks use Application Programming Interfaces (APIs) like Facebook's Open Graph. For best revenue of a social network provider users should reveal as much personal information as possible. By doing so user profiles are getting more relevant for advertisers. As a result users of social networks could receive an unwanted overflow of commercial information (Bognanni, 2008). Therefore, conflicts arise between commercial use of user profiles by social networks and the user's willingness towards their own data and user generated content (Mörl and Groß, 2008). Hence, social networks, users and advertisers are heavily depending on each other. This dependency influences information security criteria – integrity, availability and confidentiality, see figure 3.

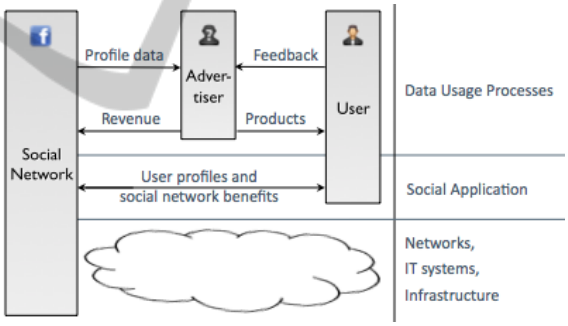


Figure 3: Social networks/users/advertisers dependencies.

The above mentioned problems are also relevant for companies which have their own social network, e.g. Lego with Rebrick[1] or companies using social networks for social commerce or social media marketing campaigns. Social media marketing and social commerce strategies often make use of fanpages or own company accounts in different social networks. Hence, companies that use social networks for their online strategy have to integrate different IT systems and external applications within their federated business process landscapes.

[1] http://rebrick.lego.com

# 3 SOLUTION

BSI (the German authority regarding IT security) (BSI, 2009) suggests a framework compatible to the requirements of the ISO 27001 in which a layered approach is used to simplify the problem of referencing safeguards to categories of information security management relevant objects. Those layers are (1) intersectoral aspects, (2) infrastructure, (3) IT systems, (4) networks and (5) applications. The approach starts with a layer that deals with general security management requirements for an organisation and is then followed by layers beginning from physical to logical object categories. We argue that BSI's approach fits single organisations information security needs but not federated processes, as for that purpose a top down approach would be necessary which begins at the level of processes, not at the level of infrastructure. Generally the layered approach seems appropriate to be pursued towards that problem.

As a conceptual model, we therefore argue that a layered model shall be used that uses the basis of the descriptive model presented by BSI but replaces the intersectoral layer by a process layer and inverts the order of the other layers. The requirements of that process layer are the same as the requirements presented in BSI's layer 1 (intersectoral aspects), but refers to the process, not the organisation. Thererfore, several organisations would have to implement safeguards identified for that process.

We now argue that BSI's remaining layers shall be used in opposite order, to receive a top down security management approach. In particular, the process layer (1) shall be followed by applications (2), networks (3), IT systems (4) and infrastructure (5), see figure 4[2].

Furthermore, due to the same structure of organisations supporting business processes and organisations using personal data of a person registered at a social network; we conclude that a business process and a personal data usage process are to be handled in the same way regarding security management.

In addition, we propose that the safeguards that need to be implemented according to ISO/BSI shall be extended by the following two constructs:

(1) For the purpose of an individual's privacy evaluation (Heidisch and Pohlmann, 2012) has presented the idea of a "data letter" where each web entity that processes personal data (e.g. a social network) regularly has to inform the user about which kind of information is stored and processed about him. As a result, the user may request change and deletion of the information presented.

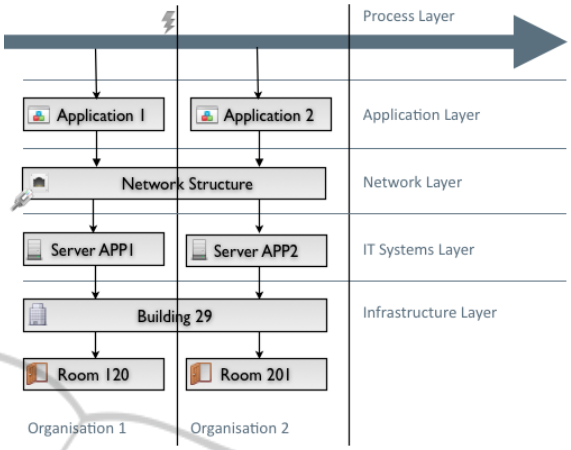


Figure 4: Proposed IS security management layers.

(2) Based on the idea of the data letter, we propose the introduction of an IT security letter (ITSL) that informs the user about the actual security measures that were implemented at the level of a providers (IT) infrastructure. This ITSL could be voluntary, thereby serving as a competitive advantage at the market.

The content of the ITSL shall include references to the implemented safegaurd categories as defined in the ISO 27001. The broad guidelines defined in that standard would form both a solid and individually formable frame of which the user can get an impression of how its stored and processed information is guarded against attacks and failure.

The actual safeguards to be implemented for those layers shall stay the same as defined in ISO 2700x and/or BSI IT-Grundschutz.

Following the proposed model, both federated business processes and personal data usage processes are secured towards threats against integrity, availability and confidentiality – especially those of personal data within social networks.

# 4 OUTLOOK

Future research shall both conduct further evidence of the presented problem and deliver an evualuation of the effectiveness of the proposed model. The common view and methodology shall be refined and further investigation be progressed regarding explicit safeguards serving the security of federated business processed. In the end, a measurement model shall be developed to assess both the effectiveness and efficiency of those safeguards.

[2]The figure was developed using Fugu Icons designed by Yusuke Kamiyamane.

## REFERENCES


Armando, A., Giunchiglia, E., Maratea, M., and Ponta, S. E. (2006). *An action-based approach to the formal specification and automated analysis of business processes under authorization constraints*. Journal of Computer and Systems Sciences: Special issue on Knowledge Representation and Reasoning, to appear.

Arsac, W., Compagna, L., Kaluvuri, S. P., and Ponta, S. E. (2011). *Security validation tool for business processes*. In Proceedings of the 16th ACM symposium on Access control models and technologies, SACMAT '11, pages 143-144, New York, NY, USA. 2011, ACM.

Bognanni, M. (2008). Mein freund der datenhändler (datensicherheit in sozialen netzwerken). Retrieved from: http://www.stern.de/digital/online/datensicherheit-in-sozialen-netzwerken-mein-freund-der-datenhaendler-636203.html.

BSI (2009). Bsi-standard 100-1, 100-2, 100-3, 100-4.

Dorrhauer, C. and Röckle, H. (2011). *Messbarkeit der Sicherheitsqualität im Lebenszyklus betrieblicher Anwendungssysteme*. In: Betriebliche Anwendungssysteme (Thomas Bartin, Burkhard Erdlenbruch, Frank Herrmann, Christian Müller), Proceedings of AKWI Symposium, Worms.

Fredricksen, C. (2011). Facebook revenues to reach $4.27 billion in 2011. Retrieved from: http://www.emarketer.com/PressRelease.aspx?R=1008601.

Gaedke, M. and Turowski, K. (1999). *Generic Web-Based Federation of Business Application Systems for E-Commerce Applications*. In: Engineering Federated Information Systems (S. Conrad, W. Hasselbring, G. Saake), Proceedings of the 2nd Workshop EFIS'99, Kühlungsborn (Germany).

Goeken, M. (2006). *Referenzmodelle für Betrieb und Entwicklung von Anwendungssystemen*. In: Vorgehensmodelle und Projektmanagement - Assessment, Zertifizierung, Akkreditierung (Höhn, R. et al.), Proceedings of 14th Workshop of WI-VM Symposium GI, Aachen.

Heidisch, M. and Pohlmann, P. D. N. (January 2012). *Der Elektronische Datenbrief*. Institut für Internet-Sicherheit - if(is), FH Gelsenkirchen.

ISO/IEC (2009). International standard iso/iec 27000 first edition.

Mirror (2011). Facebook hacker admits breaking into social network's servers. Retrieved from: http://www.mirror.co.uk/news/technology-science/technology/facebook-hacker-admits-breaking-into-social-96681.

Mörl, C. and Groß, M. (2008). *Soziale Netzwerke im Internet – Analyse der Monitarisierungsmöglichkeiten und Entwicklung eines intergrierten Geschäftsmodells*. Verlag Werner Hülsbusch, Boizenburg.

Nowey, T. and Sitzberger, S. (2006). *Lernen vom Business Engineering - Ansätze fuer ein systematisches, modellgestuetztes Vorgehensmodell zum Sicherheitsmanagement*. In: Multikonferenz Wirtschaftsinformatik 2006 (Lehner, Franz und Nösekabel, Holger und Kleinschmidt, Peter). Proceedings 2. Gito, Berlin.

Schwotzer, T. (2011). *Distributed Context Space (DCS) - foundation of semantic P2P systems*. 3rd International ICST Conference on IT Revolutions, Cordoba / Spain.

Walton, M. (1988). *Deming Management Method*. Perigee Trade.