Business Process Modeling for Insider Threat Monitoring and Handling

Vasilis **Stavrou**, Miltiadis **Kandias**, Georgios **Karoulas**, Dimitris **Gritzalis**

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business
76 Patission Ave., GR-10434, Athens, Greece
{stavrouv, kandiasm, gi.karoulas, dgrit}@aueb.gr

Abstract. Business process modeling has facilitated modern enterprises to cope with the constant need to increase their productivity, reduce costs and offer competitive products and services. Despite modeling's and process management's widespread success, one may argue that it lacks of built-in security mechanisms able to detect and deter threats that may manifest throughout the process. To this end, a variety of different solutions have been proposed by researchers which focus on different threat types. In this paper we examine the insider threat through business processes. Depending on their motives, insiders participating in an organization's business process may manifest delinquently in a way that causes severe impact to the organization. We examine existing security approaches to tackle down the aforementioned threat in enterprise business processes and propose a preliminary model for a monitoring approach that aims at mitigating the insider threat. This approach enhances business process monitoring tools with information evaluated from Social Media by examining the online behavior of users and pinpoints potential insiders with critical roles in the organization's processes. Also, this approach highlights the threat introduced in the processes operated by such users. We conclude with some observations on the monitoring results (i.e. psychometric evaluations from the social media analysis) concerning privacy violations and argue that deployment of such systems should be allowed solely on exceptional cases, such as protecting critical infrastructures or monitoring decision making personnel.

Keywords: Business Process; Business Process Management; Insider Threat; Monitoring; Privacy; Social Media.

1 Introduction

Modern enterprises and organizations operate in a dynamic environment that is constantly evolving. This dynamic environment includes the competition for high quality products and services, reduced costs, and fast development. Factors such as globalization of business activities and the rapid growth of ICT offer new opportunities and give birth to threats for the organizations, while technological novelties have created a need for new operational structures for the enterprises and organizations.

Therefore, each organization needs to develop business processes that meet the above mentioned requirements, while ensuring the fulfillment of the goals set.

A business process is defined as "*a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer*" [1]. It consists of a set of activities and tasks that, together, fulfill an organizational goal. Modeling the business processes of an organization improves the understanding of the corporate milieu and augments its flexibility and competitiveness in business environments. Modelling often includes Business Process Management (BPM) [2], a holistic approach to harmonize an organization's business processes with the needs of their clients [3]. Business processes are designed to be operated by one or more business functional units. Tasks in business processes can be performed either by means of business data processing systems (e.g. Enterprise resource planning (ERP) systems), or manually. Specifically, in an enterprise environment, some process tasks may be performed manually, while others may be automated or even batch scheduled in a variety of ways: data and information being handled throughout the business process may pass through manual or computer tasks in any given order.

Business process modeling, mainly during its first stages, lacks built-in security mechanisms so as to prevent a malevolent functional unit from causing harm to the organization through the operated process. Our research focuses on mitigating the insider threat via a combination of business process security and a series of psychosocial parameters that interfere with them. Although role-based access control [5] is used in various approaches to tackle the insider threat [6], it usually fails to be mitigated, thus leading us to consider that new approaches need to be taken into account. Furthermore, regarding role-based access control (RBAC) schemes, the insider is a legitimate user of the infrastructure, who utilizes his access rights in a disrespectful manner towards the organization's security policy [6]. Thus, such schemes tend to fail against the threat.

Other, more intrusive, approaches involve monitoring techniques varying from system call activity [7] and linguistic analysis of electronic communications [8] to tracking business processes [9] and provide logging information about them. The information acquired can provide conclusions over the functional unit (i.e. the employee) who operates it and also detect possible anomaly deviations in her usage behavior that require further examination. Along with technical countermeasures, research has proved that it is possible to detect personality characteristics shared among insiders themselves through social media [10] [11], as users tend to transfer their offline behavior to the online world [12].

In this paper we revise and extend the business process monitoring model presented in previous publication of ours [4]. The proposed model is still preliminary, as it has not been developed yet. Comparing current paper to our previous work, we considerably revise and add further commentary and desired functionality over the components of the model presented. Additionally, we also examine the limitations, as well as the requirements of this approach, in order to develop a functional mechanism. Thus, aim of this paper is to propose a model based on two of CERT's patterns [28] that suggest the use of external sources of information to monitor employees and the combination of technical and behavioral monitoring to deter the insider threat. This mechanism is able to monitor user's performance at runtime level, along with its

psychometric evaluations from social media, and issue alerts when a processes may involve a threat by a potential malevolent unit.

The model's input is comprised of: (a) psychometric evaluations, extracted from social media user profiles of the organization's employees, (b) the business processes each user is involved, and (c) the performance at workspace. Its output consists of: (a) alerts, when a user manifest a potential insider behavior is detected in online monitoring component and (b) the business processes that the user is involved with.

Online monitoring can facilitate insider threat mitigation since, unlike other technical approaches, it also takes the human factor into account. However, unconsented user monitoring, either at organization level or through online profiling, interferes with the user's personality and privacy rights, something that need to be taken into consideration. Therefore, a monitoring process can be ethically and legally acceptable only in cases involving high societal risk (as in critical infrastructures where national security, economic prosperity or national well-being are at stake). In most cases, the user's explicit consent must have been given in retrospect.

The paper is organized as follows: In section 2 we briefly review the existing literature. In section 3 we discuss the security approaches to mitigate the insider threat in business process. In section 4 we present a business process monitoring model. In section 5 we discuss the requirements and limitations of the approach proposed. In section 6 we examine the ethical and legal issues over online and organizational user monitoring. Finally, in section 7 we conclude and refer to plans for future work.

2 Related work

None of the approaches introduced in the insider threat detection literature appear to combine both business process and psychometric monitoring, so as to proactively detect the current threat in the organization. To this end, we examine approaches and methodologies used to enhance business process security, under the prism of insider threat mitigation via: (a) psychosocial approaches that may predict malevolent behavior, and (b) monitoring techniques that have been used against the insider threat.

Security in business processes involves methodologies that target at satisfying requirements in their development phase [13]. A developer is advised to be aware of the security goals the implementation should achieve, since the construction of models during requirement analysis and system design can improve the quality of the resulting systems, thus providing early analysis and fault detection along with maximization of the security lifecycle of the solution.

Security and system design models are often disjoint, as they are expressed in different ways (security models as structured text vs. graphical design models in notation languages). To this end, modeling languages, such as secure UML [14], have been developed in order to bridge the gap between security requirements and model design. In particular, secure UML is designed for specifying access control policies by substantially extending Role-Based Access Control (RBAC). RBAC has bee also extended in order to address task delegation in workflow systems. In their work, Gaaloul, et al. [15], use a role-based security model in order to show how formalized

delegation constrains can be injected to specify privileges into delegation policies within an access control framework.

As modern enterprise systems are becoming more business-process driven, an approach describing secure BPMN [16] has been developed, in an effort to create models with embedded security requirements that generate robust system architectures, including access control infrastructures. The proposed tool supports model-driven development of processes that integrate security and compliance requirements across all phases of the system life-cycle. Together with [17] a formal methodology for the automatic synthesis of a secure orchestrator, a set of BPMN processes is described to guarantee non-disclosure of messages exchanged in processes. Finally, model checking techniques are used for evaluating security aspects of business processes in dynamic environments [20]. Another approach [18] in business process security involves the modeling and analyzing of the participants' objectives; so as to extract security requirements from them use them to annotate business processes. To deal with organizational analysis and the integration of security and systems engineering, the goal-oriented requirements engineering domain includes approaches such as Secure Tropos [19]. Secure Tropos forms a methodology for security-aware software systems and combines requirements engineering with security engineering concepts to support the analysis and development of secure systems.

Regarding insider threat prediction, various approaches have been proposed [21]. Researchers have examined the psychosocial traits that indicate predisposition of delinquent behavior [22], while modern approaches indicate that such characteristics can be extracted through social media. To this extend, conclusions over traits, such as narcissism [10], or predisposition towards law enforcement [11], have been successfully extracted via **Twitter** and **YouTube**, respectively, thus leading towards the capability of online monitoring of users' behavior to detect potentially malevolent users.

Monitoring techniques are also used to detect potential insiders. At system level, LUARM [23] can be used to accurately specify insider threats by logging user actions in a relational model, as a forensic mechanism. Furthermore, linguistic analysis of electronic communications has been also used as a monitoring technique, so as to proactively detect potential insider threat risks in the organization [8].

3 Insider Threat Mitigation

Insider threat has been identified as a major issue not only in corporate security but also in cloud computing [25]. To mitigate the insider threat, security research has proposed various approaches, countermeasures and techniques, together with security policies, procedures and technical controls. Each organization should examine its design functionality, in order to tackle the threat at its business process level. The mitigating stages at process level are the following:

• **Design secure business processes** by extending the annotation of existing modeling languages, in order to encapsulate security requirements. For example, existing modeling languages, such as BPMN, can be extended to support features regarding integrity, confidentiality and access control [26].

• **Risk assessment** [27] at business process level in order to evaluate the risk involved in each process, with regard to security needs and the environment in which each process is deployed. Applying proper risk management ensures the balance of operational and economic costs of protective measures and security policies.

• **Monitoring each business process** of the organization and extracting conclusions. Monitoring may facilitate the location and redesign of problematic procedures and reduce the risk of an insider threat incident.

These above approaches may deter the insider threat to some extent but they do not aggregate the human factor in the result. Therefore, they try to solve the problem by using solely technical countermeasures and security policies, instead of trying to integrate the prediction front into the applied approaches.

The human factor is discussed in approaches regarding either insider threat prediction, or monitoring and screening, in order to extend employee monitoring outside an organization boundaries. A research involving employee's monitoring has been introduced by CERT. It focuses on analyzing insider threat cases in order to identify weaknesses in parts of the organization that facilitate the manifestation of such incidents. Part of this research outcome has led to 26 enterprise architecture patterns, developed as a means of protection from malevolent insiders [28].

Among the patterns developed by CERT, we focus on the following: (a) **Monitoring the organization**, which suggests the institution runs a monitoring program that collects information on the status of insider threats and incidents within the organization. This way, the organization can obtain an estimation of the risk involved by malicious insider activity. (b) **Monitoring employees**, which suggests the establishment of a legal, affordable and effective monitoring system that is acceptable to all stakeholders. Monitoring results should be secured and used solely for the purpose of optimizing resources and not for discrimination. (c) **Use optimized monitoring for early detection**, which indicates that organizations should configure their infrastructures in a way that insider attacks are detected in a short time period. (d) **Combine technical and behavioral monitoring**, which suggests that technical and behavioral monitoring can increase the effectiveness of insider threat detection by alert sharing, so as to investigate and detect malicious actions. (e) **Use external sources of information**, which suggests the use of external information sources, such as social networks, in order to expand employees monitoring.

We focus on proposing a model approach which enhances business process management systems (BPMS) with psychological evaluation approaches, along with monitoring techniques, so as to mitigate the insider threat.

4 Proposed model

We propose a monitoring approach that combines enterprise level monitoring with social media-extracted monitoring intelligence (Fig. 1), in order to mitigate the insider threat along with managing the risk introduced due to the human factor. In order to tackle this problem, we decided to develop an integrative model that builds upon our previous work [4] on user and usage profiling via data obtained from social media. Existing business monitoring tools can be further expanded to receive input regarding

the aforementioned psychometric evaluations. Such tools can monitor the organizational processes while recording the users involved in each process.

The paper mainly focuses on two of the above CERT's patterns: (a) "Use external sources of information" and (b) "Combine technical and behavioral monitoring". The remaining patterns can be utilized via existing and conventional monitoring tools. As a result, we aim at further enhancing existing monitoring tools by combining external sources of information (i.e. social media) with technical and behavioral patterns.

To this end, we build upon our previous research and propose a new architecture (Fig. 1). The architecture receives the following types of input: (a) data from business monitoring regarding employees' performance, (b) online monitoring, which involves data acquired from social media, and (c) the processes that the user under examination is involved with. The output comes in the form of: (a) potential incident alerts and (b) the risk that refers to the specific processes of the organization.

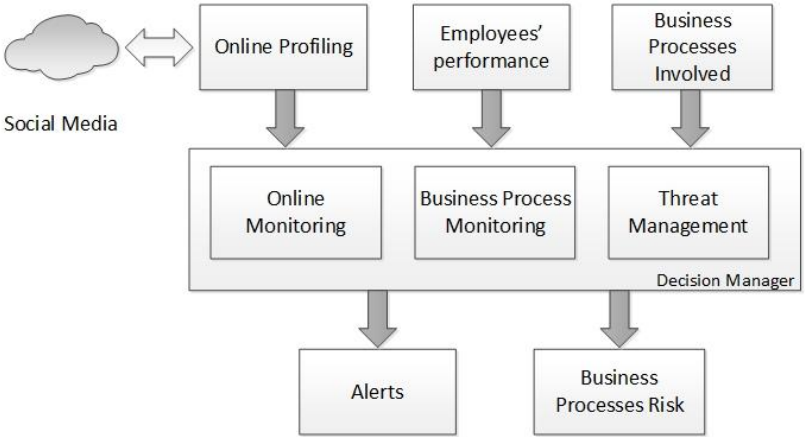

Fig. 1. Monitoring system's architecture

The model's inputs are processed by the *decision manager* module that consists of three core modules. Namely, it comprises the online monitoring, the business process monitoring, and the threat management. Each of the modules cooperates with the rest in the boundaries of the decision manager so as to achieve the desired functionality.

The contribution of this model lies on the fact that the human factor has been rarely examined in monitoring systems that focus solely on technical countermeasures. However, monitoring users at workspace usually gives rise to ethical and legal issues.

4.1 Module: Online Monitoring

The o*nline monitoring* module facilitates the process of behavioral analysis carried out on information system users, as manifested in the digital world. The ability to detect patterns of characteristics commonly shared among insiders enhances a monitoring system, as it integrates the prediction front of insider threat in the monitoring process. Online monitoring can be applied on social media profiles and extract conclusions over insider threat characteristics such as *narcissism* [10],

predisposition towards law enforcement [11], and *divided loyalty* [30]. The above traits have been examined and detected through social media and can facilitate the insider threat prediction in the digital world. Thus, they have been the topic of interest in Shaw's research [22]. These traits have been also examined by the FBI [31].

One may extract the aforementioned three traits examined to detect a potential insider by examining her online behavior, by using open source intelligence (OSINT) techniques. OSINT [32] facilitates the improvement of the online monitoring efficiency. It refers to intelligence collected from publicly available sources, such as websites, web-based communities (i.e. social networks, forums, or blogs), and (openly) publicly available data.

An interesting observation is that direct access to the user social media data is not required, at least not through the network per se. Users data content in social media is usually publicly available, as most of them neglect to use the available privacy mechanisms. Therefore, anyone interested in collecting such data is free to gather information and analyze it for conclusions, targeting any user of interest.

OSINT processes often rely on vast amounts of reliable information. Due to that fact, the following key points should be taken into account:

• **Uncovering data location**: It is required to have knowledge of the locations from where the appropriate data can be gathered.

• **Sources discrimination**: The discrimination of the useful and the irrelevant sources of information is important, so to avoid collecting outdates or useless data.

• **Results refining**: After having generated conclusions over the subject of interest, one could further process the results in order to focus on the required knowledge.

The mechanisms developed in [10], [11] and [30] rely on the above mentioned key points. Also, they can be used as a means of conclusion extraction over the insider traits of narcissism, predisposition towards law enforcement, and divided loyalty, by the online monitoring module. Each of the mechanisms can indicate whether a user shares the trait examined by having as input her username and being able to access her online user-generated content.

Consequently, the decision manager can issue alerts whether manifestation of insider characteristics is detected in the online world. Additionally, it highlights the business processes where a potentially malevolent user is involved into. Then, the operator of the system can further examine the alerts of the online monitoring module and may draw conclusions over the user performance through the *business process monitoring* module.

4.2 Module: Business Process Monitoring

This module monitors an employee's performance in workspace. Process monitoring refers to real-time observations of activities, combined to accomplish a specific organizational goal. Business process monitoring involves mainly business activity monitoring, thus helping senior management gain insight into processes deployed within the organization. It also enables organizations to measure and analyze their performance, and identify critical problems proactively, thus improving speed, quality and efficiency of their processes. Additionally, being able to monitor employee's

performance at workspace, one may detect deviations in the execution of the activities the user is involved into (Fig. 2.). Therefore, the decision manager can use the online monitoring module, to examine any potential change in user's online behavior. Whether a deviation in employee's performance is detected, it could have occurred due to manifestation of insider characteristics. To this end, the security officer should further examine the source of this deviation.

Fig. 2. Employee's performance monitoring

The growing need of organizational processes monitoring has led to the development of many platforms, which provide tools for the development of services and composite applications, allowing greater visibility, controls and analysis in the whole process lifecycle. Our model approach can utilize an existing business process monitoring platform and extend it, so as to include the functionality introduced by the online monitoring module. Process monitoring platforms that could be used and further be extended, in order to meet our needs, are the IBM Business Monitor[1], the Oracle Business Activity Monitoring[2] and the WSO2[3].

4.3 Module: Threat Management

Potential insiders introduce risk to the systems they operate, as they can manifest in a malevolent way that will cause severe impact to the organization. The threat management module handles this risk faced by potential insiders who operate organizational business processes.

To develop a more holistic perspective regarding the risks that business processes face due to their operators, the model can be enhanced with the ability to categorize the organization's business processes. To this end, an approach that takes into account both the risk faced by the assets involved in a process and the psychosocial traits of the operator, is required.

Based on the above, an approach should examine the processes under two perspectives: (a) the risk that a business process has due to the assets involved in it and (b) the risk occurred based on the psychosocial traits of the employee that operates it. The *risk that characterizes a process*, regarding the assets that are involved in it, refers to

[1] http://www-03.ibm.com/software/products/en/business-monitor
[2] http://www.oracle.com/us/products/middleware/soa/business-activity-monitoring/overview/index.html
[3] http://wso2.com

the impact to the organization due to a possible loss of confidentiality, integrity or availability. Therefore, the more important the asset, the severer the impact. Complementary, the *risk involved by the human factor* corresponds to the predisposition of delinquent behavior that characterizes user's online behavior. This discrimination contributes to the protection of critical processes since both risk factors are taken into account.

The risk faced by the psychosocial traits of the potential insider, should be able to be quantified. The existing mechanisms, used by the online monitoring module, are able to answer whether, or not, a user manifests such behavior in social media. Thus, it is required that they quantify the amount of certainty, or the extent a user expresses the aforementioned traits in the online world. One may notice that by being able to measure the psychometrics, an underlying model could use them to express the amount of risk that a process is exposed due to its operator.

At a primary stage, this module may issue alerts anytime the online monitoring system detects a potential insider. Following the alert, it could highlight the business processes in which the malevolent user is involved and help the security officer decide on proper actions to be taken.

5 Requirements and Limitations

We now discuss the requirements and limitations of the approach introduced. In order to monitor user's online behavior it is required that the user has created a profile at least in one of the social media for which we have developed evaluation mechanisms (i.e. YouTube and Twitter). If the profile is public, then our mechanisms are able to collect and process the available data so as to draw conclusions over the user's behavior. Depending on legal parameters, a user consent is usually required in order to process such data. An additional requirement for the online monitoring module is the conversion of the collected data from an SQL schema into flat data representation. Such a conversion facilitates the partitioning and distributed processing of the data, thus leading to faster processing [11].

Regarding the log storage functionality, especially for the online monitoring behavior, the system should take into account that the size of such data is expected to grow rapidly, thus indicating that big data processing techniques should be used.

The decision manager combines the functionality of the online monitoring module, the business monitoring module, and the threat management one. In order to develop the decision manager it is required that an existing Business Process Management System (BPMS) is extended so as to integrate the desired overall functionality.

A limitation of this approach is that an intelligent insider could possibly manifest a different online behavior, knowing that her profile is monitored, and thus deceive the system. In this case a more microscopic examination of a user online behavior could indicate fragments where contradictions are presented.

It appears that, for the time being, there are no other approaches that take into account the risk introduced by the psychometric evaluations. At first, the quantification of the psychosocial traits it is required and then a sophisticated risk analysis approach

should be developed in order to take into consideration the risk introduced by the psychosocial indications.

6 Ethical and Legal issues

The proposed approach introduces a mechanism for monitoring at organizational level, along with online profiling, that aims at deterring the insider threat. However, employees' monitoring interferes with their personality and privacy rights.

The rapid evolvement of Web 2.0, together with the advent of social media, has offered to workspace monitoring an opportunity to expand by screening an employee online behavior. Employees' monitoring can no longer be performed in the workspace per se, but alternatively in the online world. Monitoring the online behavior and social communication relationships of employees augments the chances of employers to influence behavior and promote the "well-adjusted employee" [33]. Moreover, information gathering about employee performances outside the traditionally conceived work sphere has a chilling effect on individuals' personality and freedom of speech. Employees may sacrifice "Internet participation to segregate their multiple life performance" [34] and thus refrain from expressing themselves.

To improve productivity and prevent potential threats, employees are often asked to sacrifice privacy rights in favor of managerial interests. Given the fact that workplace belongs to the "private sphere", employees who are hired to attend company business cannot have a (subjective) "reasonable expectation of privacy" that society (objectively) accepts and legitimizes. American Courts are reluctant to recognize a workplace privacy right. In any case, reasonable expectation of privacy of employees should be assessed under all circumstances and should be reasonable both in inception and scope. In the employment context, privacy (if any) seems to be exchanged for something of commensurate value, like taking or keeping a job [35].

Diametrically opposite in many respects, the European approach claims that privacy is not conceived as a right to seclusion and intimacy but as a phenomenon, a protectable situation that regards the relationships between a person and its environment. The European Court of Human Rights has rejected the distinction between private life and professional life (Niemietz vs. Germany). According to the Court, European employees have "a right to dignity and a private life that does not stop at the employer's doorstep".

Profiling aims to gain probabilistic knowledge from past data, propose predictions, and identify risks for the future. This goal may infringe civilian privacy, i.e. the right for everyone to be a multiple personality and also may have a serious impact on the employee regarding social selection and unjustified discrimination.

Finally, excessive monitoring has been demonstrated to affect the employer-employee relationship. Research [35] [36] has showed that employees whose communications were monitored suffered by higher levels of depression, anxiety and fatigue than those who were not. The effect of being constantly monitored, even concerning activities that fall out of the workplace frame, has negative impacts on the employer-employee relationship, which should be based on mutual trust and confidence.

7 Conclusions

In this paper we dealt with the insider threat mitigation issue and suggested a way to improve the protection against potential insider at business process level. To this end, we proposed a structural approach that combines monitoring at process level with psychosocial monitoring through social media. We mainly focused on two of CERT's insider threat patterns; namely, on the use of external sources of information (i.e. social media), as well as the combination of technical and behavioral monitoring, to mitigate the current threat.

Our approach consists of three modules, i.e. the online monitoring, the business process monitoring and the threat management. These modules cooperate in the boundaries of the model's decision manager in order to form a unified monitoring system that helps security officers to better carry out their duties.

Our ultimate goal is to integrate the human factor into the business process security. Malevolent insiders have been found to share common characteristics. Research has indicated the feasibility of extracting such traits through social media. Thus, corporate security could better deal with the insider threat by using a mechanism which can integrate psychosocial evaluation into a business activity monitoring system.

As expected, the model approach described faces a few limitations that have to be overcome, in order to achieve full functional. Such limitations include the ability of an intelligent insider to manifest a misleading behavior to deceive the system, without being detected, and the need that a user to be monitored into the online world should have at least one profile in a social medium.

Regarding the requirements, an existing business process monitoring platform should be used in order to be extended and implement the required functionality of the monitoring system. Another requirement refers to the improvement of the existing processing mechanisms, as the vast amount of information requires demanding computing power.

One could argue over the applicability of the proposed model, as screening employees (in both business level and online behavior through social media) may violate human rights and raise serious ethical issues. To this end, we exploit the principle of proportionality by considering that the use of such a method should be solely confined in a critical infrastructure, given a prior user consent [37] [38] [39].

For future work we plan to implement the model in a test environment, so as to evaluate and detect possible performance issues and also provide a more detailed step by step description of the model's functionality as a case study. In addition, we plan on improving our data collection mechanisms from social media, so as they perform more efficiently in complexity and time execution, and also present a more holistic approach of the evaluation mechanism from social media for a better understanding of the approach proposed. Following we plan on examining how to resolve the limitations described in section 5.

Last, but not least, the development of a business process risk analysis methodology that takes into consideration the insider threat characteristics a user may have is planned. Note that by being able to quantify the personality traits of the insider extracted from social media, we could use them to represent the risk faced by the user that operates a business process.

References

1. Hammer, M., Champy, J.: Reengineering the corporation: A manifesto for business revolution. HarperCollins. (2009).
2. Weske, M.: Business process management: concepts, languages, architectures. Springer. (2012).
3. Karagiannis, D.: Business process management: A holistic management approach. In: Information Systems: Methods, Models, and Applications, pp. 1--12. Springer. (2013).
4. Gritzalis, D., Stavrou, V., Kandias, M., Stergiopoulos, G.: Insider Threat: Enhancing BPM through Social Media. In: 6th IFIP International Conference on New Technologies, Mobility and Security. IEEE. (2014).
5. Basin, D., Doser, J., Lodderstedt, T.: Model driven security: From UML models to access control infrastructures. In: ACM Transactions on Software Engineering and Methodology, vol. 15, no. 1, pp. 39--91. (2006).
6. Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E.: The insider threat to information systems and the effectiveness of ISO17799. In: Computers & Security, vol. 24, no. 6, pp. 472--484. (2005).
7. Nguyen, N., Reiher, P., Kuenning, G. H.: Detecting insider threats by monitoring system call activity. In: IEEE Systems, Man and Cybernetics Society, pp. 45--52. IEEE. (2003).
8. Brown, C., Watkins, A., Greitzer, F.: Predicting insider threat risks through linguistic analysis of electronic communication. In: 46th Hawaii International Conference on System Sciences, pp. 1849--1858. IEEE. (2013).
9. Grigori, D., Casati, F., Castellanos, M., Dayal, U., Sayal, M., Shan, M.: Business process intelligence. In: Computers in Industry, vol. 53, no. 3, pp. 321--343. (2004).
10. Kandias, M., Galbogini, K., Mitrou, L., Gritzalis, D.: Insiders trapped in the mirror reveal themselves in social media. In: Network and System Security, pp. 220--235. Springer. (2013).
11. Kandias, M., Stavrou,V., Bozovic, N., Mitrou, L., Gritzalis, D.: Can we trust this user? Predicting insider's attitude via YouTube usage profiling. In: 10th International Conference on Autonomic and Trusted Computing, pp. 347--354. IEEE. (2013).
12. Amichai-Hamburger, Y., Vinitzky, G.: Social network use and personality. In: Computers in Human Behavior, vol. 26, pp. 1289--1295. (2010).
13. Backes, M., Pfitzmann, B., Waidner, M.: Security in business process engineering. In: Business Process Management, pp. 168--183. Springer. (2003).
14. Jürjens, J.: Secure systems development with UML. Springer. (2005).
15. Gaaloul, K., Proper, E., Charoy, F.: An Extended RBAC Model for Task Delegation in Workflow Systems. In: Workshops on Business Informatics Research, pp. 51--63. Springer Berlin Heidelberg. (2012).
16. Brucker, A., Hang, I., Lückemeyer, G., Ruparel, R.: SecureBPMN: Modeling and enforcing access control requirements in business processes. In: 17th ACM Symposium on Access Control Models and Technologies, pp. 123--126. ACM. (2012).
17. Ciancia, V., Martinelli, F., Matteuci, I., Petrocchi, M., Martin, J., Pimentel, E.: Automated synthesis and ranking of secure BPMN orchestrators. In: International Conference on Availability, Reliability and Security. (2013).
18. Paja, E., Giorgini, P., Paul, S., Meland, P. H.: Security requirements engineering for secure business processes. In: Workshops on Business Informatics Research, pp. 77--89. Springer Berlin Heidelberg. (2012).
19. Mouratidis, H., Jurjens, J.: From goal-driven security requirements engineering to secure design. In: International Journal of Intelligent Systems, vol. 25, no. 8, pp. 813--840. (2010).

20. Arsac, W., Compagna, L., Pellegrino, G., Ponta, S.: Security validation of business processes via model-checking. In: Engineering Secure Software and Systems, pp. 29--24. Springer Berlin Heidelberg. (2011).
21. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D.: An insider threat prediction model. In: Proc. of the Trust, Privacy and Security in Digital Business Conference, pp. 26--37. (2010).
22. Shaw, E., Ruby, K., Post, J.: The insider threat to information systems: The psychology of the dangerous insider. In: Security Awareness Bulletin, vol. 2, no. 98, pp. 1--10. (1998).
23. Magklaras, G., Furnell, S., Papadaki, M.: LUARM: An audit engine for insider misuse detection. In: International Journal of Digital Crime and Forensics (IJDCF), vol. 3, no. 3, pp. 37--49. (2011).
24. Mulle, J., Stackelberg, S., Bohm, K.: Modelling and transforming security constraints in privacy-aware business processes. In: IEEE International Conference on Service-Oriented Computing and Applications, pp. 1--4. IEEE. (2011).
25. Kandias, M., Virvilis, N., Gritzalis, D.: The insider threat in Cloud computing. In: 6th International Conference on Critical Infrastructure Security, pp. 93--103. Springer. (2013).
26. Rodríguez, A., Fernández-Medina, E., Piattini, M.: A BPMN extension for the modeling of security requirements in business processes. In: IEICE Transactions on Information & Systems, vol. 90, no. 4, pp. 745--752. (2007).
27. Altuhhova, O., Matulevičius, R., Ahmed, N.: An extension of business process model and notation for security risk management.
28. Mundie, D., Moore, A., McIntire, D.: Building a multidimensional pattern language for insider threats. In: 19th Pattern Languages of Programs Conference, vol. 12. (2012).
29. Kandias, M., Stavrou, V., Bosovic, N., Gritzalis, D.: Proactive insider threat detection through social media: The YouTube case. In: 12th ACM Workshop on Workshop on Privacy in the Electronic Society, pp. 261--266. ACM. (2013).
30. Kandias, M., Mitrou, L., Stavrou, V., Gritzalis, D.: Which side are you on? A new Panopticon vs. Privacy. In: 10th International Conference on Security and Cryptography, pp. 98--110. (2013).
31. Federal Bureau of Investigation: The insider threat: An introduction to detecting and deterring an insider spy. (2012). http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat
32. Steele, R.: Open source intelligence. In: Handbook of intelligence studies, pp. 129. (2007).
33. Simitis, S.: Reconsidering the premises of labour law: Prolegomena to an EU regulation on the protection of employees' personal data. In: European Law Journal, vol. 5, pp. 45--62. (1999).
34. Broughton, A., Higgins, T., Hicks, B., Cox, A.: Workplaces and Social Networking - The Implications for Employment Relations. Institute for Employment Studies, UK. (2009).
35. Lasprogata, G., King, N., Pillay, S.: Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the EU, US and Canada. In: Stanford Technology Law Review 4. (2004).
36. Fazekas, C.: 1984 is Still Fiction: Electronic Monitoring in the Workplace and US Privacy Law. In: Duke Law & Technology Review, pp. 15--15. (2004).
37. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Accessing n-order dependencies between critical infrastructures. In: International Journal of Critical Infrastructure Protection, vol. 9, nos. 1-2, pp. 93--110. (2013).
38. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: A multi-layer criticality assessment methodology based on interdependencies. In: Computers & Security, vol. 29, no. 6, pp. 643--658. (2010).

39. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Risk-based criticality analysis. In Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection, Springer, USA. (2009).