Insider Threat: Enhancing BPM through Social Media

Dimitris Gritzalis, Vasilis Stavrou, Miltiadis Kandias, George Stergiopoulos
Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business (AUEB)
76 Patission Ave., GR-10434, Athens, Greece
{dgrit, stavrouv, kandiasm, geostergiop}@aueb.gr

***Abstract*—Modern business environments have a constant need to increase their productivity, reduce costs and offer competitive products and services. This can be achieved via modeling their business processes. Yet, even in light of modelling's widespread success, one can argue that it lacks built-in security mechanisms able to detect and fight threats that may manifest throughout the process. Academic research has proposed a variety of different solutions which focus on different kinds of threat. In this paper we focus on insider threat, i.e. insiders participating in an organization's business process, who, depending on their motives, may cause severe harm to the organization. We examine existing security approaches to tackle down the aforementioned threat in enterprise business processes. We discuss their pros and cons and propose a monitoring approach that aims at mitigating the insider threat. This approach enhances business process monitoring tools with information evaluated from Social Media. It exams the online behavior of users and pinpoints potential insiders with critical roles in the organization's processes. 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 only allowed on exceptional cases, such as protecting critical infrastructures.**

Keywords—Insider Threat; Social Media; Business Process; Business Process Management; Privacy; Monitoring;

I. INTRODUCTION

Enterprises and organizations operate in a constantly changing environment. The rapid growth of ICT technologies, along with the globalization of business activities, has given way to new opportunities but also created a need for new operational structures that can take advantage of the coming novelties. This dynamic environment includes the competition for qualitative products and services, reduced costs and fast development. Therefore, each organization is recommended to develop business processes that meet the above mentioned requirements, while ensuring the fulfillment of the goals set.

A business process is defined [1] as "*a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer*". It consists of a set of activities and tasks that, together, fulfill an organizational goal.

To this end, modeling the business processes of an organization augments its flexibility and competitiveness in business environments. Modelling often includes Business Process Management (BPM) [2] a holistic approach to address 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. ERP systems), or manually. Specifically, in an enterprise environment, some process tasks may be performed manually, while others may be computer-based, or even performed sequentially 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.

Our research focuses on mitigating the insider threat using a combination of business process security, together with the human factor that interferes with them. We review existing technical approaches that are used to integrate such mechanisms into business processes. We further examine the applicability of psychometric evaluations that can be utilized in order to predict delinquent human behavior. By applying monitoring approaches to business level we claim that one is able to detect performance deviations of the users and also enhance these processes with information extracted from social media and Open Source INTelligence (OSINT). A possible deviation in employee's performance could be further examined by her behavior within the context of social media to proactively detect an insider threat.

One may argue that business process modeling, mainly during its first stages, lacks built-in security mechanisms to prevent a malevolent functional unit to cause harm to the organization through the operated process. Thus, various approaches have been introduced to enhance business process security, including the development of processes that are secure by design [4]. Although role-based access control [5] is used in various approaches, the insider threat [6] usually fails to be mitigated, leading us to consider that more approaches may be taken into account.

In the battle against the insider threat, organizations use several forms of monitoring in order to detect potential malevolent content. Malevolent content leads to employees posing as potential insider threats. Such monitoring forms vary, from system call activity [7] to linguistic analysis of electronic communications [8]. Another useful insider threat protection mechanism tracks business processes [9] and provides logging information about them. Information acquired through this mechanism 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]. Social

media users tend to transfer their offline behavior to the online world [12]. Thus, a monitoring mechanism could combine the monitoring of a business process with the online psychosocial profile of the functional unit that operates it. The outcome of this combination provides a holistic perspective of the users that operate an organization's business processes. The contribution of such an approach lies on the fact that, though depending on the psychometric evaluations extracted from the online world of the employee, it is possible to detect business processes that may have an increased risk to be exploited by a potential insider.

In this paper we present a business process monitoring model that combines monitoring at runtime level. Its input is comprised of psychometric evaluations, extracted from social media user profiles that belong to an organization's employees. Online monitoring can facilitate the 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 must be taken into consideration. Consequently, a monitoring process like the one presented in this paper, can be ethically and legally acceptable only in cases involving high societal risk (as in critical infrastructures where national security, economic prosperity, and national well-being are at stake) or in cases where a user's explicit consent has been given.

The paper is organized as follows: In section 2 we briefly review the existing literature. In section 3 we present approaches in business process security. In section 4 we discuss the security approaches to mitigate the insider threat in business process. In section 5 we present a business process monitoring model. 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.

II. Related Work

It appears that there exists no research that combines both business and psychometric monitoring to proactively detect potential insider threats. Thus, we examine approaches used to enhance business process security, under the prism of insider threat mitigation via a) psychosocial approaches that predict malevolent behavior and b) monitoring techniques that have been used against the insider threat.

Security in business processes involves methodologies that target exactly at satisfying requirements in their development phase [13]. Thus, certain modelling languages methodologies such as secure UML [14] and secure BPMN [15] have been developed, in an effort to create models with embedded security requirements that generate robust system architectures, including access control infrastructures.

Regarding insider threat prediction, various approaches have been proposed [16]. Research has examined the psychosocial traits that indicate predisposition of delinquent behavior [17]. Modern approaches indicate that such characteristics can be extracted through social media. To this extend, conclusions over traits, such narcissism [10] or predisposition towards law enforcement [11], have been successfully extracted via Twitter and YouTube respectively, leading towards the ability of online monitoring of users behavior so as to detect potentially malevolent users.

Insiders are also detected by monitoring techniques. At system level, LUARM [18] can be used to accurately specify insider threats by logging user actions in a relational model, as a forensic mechanism. Additionally, 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].

III. Business Process Security

Business process modeling constitutes a vital factor for the majority of the organizations, since it has a critical role in the development of information systems. One may notice that business processes have a tendency towards becoming more vulnerable as the number of their participants grows in number. Thus, exploiting a critical process can have a severe impact on an organization.

The participating functional units in a business process may cooperate and communicate sufficiently, forming a competitive advantage for the organization; however, several security issues regarding the security of the process involved may rise. To this end, security issues should be dealt during the analysis and design of the business process.

The majority of business processes should include a part of the following security requirements [19]:

- User **authorization** defines which users are allowed to operate or participate in a process. Security mechanisms should restrict permission only to required resources and data and only for a specific time period for each operating user. This requirement includes the role management of the users involved in business processes.
- User **authentication** assures that a process allows access only to authorized users and denies access to the rest. Successful authentication is a challenge for system designers, security experts and for the modelling tools.
- Business process **auditing** defines that each process is supervised in order to detect erroneous actions. Auditing involves log file analysis regarding process execution, messaging flows, communication with external processes to the environment, etc.
- **Confidentiality** refers to unauthorized access to systems or resources by processes or users not allowed to.
- **Data integrity** forms an important part of a business process. Thus, for any process that is corrupted or suddenly terminated should be guaranteed that none of the data involved are lost.

IV. Insider Threat Mitigation

Insider threat is a major issue in corporate security and has also been detected as a cloud systems threat [20]. Various approaches, countermeasures and techniques have been used to mitigate the issue, including security policies, procedures and technical controls. Each organization should examine its design

functionality, to tackle the threat at its business process level. Namely, the mitigating stages at process level are the following:

- **Design secure business processes** by extending the annotation of existing modeling languages such as BPMN so as to encapsulate security requirements. For example existing modeling languages can be extended to support features regarding integrity, confidentiality and access control [21].
- **Risk assessment** [22] at business process level to evaluate the risk involved in each process, regarding the security needs and the environment in which each process is deployed. Thus, proper risk management ensures the balance of operational and economic costs of protective measures and security policies for senior information technology managers.
- **Monitoring each business process** of the organization and extracting conclusions. This may contribute in locating and redesigning problematic procedures and reduce the risk of an insider threat incident.

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

V. PROPOSED MODEL

CERT's research has focused on analyzing a vast number of insider threat cases and identified various weaknesses in parts of the organization that facilitated the manifestation of such incidents. Part of the research's outcome has led to 26 enterprise architecture patterns developed as means of protection from malevolent insiders [23]. Among the patterns developed by CERT, we focus on the following:

- **Monitoring the organization**: This pattern suggests the institution of a monitoring program that collects information on the status of insider threats and incidents within the organization. Thus, the organization can obtain an estimation of the risk involved by malicious insider activity.
- **Monitoring employees**: The organization should establish a legal, affordable and effective monitoring system that is acceptable to all stakeholders. Monitoring results should be secured and should be used solely on the purpose of optimizing resources and not for discriminative purposes.
- **Use optimized monitoring for early detection**: Organizations should configure their infrastructures in a way that insider attacks are detected in a short time period.
- **Combine technical and behavioral monitoring**: Technical and behavioral monitoring can increase the effectiveness of insider threat detection. Such an approach involves alert sharing and trusted teams that are authorized to access all data within the organization, so as to investigate and detect malicious actions.
- **Use external sources of information**: This pattern suggests the use of external information sources, such as social networks, in order to expand employees monitoring.

Taking into consideration the above mentioned patterns, we propose a monitoring approach that combines enterprise level monitoring with the monitoring of information extracted by social media. Towards assessing the human factor we decided to integrate mechanisms we have already developed in previous work of ours. These mechanisms are able to extract psychometric evaluations from social media to enhance the insider threat prediction front. Additionally, existing business monitoring tools can be further expanded to receive inputs regarding the psychometric evaluations. Such tools are able to perform monitoring of the organizational processes and also record the users involved in each one.

Work presented in this paper focuses on two of the above mentioned CERT's patterns: (a) "Use external sources of information" and (b) "Combine technical and behavioral monitoring". Remaining patterns can be utilized using existing, conventional monitoring tools.

This work focuses on further enhancing existing monitoring tools by combining external sources of information (such as social media) with technical and behavioral patterns. To this end, we build upon our previous research and propose the following architecture:

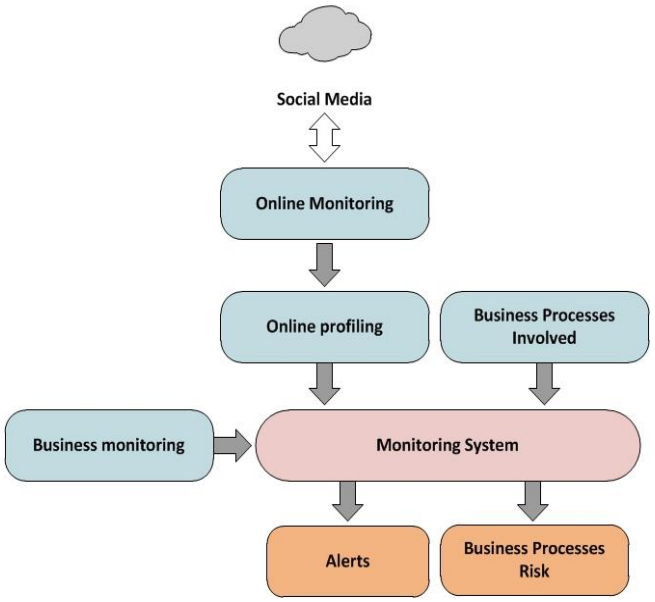

Fig. 1. Monitoring system's architecture

The depicted architecture receives the following types of input: (a) data from business monitoring, regarding employees' performance, (b) online monitoring, which involved data acquired from social media, and (c) the processes that the user under examinations is involved into. The output comes into the form of potential incident alerts and the risk that characterizes the processes of the organization.

Online monitoring can facilitate the process of behavioral analysis carried out on information system's users, as manifested in the digital world. Additionally it detects patterns of characteristics that are commonly shared among insiders. This way, when a user happens to manifest such characteristics in the online world, the monitoring system will issue *alerts* and highlight

the business processes that user is involved into. Then, the operator of the *monitoring system* can further examine the alerts and draw conclusions over the user's performance through the *business process monitoring* module.

We consider online monitoring to be an important component of the proposed approach. Insider threat mitigation forms a vital factor for an organization. Traits such as narcissism [10], predisposition towards law enforcement [11] and divided loyalty [25] can be extracted from social media profiles and detect potential insider threats, as a success or horror story respectively. The above mentioned traits have been examined and detected through social media and can facilitate the insider threat prediction in the digital world. Fig. 2 presents the psychosocial traits examined to detect a potential insider via her online behavior.

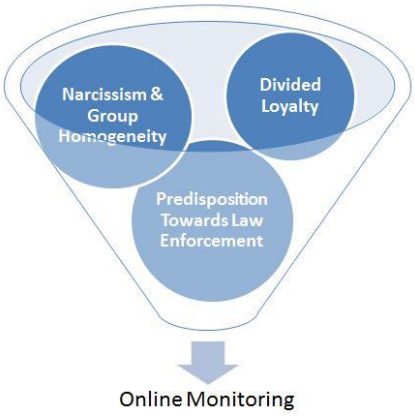

Fig. 2. Online monitoring psychosocial traits

The above mentioned traits have been the topic of interest in Shaw's research [17] and have been also examined by the FBI [26], indicating that the human factor is an important part in the insider threat mitigation.

Online monitoring can improve in efficiency by using open-source intelligence techniques (OSINT) [27]. OSINT refers to intelligence collected from publicly available sources, such as websites, web-based communities (i.e. social networks, forums, or blogs) and publicly available data (Fig. 3). Techniques such as these facilitate the extraction of knowledge that is not easily accessible.

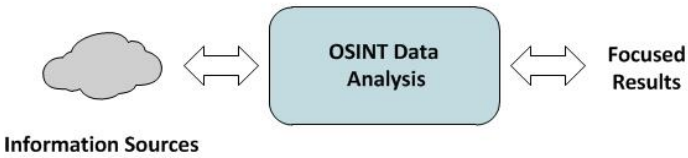

Fig. 3. Open-source intelligence perspective

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 is publicly available, since most of them neglect to use any privacy mechanisms offered. Consequently, anyone interested in collecting such data is free to gather information and analyze it for conclusions. Anyone can be targeted. Forums posts, personal blogs and any public source can be used to gather material offered by the user on his own, free will.

OSINT processes rely on vast amounts of reliable information. It is because of this that the following key points must be taken into consideration:

- **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, it could be useful to further process the results in order to focus on the required knowledge.

The approach introduced in Fig. 1 can be further enhanced by the ability to categorize the organization's business processes regarding the risk they face due to potential insiders that operate them. Thus, a business process risk analysis methodology could be enhanced by taking into consideration the risk involved by the psychosocial traits of its operator. When a potential insider employee is involved in critical business processes, the impact of a malevolent manifestation might be quite severe.

The proposed approach examines the processes by 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 the impact to the organization due to a possible loss of confidentiality, integrity or availability. Thus, the more important the asset is, the severer the impact. Complementary, the *risk involved by the human factor* corresponds to the predisposing of delinquent behavior that characterizes the user's online behavior. The described discrimination contributes in the protection of critical processes, since both risk factors are taken into consideration.

The contribution of this model lies on the fact that human factor has rarely been examined in monitoring systems, which have focused solely on technical countermeasures. Contributions aside, monitoring users at their workspace to evaluate their performance and online behavior may give rise to several ethical and legal issues. These issues are discussed in the sequel.

VI. Etchical And Legal Issues

Workspace monitoring raises several ethical and legal issues, as it is no longer performed in the workspace per se, but is extended to the online world of social media. Monitoring the online behavior and social communication relationships of employees augments the chances of employers to influence behavior and promote the "well-adjusted employee" [28]. 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" [29] and thus refrain from expressing themselves.

Employees are often asked to sacrifice privacy rights to managerial interests like productivity, prevention and detection of

threats. 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 judged under all the circumstances and must 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 [30].

The European approach seems diametrically opposite in many respects: 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. 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, carrying far-reaching consequences in terms of social selection and unjustified discrimination.

Finally, it has been demonstrated that excessive monitoring affects the employer-employee relationship. While studying citizens employed in the same organization, it has been showed that employees whose communications were monitored, suffered from higher levels of depression, anxiety and fatigue than those who were not [31]. The effect of being constantly monitored even concerning activities that fall out of the workplace frame has negative impacts on the employer-employee relationship that should be based on mutual trust and confidence.

VII. Conclusions

In this paper we dealt with insider threat mitigation at business process level. We approached the issue by proposing a structural method that combines monitoring at process level with psychosocial monitoring through social media. Judging from the results, malevolent insiders have been found to share common characteristics and research has indicated that the extraction of them through social media is feasible. Thus, a mechanism able to integrate psychosocial evaluation to a business activity monitoring system could enhance corporate security against the insider threat.

Screening employees in both business level and online behavior through social media raises several ethical and legal issues. We interpolate the principle of proportionality regarding the implementation of the proposed system. We consider that the use of such methods should be confined solely on critical infrastructures, along with user's consent. In this way the protection of such infrastructures could be improved [32][33].

For future work we plan on proposing implementation techniques of the proposed approach and further examine a business process risk analysis methodology that takes into consideration the psychosocial characteristics of the functional unit that operates it. Finally, we plan on further examining the legal aspects of the issue, so as to strengthen employee protection against monitoring techniques.

References

[1] M. Hammer, J. Champy, "Reengineering the corporation: A manifesto for business revolution", A. HarperCollins, 2009.

[2] M. Weske, "Business process management: concepts, languages, architectures", Springer, 2012.

[3] D. Karagiannis, "Business process management: A holistic management approach", Information Systems: Methods, Models, and Applications, pp. 1-12, Springer Berlin Heidelberg, 2013.

[4] D. Gollmann, "From insider threats to business processes that are secure-by-design", INCoS, pp. 627, 2011.

[5] D. Basin, J. Doser, and T. Lodderstedt, "Model driven security: From UML models to access control infrastructures", ACM Transactions on Software Engineering and Methodology, vol. 15, no. 1, pp. 39-91, 2006.

[6] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799", Computers & Security, vol. 24, no. 6, pp. 472-484, 2005.

[7] N. Nguyen, P. Reiher, and G.H. Kuenning, "Detecting insider threats by monitoring system call activity", Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, pp. 45-52, IEEE, 2003.

[8] C. Brown, A. Watkins, and F. Greitzer, "Predicting insider threat risks through linguistic analysis of electronic communication", System Sciences, 46th Hawaii International Conference on, pp. 1849-1858, IEEE, 2013.

[9] D. Grigori, F. Casati, M. Castellanos, U. Dayal, M. Sayal, and M. Shan, "Business process intelligence", Computers in Industry, vol. 53, no. 3, pp. 321-343, 2004.

[10] M. Kandias, K. Galbogini, L. Mitrou, and D. Gritzalis, "Insiders trapped in the mirror reveal themselves in social media", Proc. of the 7th International Conference on Network and System Security Conference, pp. 220-235, Springer, 2013.

[11] M. Kandias, V. Stavrou, N. Bozovic, L. Mitrou, D. Gritzalis, "Can we trust this user? Predicting insider's attitude via YouTube usage profiling", Proc. of the 10th International Conference on Autonomic and Trusted Computing, pp. 347-354, IEEE, 2013.

[12] Y. Amichai-Hamburger and G. Vinitzky, "Social network use and personality", Computers in Human Behavior, vol. 26, pp. 1289-1295, 2010.

[13] M. Backes, B. Pfitzmann, and M. Waidner, "Security in business process engineering", Business Process Management, pp. 168-183, Springer, 2003.

[14] J. Jürjens, "Secure systems development with UML", Springer, 2005.

[15] A. Brucker, I. Hang, G. Lückemeyer, and R. Ruparel, "SecureBPMN: Modeling and enforcing access control requirements in business processes", Proc. of the 17th ACM Symposium on Access Control Models and Technologies, pp. 123-126, ACM, 2012.

[16] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model", Proc. of the 3rd International Conference on Trust, Privacy and Security in Digital Business, pp. 26-37, Springer, 2010.

[17] E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider", Security Awareness Bulletin, vol. 2, no. 98, pp. 1-10, 1998.

[18] G. Magklaras, S. Furnell, and M. Papadaki, "LUARM: An audit engine for insider misuse detection", International Journal of Digital Crime and Forensics, vol. 3, no. 3, pp. 37-49, 2011.

[19] J. Mulle, S. von Stackelberg, and K. Bohm, "Modelling and transforming security constraints in privacy-aware business processes", Proc. of the IEEE International Conference on Service-Oriented Computing and Applications, pp. 1-4, IEEE, 2011.

[20] M. Kandias, N. Virvilis, and D. Gritzalis, "The insider threat in Cloud computing", Proc. of the 6th International Conference on Critical Infrastructure Security, pp. 93-103, Springer, 2013.

[21] A. Rodríguez, E. Fernández-Medina, M. Piattini, "A BPMN extension for the modeling of security requirements in business processes", IEICE Transactions on Information & Systems, vol. 90, no. 4, pp. 745-752, 2007.

[22] O. Altuhhova, R. Matulevičius, and N. Ahmed, "An extension of business process model and notation for security risk management".

[23] D. Mundie, A. Moore, and D. McIntire, Building a multidimensional pattern language for insider threats, CERT, Carnegie Mellon University, USA, 2012.

[24] M. Kandias, V. Stavrou, N. Bosovic, and D. Gritzalis, "Proactive insider threat detection through social media: The YouTube case", Proc. of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society, pp. 261-266, ACM, 2013.

[25] M. Kandias, L. Mitrou, V. Stavrou, and D. Gritzalis, "Which side are you on? A new Panopticon vs. Privacy", Proc. of the 10th International Conference on Security and Cryptography, pp. 98-110, 2013.

[26] 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

[27] R.D. Steele, "Open source intelligence. Handbook of intelligence studies", pp. 129, 2007.

[28] S. Simitis, "Reconsidering the premises of labour law: Prolegomena to an EU regulation on the protection of employees' personal data", European Law Journal, vol. 5, pp. 45-62, 1999.

[29] A. Broughton, T. Higgins, B. Hicks, and A. Cox, "Workplaces and social networking - The implications for employment relations", Institute for Employment Studies, Brighton, 2009.

[30] G. Lasprogata, N. King, and S. Pillay, "Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, US and Canada", Stanford Technology Law Review 4, 2004.

[31] C. Fazekas, "1984 is still fiction: Electronic monitoring in the workplace and US privacy law", Duke Law & Technology Review, pp. 15-15, 2004.

[32] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Accessing n-order dependencies between critical infrastructures", International Journal of Critical Infrastructure Protection, vol. 9, nos. 1-2, pp. 93-110, 2013.

[33] M. Theoharidou, P. Kotzanikolaou, and D. Gritzalis, "A multi-layer criticality assessment methodology based on interdependencies", Computers & Security, vol. 29, no. 6, pp. 643-658, 2010.