Insider Threats: The Major Challenge to Security Risk Management

Teresa Pereira[1(✉)] and Henrique Santos[2]

[1] Polytechnic Institute of Viana do Castelo, Viana do Castelo, Portugal
tpereira@esce.ipvc.pt
[2] University of Minho, Guimarães, Portugal
hsantos@dsi.uminho.pt

Abstract. Security risk management is by definition, a subjective and complex exercise and it takes time to perform properly. Human resources are fundamental assets for any organization, and as any other asset, they have inherent vulnerabilities that need to be handled, i.e. managed and assessed. However, the nature that characterize the human behavior and the organizational environment where they develop their work turn these task extremely difficult, hard to accomplish and prone to errors. Assuming security as a cost, organizations are usually focused on the efficiency of the security mechanisms implemented that enable them to protect against external attacks, disregarding the insider risks, which are much more difficult to assess. All these demands an interdisciplinary approach in order to combine technical solutions with psychology approaches in order to understand the organizational staff and detect any changes in their behaviors and characteristics. This paper intends to discuss some methodological challenges to evaluate the insider threats and its impacts, and integrate them in a security risk framework, that was defined according to the security standard ISO/IEC_JTC1, to support the security risk management process.

Keywords: Information security risk · Security risk management · Insider risk · Insider threats and insider behavior

1 Introduction

Information systems security and communication technologies have received a significant attention, especially in the last decade. This includes various dimensions of computer and network security and several application domains (e.g. critical infrastructures such as banking, energy, transportation systems and networks). Information security (or cyber security) has been recognized increasingly critical to society today, since its well being is highly dependent on the performance of information systems and communication technologies [1]. However, more and more citizens and businesses are likely to suffer security breaches, which not only damage reputation but can also cause heavy financial losses, usually difficult to recover from. Such security breaches may be

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 654–663, 2015.
DOI: 10.1007/978-3-319-20376-8_58

IT related, for example through computer viruses or other malicious software, system failure or data corruption, or may be socially motivated, for example through theft of assets or other incidents caused by direct human action.

Security risks arise from multiple sources and motivations, are very dynamic and consequently demand a proper management. In general, organizations are more focused on being protected against external attacks and threats to ensure the confidentiality, integrity and availability of their information assets, often without considering insider threat. In fact, there are several studies [1, 20] arguing that there are more threats coming from the inside then from anywhere else. It is undoubtedly the risks raised from insider threat are an important issue, with severe consequences to an organization. Therefore insider threat has to be included and treated in the security risk management process, the same way the traditional technical vulnerabilities are handled. Due to the different organizations' environments and the diverse natures of human behavior, it is required to consider the involvement of psychological approaches in combination with technological mechanisms, to understand and observe any changes in employees' behaviors and characteristics. In fact, it is important to know how well a particular set of technological controls is functioning, but it is much more important for decision makers to be able to "know what they don't know", or what is hidden in the human behavior, which can derive in a security risk.

In this context, the goal of this paper is to discuss some methodological challenges to evaluate the insider threats and its impacts, and integrate them in a security risk framework, that was defined according to the security standards ISO/IEC_JTC1, to support the security risk management process. This paper is structured as follows: in Sect. 2, some reflections regarding the risk evaluation of insider threats and its role in the risk management process are presented; Sect. 3 focuses on an overview of current approaches to address insider threats; in Sect. 4 a security risk framework and proposed methodological challenges to be included in the security risk management process are highlighted; and conclusions are presented in Sect. 5.

2 Risk Insider Threat and Security Risk Management

Nowadays, the security risk management process is well accepted and widely used by organizations. Security standards guide the information security administrator to identify critical assets and processes, to define objectives and to identify proper security controls as a main input to the risk management model. Nevertheless, security managers consider these standards not covering all the organizational security needs, mostly because they fail to address the requirements concerning assessment, which is fundamental to measure efficiency. Despite some guides towards characterization of what a good metric is, there is a long way to find models enabling objective and helpful assessments, especially within human-oriented security controls [3].

Risk is defined by the standard ISO/IEC FDIS 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary [4], as the relation between the probability of occurrence of an event and its impacts.

In simple terms, when modeling risk, human threat can be decomposed into the factors of motivation, opportunity and capability. This approach is generally referred to as CMO Model asserting that to commit an attack, the perpetrator must first have the [5]:

- Capability: the skills to commit the attack.
- Motive: the reasons to commit an attack.
- Opportunity: the time-window and/or settings required to commit an attack.

These factors should be included in insider threat management, because the impact of insider threats can occur in multiple dimensions, such as financial loss, disruption to the organization, loss of reputation, and long-term impacts on organizational culture. These impacts are extremely difficult to measure or quantify. For example, an organizational bonus distribution may result in actions taken with angry, revenge, compensation, et cetera, with severe impacts on diverse levels of an organization. Thus, a minor or meaningless motivation can have a huge impact. In the same way, the impact may not be strictly dependent on motivation, since an accidental or unintentional act can have the same dramatic effect as a malicious motivated attack. Therefore, the main goal should be focused on avoiding crucial consequences regardless the motivation. These aspects as well as other risk accelerators should be represented in a security risk management process.

Lastly, it still remains unclear how efficient are the indicators used to assess the various prevention, detection and response techniques, in mitigating and reducing insider threat and consequently in reducing related vulnerability. In practice, there is a lack of data and studies that enable to evaluate the efficiency and effectiveness of different security policies against acts stemming from different motives.

3 Current Approaches

Currently a number of independent bodies have developed well-documented methodologies for assessing risk. In IT security, perhaps the best well known is Carnegie-Mellon's OCTAVE method [6]. Other worthy methods include (or are part of) COBIT [7], ITIL [8], CORAS [9], ISRAM [10] and CRAMM [11], as well as others that are presented and listed by ENISA [12]. However, the studies about these practices implemented in real environments reveal a poor effectiveness of the information security management processes [13, 14]. Moreover, Sadok and Spagnoeletti demonstrate with their studies that enterprises implementing widely used security practices continue to experience difficulties regarding assessing and managing their security risks, implementing appropriate security controls, and preventing security threats. This is because the available information security risk management models and frameworks mainly focus on the technical aspects of security, and do not pay much attention to the influence of environmental and insider-related problems, such as users motivation and behavior, on the reliability of the provided solutions [13, 15, 16].

In the scope of insider threats, several models have been proposed in the literature review. Some models are more focused on the prevention and detection of insider threats and others are following technical approaches. Facing a more prevention and detection-oriented approach, Schultz [2] proposes a framework for understanding and predicting insider attacks essentially based on personality traits and verbal behavior. Another model brought up by Wood [5], uses the attributes of users' knowledge, privileges and skills metrics. Moreover, Hidden Markov Models [17] have been aligned with other activity models to infer divergence activity patterns of a user. Other sciences such as psychology have been drawn up, in order to achieve the identification of an insider profile through the identification of personnel attributes, such as introversion and depression. From the background of psychology, Caputo *et al.* [18] investigate the relation between intent and user action based on the development of experimental tests. In addition, Theoharidou *et al.* [19] relates to criminology theories, designed to measure insider misuse and explore the possible enhancements to the standard ISO17799 [19]. Finally, Kandias *et al.* [20] present a model aim to predict insider behavior, through the use of user taxonomy, psychological profiling and a decision algorithm in order to identify potentially dangerous users. This model introduces a more interdisciplinary approach, since it combines technical solutions with approaches that draw upon psychology [20].

On the technical approach, Intrusion Detection Systems (IDS), in various technological architectures, are widely used, in particularly on the detection of insider violations of security policies in place. An IDS system intents to monitor the abnormal activity within the information system on a regular basis. This can be achieved using several technologies from the AI (Artificial Intelligence) area, such as the system presented by Cappelli *et al.* [21], which is based on machine learning algorithms, to analyze collected search events to detect anomalous user search behavior. Moreover, Duran [22] presents a system that models the user life cycle to analyze user interaction with insider security protection strategies. Other approaches are based on the production of baits, in order to detect potential insider abuses. The main goal is to detect derivations from an expected behavior, usually described in a security policy. However, the ultimate threats are those that don't leave a technological detectable trail in the system or make use of normal activities to undertake malicious actions.

There are multiple well-known direct sources that enable the analysis and anomalous behavior and from where a risk alert may result. This information is available from tools that an organization may already possess and use, such as security information and event management tools, like OSSIM, McAfee Enterprise Security Manager, UmbroData, Digital Attack Map, Unisys Security Index, IP reputation, among others. In addition, we can extend this list to indirect sources that typically publish information related with security threats, such as CERT repositories, CAPEC (Common Attack Pattern Enumeration and Classification enumerations and classifications), Google Help Net Security, CVE, ATLAS threat index, among others. From this information sources, it is expected that several security indicators emerge. However, to automatically process these information, it is important to (1) understand exactly what is being measured and give (useful) meanings to values; and (2) develop and define a flexible enough model framework aiming on machine based processing, as similarly seen in security policies computational enforcement frameworks. Since information security, by definition, imposes restriction to flexibility and consequently may impact business negatively, it is also desirable to carefully align security policies with business objectives. This dimension should also be part of the set of metrics used to assess risks and security controls' efficiency.

Despite there exists a substantial number of models addressing insider threats, they tend to solve the problem in a limited point of view, focusing on dedicated metrics which are very difficult to integrate in a unified risk assessment approach [20, 23]. In the following section, we present a model that structure a hierarchy of security concepts, in order to facilitate a proper management of information security risks, emphasizing some methodological challenges due to organizational insider threat.

4 A Conceptual Model Developed in the Context of IS Security Risk Management

The study work in the field of attacks, threats and assets' vulnerabilities concerning information systems continues to grow because they are evolving and have a significantly impact. Managing such an environment requires both a detailed understanding of security concepts and their relationships. The concepts defined in the conceptual model are based on a wide recognized standard, produced by ISO/IEC_JTC1 (the ISO/IEC 27000). The hierarchical relation between the concepts assists organizations with regard to an implementation of the right combination of protection controls to mitigate security risks. In practice, the implementation of a conceptual model, richly represents security concepts and their relationships in terms of threats, attacks, vulnerabilities, assets and countermeasures, and thus facilitates a more efficient management of information systems security [24].

The advantages of this approach to organizations are:

1. a proper identification of the valued or critical assets
2. an accurate identification of the assets vulnerabilities
3. to be able to identify and mitigate potential threats
4. a proper evaluation of organizational risks
5. an adequate evaluation of the efficiency and effectiveness of the security policies and safeguards defined and therefore analyze and implement the necessary adjustments to security policy adopted.

The defined conceptual model comprises 8 concepts and 16 relationships, and is built up as a hierarchy structure, as illustrated in Fig. 1. These concepts are described as follows [26]:

Incident: a single or series of unwanted or unexpected events that might have significant probability to compromise the information system security.

(Security) Event: an identified occurrence of a particular set of circumstances that changed the status of the information system security.

Asset: any resource that has value and importance to the organization, which includes information, programs, network and communications infrastructures, software, operating systems, computers and people.

Confidentiality, integrity, availability properties (CIA): the information properties to be ensured, namely confidentiality, integrity and availability; besides these aspects, main security properties, and depending on the context, other security properties may need to be addressed, such as authenticity, accountability and reliability.

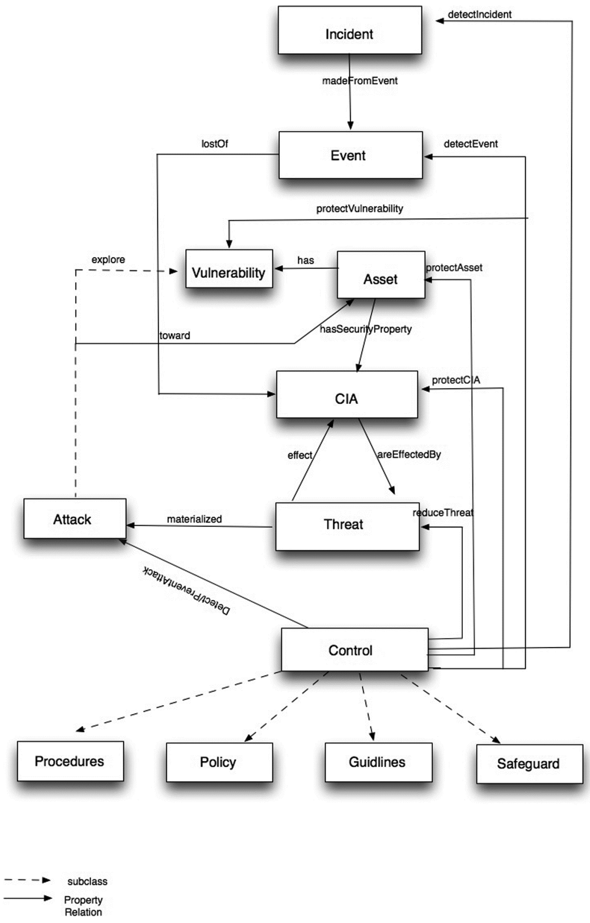

Fig. 1. Hierarchical concepts defined in the conceptual model [26]

Threat: the types of dangers against a given set of properties (security properties). The attributes defined in this concept follow the Pfleeger approach [25], which includes an attacker (insider or external), actions or a position to perform an interception, fabrication, modification and interruption, over a resource.

Attack: a sequence of actions executed by some agents (machine-aided or manual) exploring any vulnerability.

Control: mechanisms used to detect an incident or an event, to protect an asset and security properties, to reduce a threat and to minor or prevent the effects of an attack.

Vulnerability: represents any weakness of the system.

In short, the rationale behind this model is structured as follows: an incident is made from – *madeFromEvent* – events; the occurrence of an event can lead to a loss of – *lostOf* – a set of security properties (CIA); an asset has security properties – *hasSecurityProperties* – and each one can be affected by a threat, while a threat can affect one or more security properties and finally, an asset has vulnerabilities. A threat is materialized by an attack, while the attacks exploit one or more vulnerabilities; an attack is also triggered toward an asset. Furthermore, the implementation of control mechanisms help to reduce threats, are able to detect and prevent an attack, to protect security properties, to protect assets and vulnerabilities, as well as to detect events, in order to protect assets [26].

The standard, and consequently the conceptual model, do not go into fine grain details concerning the concept's characterization when different views are possible. For instance, the attack concept can be characterized by the use of a taxonomy, taking in account different views, purposes or even perceptions [27]. However, there is nothing limiting the possibility of extending concept classes, for instance, regarding a definition of attack classes with common characteristics, all deriving from the same main fundamental concept. This feature gives the opportunity of customization, but with the risk of a decrease of generalization, if not used carefully. Moreover, the developed model was defined according to the security standard ISO/IEC 27000, exhibiting a simplicity and a high flexibility, which enables its adoption by any organization, regardless their business activity. However, to address the protection and mitigation of threats to information assets, the organization must consider other domains, including the socio-physiological and socio-organizational domains [28]. In general, information security management is primarily focused on technical issues concerning the design and implementation of security systems, technical approaches to prevent intrusion into organizational systems, detection of denial of services attacks, and more advanced solutions for firewall protection. Although, these technical approaches are highly focused on external threats and are important, the individual user actions inside an organization are also a meaningful weakness with significant impact [2, 17–22]. In this context, it is underlined the need to relate two different components – the psychological profile component and the IT component of an information system, in order to collect useful information about internal users. Anyhow, the psychological component needs further investigation/attention. However, the main concern is to identify a set of relevant instruments, to enable the definition of potential insider threat profiles. In practice, it must be considered an analysis of organizational users' behavior related to information security, their attitudes concerning the use of technologies and their estimations about risks in the context of their daily work. This analysis must be framed (and supported) by the organization's business strategy, including an alignment with other regulations and/or obligations.

After the risk assessment, the Chief of the Information Security Officer has all the information required to define an adequate security policy. However, aiming on the necessary managerial aspects of information security, he/she also needs to put in place the measuring process to (1) keep risk evaluation under surveillance; and (2) evaluate the efficiency of security controls chosen in order to validate the prior decisions. Desirably, this evaluation should be carried out continuously but can be an impossible task, especially concerning the aspects depending on user behavior. Indeed, if we use interviews or surveys to measure the desirable indicators and since the application of such instruments collides with the usual working tasks, we can easily figure out a negative impact on business, which will not be admissible. So we need to look for alternative ways of measuring the same behaviors, which may be achieved, at least partially, by profiling users' interaction with the help of information systems, for example through logs and events. This information is already available and used mainly for intrusion detection purposes [29], but it is possible to explore it for a more general users' behavior evaluation.

In practice, the methodological challenges include the following research tasks:

- Specification of the psychological and behavioral indicators on well-being, as well on stress/disorders of users, in accordance with the organization's security policy, its culture and legal structure. In practice, a related analysis focuses on the assess of the user's predisposition to malicious behavior;
- Evaluation of IT skills of a user. The goal is to evaluate the user's practical computer, his/her knowledge of organizational networks, databases, and techniques implemented, familiarization with specific technologies, et cetera. These information will enable the organization to identify the users' sophistication attributes;
- Development of an assessment protocol to collect users' information regarding their perceptions, meanings, attitudes and feelings, their security behavior and related risks in their daily work;
- Development of measurement indicators.

An analysis of the mentioned measures will facilitate the identification of unusual behavior within an organization, as well as other measurable insider-related characteristics, which will serve as input to responsible managers, enabling them to assess whether a user is potentially dangerous or not.

Finally, all this activities should be framed by standards used to certify organizations concerning their attitude, towards the growing risks of information security. And since organizations are increasingly interconnected and interdependent, being certified becomes a relevant management goal.

5 Conclusions

It should be accepted that employees are an important organizational' asset, but also probably causing multiple vulnerabilities that must be handled (managed and assessed) as others security vulnerabilities. However, these vulnerabilities involve people and their behaviors, which require an interdisciplinary approach to combine technical solutions with psychological approaches. A better understanding of the psychological behavior of employees and the detection of changes in their behavior and characteristics will enable organizations to gain a better understanding of the real risks and thus face them more efficiently. Meanwhile organizations must be prepared for the cultural, technological, social and economic environment changes, and be able to perform evaluations in a continual basis in order to protect their information assets.

Technology is an essential tool that supports the control accesses to information, and helps in monitoring and detecting malicious activities. Nevertheless, it is the working environment and the organizational staff that will provide the real foundations to success. The security controls must be agile and workable in multiple environments and preferably with end user cooperation, because it will certainly contribute to a better understand of the reasons for security controls implementation.

Insider risks need to be moved up in importance and discussed by decision makers prior to attacks, and not after the occurrence of a significant security incident. Currently, for any business, particularly in the security domain it is important to take proactive measures to stop the occurrence of insider attacks, instead of reactive measures. Risk management and compliance should be extended to create means of recognizing, capturing, assessing and testing insider behavior and its impact. However it is extremely difficult to measure and quantify malicious insiders' behavior unlike the measures of IT components' performance. The security benefits will certainly be higher in a longer-term rather than in a shorter-term. This must be weighted against the organizational priorities. The investments spend to face insider threats may require a substantial justification, but this is the challenge.

Acknowledgements. This work has been supported by FCT - Fundação para a Ciência e Tecnologia in the scope of the project: PEst-UID/CEC/00319/2013.

References

1. Whitman, M., Mattord, H.: Management of Information Security, 4th edn. Cengage Learning, Boston (2013)
2. Schultz, E.E.: A framework for understanding and predicting insider attacks. Comput. Secur. **21**(6), 526–531 (2002)
3. Cohen, F.: How do we measure security? INCOSE Insight **14**(2), 30–32 (2011)
4. ISO/IEC_JTC1: ISO/IEC FDIS 27000 information technology - security techniques - information security management systems - overview and vocabulary. ISO Copyright Office, Geneva, Switzerland (2009)
5. Wood, B.: An insider threat model for adversary simulation. In: Anderson, R.H. (ed.) Research on Mitigating the Insider Threat to Information Systems. RAND (2000)
6. Alberts, C., Dorofee, A.: Managing Information Security Risks: the OCTAVE (SM) Approach, 1st edn. Addison Wesley, Boston (2002)
7. ISACA (2011) COBIT 4.1: Framework for IT governance and control [on-line]. ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx
8. ITIL 2000. Official ITIL® Website [on-line]. itSMF International. The IT Service Management Forum. http://www.itsmfi.org/content/official-itil®-website
9. Stolen, K., den Braber, F., Dirmitrakos, T.: Model-based risk assessment –the CORAS approach (2002). http://www.nik.no/2002/stolen.pdf
10. Karabacaka, B., Songukpinar, I.: ISRAM: information security risk analysis method. Comput. Secur. **24**(2), 147–169 (2005)
11. Yazar, Z.A.: Qualitative risk analysis and management tool – CRAMM. SANS Institute InfoSec Reading Room (2011)
12. ENISA. Inventory of risk management/risk assessment methods [on-line]. European Network and Information Security Agency (2011). http://rm-inv.enisa.europa.eu/rm_ra_methods.html
13. Sadok, M., Spagnoletti, P.: A business aware information security risk and analysis method. In: D'Atri, A., Ferrara, M., George, J.F., Spagnoletti, P. (eds.) Information Technology and Innovation treads in Organization, pp. 453–460. Springer, Heidelberg (2011)

14. Asosheh, A., Dehmoubed, B., Khani, A.: A new quantitative approach for information security risk assessment. In: IEEE International Conference on Intelligence and Security Informatics 2009 (ISI 2009), pp. 229–239, 8–11 June 2009. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5137311&isnumber=5137253. doi: 10.1109/ISI.2009.5137311
15. Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., Courtney, J.: Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Q **37**(4), 1189–1210 (2013)
16. Posey, C., Roberts, T.L., Lowry, P.B., Hightower, R.T.: Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Inf. Manag. **51**(5), 551–567 (2014). doi: 10.1016/j.im.2014.03.009. http://dx.doi.org/
17. Thompson, P.: Weak models for insider threat detection. In: Carapezza, E.M. (ed.) Sensors & Command, Control, Communications & Intelligence (C3I) Technologies for Homeland Security & Homeland Defense III, vol. 5403, pp. 40–48 (2004)
18. Caputo, D., Marcus, A., Maloof, M., Stephens, G.: Detecting insider theft of trade secrets. IEEE Secur. Priv. **7**(6), 14–21 (2009)
19. Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E.: The insider threat to information systems and the effectiveness of ISO17799. Comput. Secur. **24**(6), 472–484 (2005)
20. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D.: An insider threat prediction model. In: Katsikas, S., Lopez, J., Soriano, M. (eds.) TrustBus 2010. LNCS, vol. 6264, pp. 26–37. Springer, Heidelberg (2010)
21. Cappelli, D.M., Moore, A.P., Trzeciak, R.F., Shimeall, T.J.: Common Sense Guide to Prevention and Detection of Insider Threat, 3rd edn. Carnegie Mellon University, Pittsburgh (2009)
22. Duran, F., Conrad, S., Conrad, G., Duggan, D., Held, E.: Building a system for insider security. IEEE Secur. Priv. **7**(6), 30–38 (2009)
23. Beres, Y., Mont, M.C., Griffin, J., Shiu, S.: Using security metrics coupled with predictive modeling and simulation to assess security processes. In: 3rd International Symposium on Empirical Software Engineering and Measurement, pp. 564–573 (2009)
24. Onwubiko, C., Lenaghan, A.P.: Challenges and complexities of managing information security. Int. J. Electro. Secur. Digit. Forensics **2**(3), 306–321 (2009)
25. Pfleeger, C., Shari, L.: Security in Computing, 4th edn. Prentice Hall PTR, Upper Saddle River (2007)
26. Pereira, T.; Conceptual framework to support information security risk management. Ph.D thesis, University of Minho (2012)
27. Hansman, S., Hunt, R.: A taxonomy of network and computer attacks. Comput. Secur. **24**(1), 31–43 (2005)
28. Crossler, R., Johnston, A., Lowry, P., Hud, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. **32**, 90–101 (2013)
29. Oliner, A., Ganapathi, A., Xu, W.: Advances and challenges in log analysis. Commun. ACM **55**(2), 55–61 (2012)