External Insider Threat: a Real Security Challenge in Enterprise Value Webs

Virginia N. L. Franqueira, André van Cleeff, Pascal van Eck, Roel Wieringa
University of Twente
Enschede, The Netherlands
Email: {franqueirav, a.vancleeff, p.a.t.vaneck, r.j.wieringa}@ewi.utwente.nl

***Abstract*—Increasingly, organizations collaborate with other organizations in value webs with various arrangements, such as outsourcing, partnering, joint ventures, or subcontracting. As the Jericho Forum (an industry consortium of the Open Group) observed, in all these forms of collaboration, the boundaries between organizations become permeable and, as a consequence, insiders and outsiders can no longer be neatly separated using the notion of a perimeter. Such organizational arrangements have security implications because individuals from the value web are neither outsiders nor completely insiders. To address this phenomenon this paper proposes a third set of individuals, called External Insiders.**

External insiders add challenges to the already known insider threat problem because, unlike outsiders, external insiders have granted access and are trusted; and, unlike traditional insiders, external insiders are not subjected to as many internal controls enforced by the organization for which they are external insiders. In fact, external insiders are part of two or more organizational control structures, and business-to-business contracts are often insufficiently detailed to establish security requirements at the level of granularity needed to counter the threat they pose.

***Index Terms*—Risk Management, B2B contract, Enterprise Network, Security Metrics, Extended Enterprise.**

I. Introduction

All organizations, businesses as well as governments, distinguish insiders from outsiders. Insiders are trusted, outsiders are not. The security measures of the organization protect against outsider threats by creating a "perimeter" around the organization's assets, consisting of defenses against possible attacks by outsiders. This, however, does not solve the *insider threat problem*, which is the problem that insiders may use their privileges to compromise and abuse assets of the organization. The insider problem is real: the 2008 CSI Computer Crime and Security Survey [1] ranked insider abuse in second place in terms of most frequently occurring incidents, according to 522 respondent organizations (virus was ranked in first place with 50%, insider abuse in second place with 44% and theft of laptops in third place with 42%). Moreover, the insider problem is complex: according to the INFOSEC Research Council of the U.S. Department of Homeland Security, insider threat is one of the hard problems of information security [2].

In addition, insiders attacks tend to be more harmful than outsiders attacks. Two studies by Verizon, one with 500 cases of data breaches between 2004 and 2007 [3] and another with 90 cases of data breaches in 2008 [4], show that although the likelihood of cases involving insiders were lower than the ones involving outsiders, their impact in terms of number of records compromised were higher. Their last study also shows that one third of the breaches in 2008 involved partners. The Verizon studies were primarily concerned with data breaches involving consumers information, therefore, theft of intellectual property is not part of their analysis. However, other sources reveal that such theft of information is also frequently performed by insiders, specially in times of economic slowdown. According to a recent study (2009) sponsored by Symantec that surveyed 945 adults in the U.S. who lost their jobs due to downsizing of companies in the past months, 63% walked away with proprietary information [5].

In the current networked world, the insider threat problem has become even more complex because the distinction between insiders and outsiders is fading away, i.e. an increasing number of people may cause insider threat even though they do not fall under the hierarchical control of the organization. The erosion of the organizational perimeter that separates insiders from outsiders is called *deperimeterization* by the Jericho Forum[1]. Businesses enter partnerships, outsource application management, subcontract services run on data centers owned and maintained by third parties, have their assets managed remotely by third party vendors, have point-of-sale systems supported by others, employ IT across several partners along a value chain, and engage in joint product development. We call all these different kinds of cross-organizational cooperative networks *value webs*. They create *external insiders* that do not fall under the hierarchical control of a single organization, and for which none of the organizations in isolation has full control of the threat they represent.

The cooperation of organizations in value webs is largely facilitated by IT [6] and is actively aimed for in the attempt to cut costs, to increase flexibility or to create new business opportunities [7]. However, security standards, such as ISO 27001-27002 [8], [9], still rely heavily on the concept of logical perimeter and in blocking unauthorized access from outside to inside[2]. Additionally, as an evidence of trustworthiness to the outside world, and to minimize time-consuming auditing activities each time a new collaboration is established,

[1] http://www.opengroup.org/jericho/deperim.htm

[2] In terms of value webs these standards set guidelines and best practices about performing risk assessment of third parties before engaging in cooperations, and about what B2B contracts should specify, e.g., in terms of access control.

participants in a value web can make use of auditing standards such as SAS 70 for Service Organizations [10]. Once certified, the certification can be shown to other parties in the value web without additional inspections. However, such certifications are costly and must be performed periodically (typically every 6 or 12 months), therefore, it may happen that not all organizations member of a value web are certified. Moreover, securing organizations individually is not enough [11] to counter the external insider threat.

An instrument often used to regulate B2B relationships are legal contracts between parties. Therefore, in value webs there is a variety of roles as established by contracts between cooperating companies—if there is a contract, which is not always the case. And if there is a contract, the collaborations described by it are usually so complex that the contract is usually incomplete with respect to the threats offered by this constellation of roles in this particular IT network configuration. And in the unlikely case that the contract is not incomplete, IT architectures will evolve, which makes any threat analysis obsolete because they may create new insider threats not foreseen in the contract. In addition, the contract may interact with other contracts with the same or other partners in unexpected ways, which may create surprising vulnerabilities resulting in cascade failures. Also, accountability in value webs is a hard requirement to fulfil precisely because (as already mentioned) a value web represents the erosion of perimeters. It is more difficult in a value web for a CxO to show that she is in control of the business assets she is accountable for, although today's legislation, such as the European Union's Directive 95/46/EC and the United States' Sarbanes-Oxley (SOX) have stepped up the requirements of accountability.

A. Contributions

We argue in this paper that the dichotomy of outsider-insider is no longer enough in a value web context. To address this phenomenon we propose a third set, called External Insiders, that is our main contribution. In more details, the contribution of this paper is threefold: (i) it defines external insiders and discusses differences between external insiders and traditional insiders that make the external insider threat problem even harder than the (internal) insider threat problem, (ii) it reviews classifications of insiders and solutions proposed by academia and commercial vendors to cope with insider threat, and discusses the applicability of those solutions in the context of external insider threat, and (iii) it argues that the first step that organizations need to take is to measure the phenomena of external insider threat.

II. Characteristics of Outsiders

We use the following definition of *outsider* in this paper.

> **Outsiders** are individuals that are not trusted, and have no authorized access over the organization's assets.

Having in mind this definition, we review next relevant characteristics of an outsider.

1) Distrust
   Outsiders are not trusted and, therefore, are regarded with suspicion.
2) Unauthorized access
   Outsiders are not authorized to access any of the organizational assets. Therefore, any attempt to do so represents as an illegal act. In the digital world such attempt is an attack (that may be successful or not), and in the physical world is a burglary or an attempt burglary.

In the next section we define insiders and review their characteristics in comparison to outsiders.

III. Characteristics of Insiders

There is no agreed definition of *insider*; different authors (e.g., [12]–[14]) emphasize different characteristics. In this paper, we use the following definition of insider.

> **Insiders** are individuals that are trusted, and have (some) authorized access over the organization's assets.

Having in mind this definition, we review next the characteristics that distinguish an insider from an outsider.

1) Trust
   Trust is maybe the most fundamental aspect that distinguishes outsiders and insiders. Outsiders are, by default, not trusted while insiders are. In fact, organizations have to trust insiders to a certain degree, otherwise they cannot perform their duties. However, trustworthiness is subjective and may be affected by different factors such as the possibility of financial gain and revenge.
2) Authorized access
   While outsiders first need to acquire access to the inner core of an organization to be in a position to exploit its assets, insiders already have access granted. However, although insiders have authorizations to access information, they may not have the *need to know* this information to perform their duties [15]. Furthermore, this need to access information is not static and, therefore, access rights require management. For example, individuals' access rights have to be updated accordingly upon project completion, changes in job functions, and job termination. However, management of access rights may be deficient and deteriorate over time, raising opportunities for insiders to misuse access.
   Another aspect related to authorized access is the accountability of the granting process itself. There is a balance to be considered between complete logging of who, when, and why each access was granted, which requires time and effort to perform and analyze, and the need for efficiency in the working environment. In practice, full accountability is hard to achieve, creating again opportunities for insiders to misuse access.
3) Legitimate privileges

Besides having authorized access, insiders also have legitimate reasons to perform certain sensitive tasks which require privileges[3]. This combination puts insiders in a position that can easily lead to misuse, both on purpose or by mistake. This happens when organizational resources and privileges are used with a different intent from what and how they were supposed to [3], causing a violation of security policies enforced by the organization [12].

The risk derived from the capabilities of an insider tends to get aggravated over time if proper mechanisms of prevention are not in place. First, the accumulation of roles for various reasons mentioned in the previous item (e.g., changes in job function) can allow insiders to acquire a combination of privileges resulting in unpredicted consequences. Second, the indirect accumulation of privileges (e.g., via delegation) can also undermine security significantly.

Additionally there is the problem of privileged IT administrators, who normally should take care that users have only the access rights they need. However, administrators can become a serious threat themselves, which is most often treated reactively when a suspicion is raised somehow. According to the Verizon study [3], in half of the cases analyzed, breaches were performed by administrators themselves.

4) Knowledge
   Inside knowledge is an advantage of insiders compared to outsiders. It is cumulative, and spans across many fronts, such as the technical, administrative, personal, and professional domains. Knowledge is very useful to uncover vulnerabilities in organizational controls and to increase the perception of risk.
5) Organizational controls
   Typically, there is a contract of employment between an insider and the organization although this does not necessarily hold. Anyway, an insider is subject to any means of organizational control enforced by the organization such as, e.g., physical controls, access control like separation of duties and dual-control policies, and hierarchical controls such as supervision and review procedures.
6) Perception of risk
   Insiders have a better perception of risk compared to outsiders. According to Fariborz and Spafford [16] risk perception involves two aspects: (i) *understanding of the risks* themselves, reflected in familiarity and experience with the practices adopted by the organization, and (ii) *understanding of the consequences*, reflected in knowledge of scope, duration and impact of risks involved in a misuse. As a consequence, on the one hand, insiders are in a better position to successfully breach controls enforced by the organization, to cover traces and end up undetected. On the other hand, insiders tend to be more cautious than outsiders because they have, in principle, more to loose (their jobs).

[3]Access involves the right to *read* information while privileges involve the right to manipulate information i.e. *write*, *execute* and *delete*.

In the next section we define external insider and discuss their characteristics compared to insiders and outsiders.

IV. Characteristics of External Insiders

The distinction between insiders and external insiders is more subtle than between insiders and outsiders. However, external insiders are *not* a sub-set of insiders but rather a separate set that falls somewhere between the set of insiders and the set of outsiders, therefore, having characteristics of both.

> **External Insiders** are individuals that are not trusted and have (some) authorized access over the organization's assets.

Having in mind this definition and the characteristics of outsiders (reviewed in Section II) and of insiders (reviewed in Section III), we review next the characteristics of external insiders.

1) Distrust
   External insiders arise when there is business reason for the organization to cooperate with third parties. It means that the cooperation is only established if there a certain level of trust between the business parties involved. However, this does not mean there is trust between the organization and individuals that are insiders for other parties in the value web. Therefore, fundamentally, external insiders are not trusted.
2) Authorized access
   External insiders need to have access granted over the organizational assets to fulfill a contract between business parties. The extent of this access and the privileges required over which assets should result from risk assessment, according to security best practices such as ISO 27001-27002 [8], [9]. However, these guidelines recognize that it may be unfeasible to carry out risk assessment in an individual basis (what usually happens in practice) and, instead, standard access policies can be agreed upon. As a consequence, contracts become vague, and typically do not contain the level of details required, when it comes the time to grant access to external insiders.
3) Organizational controls
   In principle, external insiders (similar to insiders) are subject to any controls enforced by the organization. However, in practice there are several challenges in actually implementing such controls in the case of external insiders, as we will see in the next section.

V. Challenges of External Insider Threat Compared to (Internal) Insider Threat

In the previous section we have positioned external insiders as a separate set of individuals, distinguished from outsiders

and insiders. At first glance the threat they pose is similar to the threat posed by (internal) insiders, however, this is not completely true.

We now analyze the problem of external insider threat in comparison with the insider threat problem. Table I summarizes the results of our analysis.

Since external insiders have more characteristics in common with insiders than with outsiders, it becomes natural to investigate whether classifications of insiders and solutions to deal with the (internal) insider threat problem apply to external insiders and to the external insider threat problem, respectively. We do so in the next two sections.

VI. A Review of Insiders Classification

Understanding insider threat has been the focus of many researchers, and led to several classification schemes. An early classification was performed by Anderson [17], who grouped insiders into three categories: (i) *masqueraders*, which are individuals who steal the identity of a legitimate user becoming an impersonated legitimate user, (ii) *misfeasors*, which are legitimate users who are authorized to use systems and to access information but misuse their privilege, and (iii) *clandestine users*, which are individuals who evade access control and audit mechanisms and therefore are unknown until they become masqueraders or misfeasors. Other classifications focus on insiders' intention, such as the one used by CERT[4], that classifies insiders' intentions into three categories: (i) *theft of information*, also called espionage, when someone steals confidential or proprietary information from the organization, (ii) *IT sabotage* when someone harms, in any sense, the organization or individuals within the organization, and (iii) *fraud* when someone obtains unjustifiable services or property from the organization [18], [19]. There are some correlations between these classifications, e.g., masqueraders are in a better position to execute fraud, while misfeasors are in a better position to perform espionage and sabotage.

Some classifications have a specific purpose. For example, Phyo and Furnell [20] propose a detection-oriented classification of insider IT misuse. Their starting point is the fact that different types of misuse manifest themselves at varying levels of the system. Some misuses are apparent at the network level, whereas others are only apparent at the host level, either via the operating system or via applications. They list misuses indicating the monitoring level and attributes to be monitored. Yet other classifications take the perspective of insider attack prevention, such as the one proposed by Magklaras and Furnell [21]. They classify insiders based on: (i) system role, (ii) reason of misuse, and (iii) system consequences, and use evidences of actual behavior and usage of systems to score individuals and predict misuse.

All of these classifications can be applied to external insiders just as they can be applied to internal insiders. However, in the case of external insiders additional classifications based on typical characteristics of business arrangements in value webs, such as outsourcing, partnerships, and subcontracting, would be an advantage to increase understanding of the external insider threat and allow more effective countermeasures. This is one of our future work directions.

[4]Carnegie Mellon University Computer Emergency Response Team, http://www.cert.org/

VII. A Review of Defense Mechanisms against Insider Threat

We now turn to currently known mechanisms to defend against insider threat.

Log analysis is the main approach proposed by researchers to deal with insider threat [22]. The exact approach depends on the class of insider threat one wants to focus on. For example, masqueraders can best be detected using anomaly detection [23], [24] or using profiling approaches based on sequential patterns or statistical features [25], [26], because it is unlikely that a masquerader will behave as the impersonated user in a consistent manner. Credit card and online shopping companies use these approaches to detect fraud, at the level of hosts or applications. However, these detection approaches are not suitable for detecting misfeasors because changes in misfeasor behavior are more subtle, and may be diffused across a longer time span. In the case of misfeasors, a network-based approach to detect violations of need-to-know policies [27], or a top-down *structured analysis* of insider actions from high-level goals [28], are more appropriate. They allow the identification of unauthorized activities such as anomalous downloads, suspicious installation of software and retrieval of documents outside some constraints.

Another approach to detect misfeasors relies on a bottom-up approach based on the correlation of evidence collected from several sensors [28] to infer malicious intents from insiders. Two challenges here are to log with sufficient details about the events taking place, and to be able to relate actions logged to unique individuals. In fact, Verizon [4] reports that only 19% of the analyzed organizations that had data breaches in 2008 had a unique ID (digital identification such as login) assigned to each person with computer access to their assets; in 81% of the cases the organization used shared accounts for system access. In a value web context this practice may be particularly useful, on the hand, for partners to avoid revealing turnover of personnel to other participants of the value web and, on the other hand, to facilitate identity management. An additional challenge is the amount of logged data to be analyzed. Again, another interesting finding uncovered by the Verizon study [4] is that 71% of the organizations that were investigated logged data in a constant basis but only 11% of them actually analyzed this data.

Very few approaches aim at addressing insider threat proactively [21], [29], [30], apart from best practice guidelines (e.g. [31]). Rich et al. from CERT [29] propose a simulation tool which helps to understand technical and behavioral precursors of an attack. The tool also allows reasoning about the effectiveness of security measures to mitigate the risk of such attack. It is basically a learning and awareness tool for organizations. Other approaches [21], [30] propose a set of

Organizational means of control	Insiders	External insiders
auditing	the organization has full access to fine-grained logged information about internal insiders and auditing is always possible	information logged about external insiders within the organization tends to be coarse-grained, and some integration with information logged by other parties may be required for auditing; other parties may keep this information confidential
revocation and update of access rights	job terminations, changes in roles and responsibilities, transfer to different organizational units require update in access rights; keeping those rights up-to-date within the same organization is a challenge and a major cause of insider misuse	the problem becomes more complicated when parties with different working processes are involved; and when organizations hide their internal job rotations from their partners in the value web
ownership of expertise to detect insider threat	there is internal expertise about the technologies used by the organization, e.g., if the organization has Oracle databases there are employees able to detect misuse by insiders in respect to this technology; therefore, the organization is more likely to know misuse patterns and expected behavior	in value webs, it is common to have technology transfer, causing a transfer of expertise from the organization to a partner organization; the organization itself may even lose the expertise to detect the threat that external insiders dealing with this technology may pose to their assets
control of access paths	the increasing mobility of insiders belonging to an organization and work-from-home initiatives are creating new access paths to organizational assets; it is already a challenge to avoid attacks initiated by outsiders and misuse from insiders under these circumstances	the possibility of indirect access paths through one or more parties, increases the risk of assets misuse; it is not uncommon that an organization subcontracts another party to perform a service and this party itself subcontracts a third party without the knowledge and consent of the original organization and this chain of authorized access makes the scope of the external insider threat problem larger compared to traditional insider threat problem
screening and behavior monitoring	employee screening is typically performed prior to employment, and continuous social interaction increases the chances of detection of suspicious (internal) insider behavior	the organization has to trust that external insiders that have access and privileges over its assets have been screened; besides, due to reduced and sporadic social interactions, the chances for detection of external insiders suspect behavior are limited
authorizations and identity management	authorizations are usually granted on a need-to-know, individual basis and separation of duty policies are enforced to decrease the chance of assets misuse by internal insiders	authorizations tend to be granted on a worst-case, partner basis (no unique identification of individuals), i.e. higher-than-needed privileges may be granted, and separation of duty policies are not guaranteed to be enforced across the value web; moreover, the digital identification of external insiders is more complex
security policies	the organization enforces security policies that insiders have to comply with; e.g., most of the times, insiders must use corporate-supported hardware and software configured in a standard way and subject to (automatic) patch management procedures adopted by the organization	external insiders tend to use hardware and software that comply with the security policies of a third party in the value web to access the organization's assets; this makes it difficult to ensure their compliance with security policies enforced by the organization
security assurance	there is detailed information about how the organization ensures security: for example, through awareness campaigns, and enforcement of internal controls	security governance is assured by means of certifications, reputation, and (most importantly) legal contracts; however, contracts are often under-specified and, as a consequence, contract violations are difficult to define, and hence very difficult to detect

TABLE I
KEY DIFFERENCES BETWEEN (INTERNAL) INSIDER AND EXTERNAL INSIDER

indicators or attributes to quantify potential threats represented by insiders that can lead to particular malicious actions. These approaches are less suitable to external insiders because typically there is limited communication between employees of the organizations participant of a value web. For example, it may be very difficult, if not an impossible job, to assign indicators that may trigger suspicion about external insiders that perform tasks such as remote administration of servers.

There are insider misuses performed by misfeasors that can only be detected at the application level [22]. They involve, for example, privileges to use software features and functionalities, and to execute, modify and delete data, rather than just the authorizations necessary to access an application. Therefore, they require granular access control policies over the data such as enforcement of separation of duty policies. Furthermore, misuses may involve violations of static or dynamic separation of duties, requiring the detection engine to have knowledge of business processes and roles performed by insiders within the organizational structure. Phyo et al. [32] propose a theoretical framework based on the assumption that users with similar roles and responsibilities will exhibit similar behavior within an application. Deviating activities from the normal profile defined by a role is considered as suspicious. Park and Ho [33] propose a role-based monitoring approach. Each user may be assigned three types of roles: "organization" (e.g. employee), "application" (e.g. analyst) and "operating system" (e.g. administrator), and there is a mapping between them. Besides, roles have expected or unexpected behaviors

assigned to them. The monitoring engine compares actual behavior allowed by the activation of a role by an user with pre-defined role behavior. However, the manual elaboration of normal profile or expected/unexpected activities for each role may be very time consuming, representing a drawback of these approaches. In case of external insiders we have noted that roles are often not defined completely by a contract, making these approaches less suitable for mitigating external insider threat.

So far, we have reviewed academic solutions to insider threat mitigation. Commercial products address the insider threat problem too. For example, LogRhythm[5] detects fraud using anomaly-based detection from logged events. It issues alerts on suspicious behavior of users taking the context into account, such as asset value and time of the day. Another commercial product is ArcSight[6], that also relies on anomaly-based detection, but in addition considers detection of known patterns of insider misuse. Suspicious behavior, such as off-hours access to data and encrypted file uploads, escalates the user threat level. IBM IRIS (Identity Risk and Investigation Solution) [23] is another commercial tool that uses anomaly-based detection to alert on suspicious behavior. Currently, these tools are used to mitigate insider threat to a certain extent; note that they apply to mitigate external insider threat too, as long as each external insider can be uniquely identified, and normal behavior can be well defined.

We have seen that anomaly-based reasoning is very much appropriate for detection of masqueraders. Therefore, if the value web involves *only* a provider and its customers, most probably external insider threat prevention is similar to the detection of masqueraders and can be managed that way. However, we have also seen that detection and prevention of misfeasors in value webs become more complex than when only one single organization is involved because, e.g., patterns of external insider misuse are not completely understood, accountability of external insiders is not always present in practice, indicators of increasing levels of threat in the case of external insiders (most of the times) remain hidden. Therefore, in the next section we turn to other directions for coping with the external insider threat.

VIII. Alternatives to Counter External Insider Threat

As we have seen in Sections V and VII traditional means of organizational controls and security mechanisms that work to detect and prevent classical insider threat may simply not apply, or apply only partially, to counter external insider threat. The solution proposed by the Jericho Forum[7] is to introduce data-centric security. It shifts security from complete systems or infrastructure to the data itself; examples are encryption, database security such as Hippocratic database, and sticky policies [6]. However, data-centric security can be very expensive because it may require classification of large amounts of data at a low level of granularity. Moreover, it does not solve all problems listed in Table I. For example, an organization can have a very efficient interaction between the Information Technology and the Human Resources departments, to assure that access and privileges of terminated insiders are revoked quickly; this routine may even be automated. But if the terminated insider is employed by a third party, this feedback becomes complex. Moreover, data-centric security helps to improve confidentiality but not other security attributes such as integrity or non-repudiation.

To sum up, data-centric security helps to improve some, but not all security challenges in the face of external insiders, and it does not help against all threats; and where it helps, it may be prohibitively expensive. Defense against external insider threat must be also based on agreements made explicit in the B2B contracts in terms of sharing of logs, audit of the organizational data in the partner premises and network, process and timeframe to inform turnover of personnel employed by the other party that has access to the organizational data, etc. Classification of external insiders must also be based on contracts, but since different types of business relationships in a value web can be categorized, a classification of value webs can provide a starting point for classifying external insider threat. For example, outsourcing software development has its typical external insiders, as does partnering in product development, as does cooperation to sell goods and services to consumers over the Internet, and so on. Some properties of value webs can be used to understand and control threat and to improve B2B contracts. For example, the economic self-interest of all actors in a value web can be used to define fines for undesirable behavior and incentives for desirable behavior. Kartseva et al. [34] explore this for protection against unwanted (economic-related) behaviors in value webs and some of these inter-parties control mechanisms may be applicable in defense against external insider threat too (this will remain as future work). However, a natural step prior to exploring the economic aspect of value webs to reduce the external insider threat is to measure it; this is the subject of the next section.

IX. A First Step: Measure of the External Insider Threat Phenomena

A metric defines an unambiguous measurement instruction for something that can be measured. Metrics, sometimes called indicators, are basically used for two purposes: (i) provide a quantitative snapshot of anything measurable with the purpose of obtaining insights not only about business-as-usual-related-operations, but also about a phenomenon, a hypothesis, or a risk, or (ii) provide a continuous quantitative view of anything measurable over time for analysis of trends and performance. Applied to security, metrics allow assessment of security risks and allow directing efforts to areas that need improvement.

We see two groups of metrics that are relevant for an initial understanding of external insider threat in organizations (collected from Jaquith [35]):

1) Measuring external insiders access and privileges

[5] www.logrythm.com
[6] www.arcsight.com
[7] http://www.opengroup.org/jericho/deperim.htm

- number of systems that interface with partners
- number of partners that have access to the organization's assets
- number of unique IDs (logins) used to access the organization's assets, by partner
- number of IDs (logins) with administrator privilege over the organization's assets, by partner
- % of authorized and unauthorized transactions initiated by partners, by application

2) Measuring external insiders security governance

- % of B2B contracts with documented security requirements
- % of partners certified by SAS 70 (type 2)[8]
- % of partners whose access and privileges were reviewed in a period (e.g. in the last 6 or 12 months)

These metrics allow an organization to have a first impression of the external insider threat problem as a whole. It is a starting point for further analysis. For example, if the number of systems that interface with partners is small, let's say is 1 (this threshold is organization-specific), then the scope of the problem is reduced to the partners that have access and privileges over this specific system. It does not mean that the *problem* is small though because an organization can have a not-so-small number of partners accessing this unique system, let's say it has 10 partners. A next step could be to find out, for each partner, the number of unique IDs used for access. This number has to be put into context; let's say that a partner A accesses the system for maintenance tasks and a partner B accesses the system for viewing technical drawings needed for product development. If partner A has one unique ID authorized for access and partner B has three, it means there is a potential problem because it is not realistic to assume that partner A's ID is only used by a single user since this user has holidays, has time-off sick, etc. The problem might escalate if we find out that this unique ID has administrator privileges. This way, metrics can be helpful not only to spot problems but to dig into problems detected, and take countermeasures.

Therefore, we claim that security metrics are a feasible and practical starting point to understand the external insider threat phenomena. The metrics can be tailored to specific value web contexts, as long as these metrics comply with general guidelines that determine good metrics. As stressed by Jaquith [35], security metrics are only good if they are "consistently measured" with no subjectivity involved, "cheap to gather" preferably in an automatic way, expressed as meaningful quantitative "numbers or percentages", associated with at "least one unit of measure" , and "contextually specific" to allow decision making.

Continuous use and analysis of such metrics allow a continuous management of the external insider threat.

[8]SAS 70 [10] type 1 reports an auditor opinion about whether relevant policies and procedures were placed in operation as of a specific date, and type 2 reports whether such policies and procedures were in fact operating effectively, according to tests performed.

X. Conclusion and Future Work

In this paper we argued that under the perspective of a highly deperimeterized world, current reality of organizations that cooperate in value webs, the dichotomy of outsiders and insiders must be extended with an intermediate set of individuals called External Insiders. We have defined and distinguished outsider, insider and external insider, and discussed what makes the external insider threat much more challenging than the insider threat. We reviewed current solutions in academia and industry to counter internal insiders and identified some aspect that make them not sufficient to counter the external insiders. Finally, we proposed the use of security metrics as a starting point to measure the external insider threat phenomena.

We have three directions for future work:

- evaluate the use of security metrics to understand the external insider threat by conducting case studies in industrial partners related to our research project
- classify misfeasors in different value web contexts by means of literature review
- evaluate whether economic-related controls are applicable in defense against external insider threat

Acknowledgements

This research is supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

References

[1] R. Richardson, "2008 CSI Computer Cime and Security Survey," 2008, http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf. Visited on Sep 2009.

[2] I. R. Council, "Hard problem list," November 2005, http://ww.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf, Visited on Oct 2008.

[3] W. H. Baker, C. D. Hylender, and J. A. Valentine, "2008 data breach investigations report," Verizon Business Security Solutions, June 2008, www.verizonbusiness.com/resources/security/databreachreport.pdf, Visited on Sep 2008.

[4] W. H. Baker, A. Hutton, C. D. Hylender, C. Novak, C. Porter, B. Sartin, P. Tippett, and J. A. Valentine, "2009 data breach investigations report," Verizon Business Security Solutions, April 2009, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, Visited on Sep 2009.

[5] L. Ponemon, "Data loss risks during downsizing," Study sponsored by Symantec Corporation, and conducted by Ponemon Institute LLC, February 2009, http://scm.symantec.com/DLP/en/resources.php, Visited on Sep 2009.

[6] A. van Cleeff and R. J. Wieringa, "Rethinking De-Perimeterisation: Problem Analysis and Solutions," in *Proc. of the IADIS Int. Conf. Information Systems 2009*. IADIS press, February 2009, pp. 105–112.

[7] D. Tapscott, D. Ticoll, and A. Lowy, *Digital Capital: Harnessing the Power of Business Webs*. Harvard Business Press, 2000.

[8] ISO/IEC-27001, "Information technology. Security techniques. Information security management systems. Requirements," 2005.

[9] ISO/IEC-27002, "Information technology. Security techniques. Code of practice for information security management," 2005.

[10] AICPA, "SAS No. 70, Service Organizations," http://www.aicpa.org/download/members/div/auditstd/AU-00324.PDF, 2000.

[11] C. D. Huang, R. S. Behara, and Q. Hu, "Managing Risk Propagation in Extended Enterprise Networks," *IT Professional*, vol. 10, no. 4, pp. 14–19, 2008.

[12] M. Bishop, "Position: Insider is relative," in *NSPW '05: Proceedings of the 2005 workshop on New security paradigms*. New York, NY, USA: ACM Press, 2005, pp. 77–78.

[13] M. V. Hayden, "The Insider Threat to U.S. Government Information Systems," July 1999, advisory Memoranda NSTISSAM INFOSEC 1-99.

[14] R. C. Brackney and R. H. Anderson, "Undersatanding the insider threat: Proceedings of a march 2004 workshop," California, USA, 2004.

[15] L. Spitzner, "Honeypots: Catching the Insider Threat," in *ACSAC'03: Proc. of the 19th Annual Computer Security Applications Conference*. Washington, DC, USA: IEEE Computer Society Press, December 2003, pp. 170–179.

[16] F. Farahmand and E. H. Spafford, "Insider Behavior: An Analysis of Decision under Risk," in *MIST'09: Proc. of the 1st International Workshop on Managing Insider Security Threats*, vol. 469. CEUR-WS, http://CEUR-WS.org, June 2009, pp. 22–33.

[17] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Fort Washington, PA, USA, Tech. Rep., 1980, http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf.

[18] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers, "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," May 2005, U.S. Secret Service and CERT Coordination Center.

[19] M. R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," August 2004, U.S. Secret Service and CERT Coordination Center.

[20] A. . Phyo and S. M. Furnell, "A detection-oriented classification of insider it misuse," in *Proceedings of the 3rd Security Conference*, April 2004.

[21] G. B. Magklaras and S. M. Furnell, "Insider Threat Prediction Tool: Evaluating the probability of IT misuse," *Computers & Security*, vol. 21, no. 1, pp. 62–73, 2002.

[22] M. B. Salem, S. Hershkop, and S. J. Stolfo, *Insider Attack and Cyber Security*. Springer-Verlag, 2008, ch. A Survey of Insider Attack Detection Research, pp. 69–90.

[23] R. Anderson and T. Moore, "Information Security Economics - and Beyond," in *CRYPTO'07: 27th Annual International Cryptology Conference*, August 2007, pp. 68–91.

[24] S. J. Stolfo, F. Apap, E. Eskin, K. Heller, S. Hershkop, A. Honig, and K. Svore, "A Comparative Evaluation of two Algorithms for Windows Registry Anomaly Detection," *J. Comput. Secur.*, vol. 13, no. 4, pp. 659–693, 2005.

[25] R. A. Maxion, "Masquerade Detection Using Enriched Command Lines," in *DSN'03: Proc. 2003 Int. Conf. on Dependable Systems and Networks*, IEEE, Ed. Washington, DC, USA: IEEE Computer Society, June 2003, pp. 5–14.

[26] N. Nguyen, P. Reiher, and G. Kuenning, "Detecting Insider Threats by Monitoring System Call Activity," in *Proc. of IEEE Workshop on Information Assurance*. Washington, DC, USA: IEEE Computer Society Press, 2003, pp. 45–52.

[27] M. A. Maloof and G. D. Stephens, "ELICIT: A System for Detecting Insiders Who Violate Need-to-Know," in *RAID'07: In Proc. of the*, ser. LNCS, vol. 4637. Springer-Verlag, August 2007, pp. 146–166.

[28] M. Maybury, P. Chase, B. Cheikes, D. Brackney, S. Matzner, T. Hetherington, B. Wood, C. Sibley, J. Marin, T. Longstaff, L. Spitzner, J. Haile, J. Copeland, and S. Lewandowski, "Analysis and Detection of Malicious Insiders," in *IA'2005: Proc. 2005 Int. Conf. on Intelligence Analysis*. MITRE, http://www.mitre.org/, May 2005.

[29] E. Rich, I. Martinez-Moyano, S. Conrad, D. Cappelli, A. Moore, T. Shimeall, D. Andersen, J. Gonzalez, R. Ellison, H. Lipson, D. Mundie, J. M. Sarriegi, A. Sawicka, T. Stewart, J. M. Torres, J. Wiik, and E. Weaver, "Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model," in *Proc. 23rd Conference of System Dynamics Society*. System Dynamics Society, July 2005.

[30] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security*, vol. 21, no. 6, pp. 526–531, October 2002.

[31] D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, "Common Sense Guide to Prevention and Detection of Insider Threats," CERT, http://www.cert.org, January 2009, 3rd Edition - Version 3.1.

[32] A. H. Phyo, S. Furnell, and F. Portilla, "A Framework for Role-based Monitoring of Insider Misuse," in *In Proc. of the 19th Int. Information Security Workshops, part of IFIP World Congress*, August 2004, pp. 51–66.

[33] J. S. Park and S. M. Ho, "Composite Role-Based Monitoring (CRBM) for Countering Insider Threats," in *Intelligence and Security Informatics*, ser. LNCS, vol. 3073. Springer, August 2004, pp. 201–213.

[34] V. Kartseva, J. Gordijn, and Y.-H. Tan, *Design Requirements Engineering: A Ten-Year Perspective*, ser. Lecture Notes in Business Information Processing. Springer Press, January 2009, vol. 14, ch. Designing Value-Based Inter-organizational Controls Using Patterns, pp. 276–301.

[35] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional, 2007.