Engineering Security Agreements Against External Insider Threat

Virginia N. L. Franqueira, Department of Computing, University of Central Lancashire, Preston, UK

André van Cleeff, Department of Computer Science, University of Twente, Enschede, The Netherlands

Pascal van Eck, Department of Computer Science, University of Twente, Enschede, The Netherlands

Roel J. Wieringa, Department of Computer Science, University of Twente, Enschede, The Netherlands

ABSTRACT

Companies are increasingly engaging in complex inter-organisational networks of business and trading partners, service and managed security providers to run their operations. Therefore, it is now common to outsource critical business processes and to completely move IT resources to the custody of third parties. Such extended enterprises create individuals who are neither completely insiders nor outsiders of a company, requiring new solutions to mitigate the security threat they cause. This paper improves the method introduced in Franqueira et al. (2012) for the analysis of such threat to support negotiation of security agreements in B2B contracts. The method, illustrated via a manufacturer-retailer example, has three main ingredients: modelling to scope the analysis and to identify external insider roles, access matrix to obtain need-to-know requirements, and reverse-engineering of security best practices to analyse both pose-threat and enforce-security perspectives of external insider roles. The paper also proposes future research directions to overcome challenges identified.

Keywords: *Business Network, Conceptual Modelling, Extended Enterprise, Inter-Organisational Network, Security Analysis, Security Management, Service Level Agreement*

INTRODUCTION

In the past, companies were loosely linked only to a few other companies and their IT resources, i.e. IT infrastructure, data and business processes, remained in-house under their custody and control. Today, companies no longer operate in isolation but are rather tightly connected to other companies in a network-like structure, called *business networks*, *inter-organisational networks* or *extended enterprises* (Wiendahl & Lutz, 2002; Jagdev & Thoben, 2001; Baraldi et al., 2012; Hakansson & Ford, 2002), with different levels of integration and cooperation.

DOI: 10.4018/irmj.2013100104

Extended enterprises are ever more attractive because they provide competitive advantage by allowing cost savings, time and quality-related benefits, and by increasing business agility and flexibility; each participant in an extended enterprise specializes on its core competencies and takes advantage of other organisations' expertise to deliver its business mission (Jagdev & Thoben, 2001; Starr et al., 2003). The growth in the adoption of Cloud Computing and the diversity of service bundles on offer exacerbate the fact that organisational boundaries in an extended enterprise context are overwhelmingly fuzzy (Jericho-Forum, n.d.; Thoben & Jagdev, 2001; Jagdev & Thoben, 2001). The size of an extended enterprise can be significant, typically reaching hundreds; research from the Information Security Forum indicates that, on average, companies work with 750 service providers (Davis, 2010). This adds-up to other factors, such as the complexity of dependencies among participants of the network, geographic dispersion, and distributed sources of risk (Thoben & Jagdev, 2001; Davis, 2010), and to the fact that each company part of an extended enterprise is most likely to be itself an extended enterprise, creating a chain of non-transparent B2B relationships.

Extended enterprises create a security management problem in part because it is difficult to have a holistic overview of security across systems, technologies and resources in the entire network. One specific sub-problem of security management in extended enterprises is what we call the *external insider threat.* Such threat is posed by a class of individuals employed by participants of a company's extended enterprise network − or their network − who need access to a certain extent to the assets (e.g., data, IT infrastructure, processes) the company owns and is accountable for, regardless of where and by whom it is handled. External insiders are a class of individuals which do neither completely fall under the class of insiders nor of outsiders of one company, and therefore, mitigations to insiders and outsiders do not completely solve the external insider threat problem. External insiders of a company assume a large number of roles across numerous other companies part of its extended enterprise in a variety of B2B arrangements. Those arrangements involve different levels of integration, cooperation and resources sharing (Kumar & van Dissel, 1996; Jagdev & Thoben, 2009). They can span from more traditional arrangements such as trading partners in a value chain, service providers, business partners, to less traditional arrangements such as outsourced operations or facilities providers, security managed providers, Federated Cloud service providers (Bernsmed et al., 2011), or even innovation-driven cooperatives (Thorgren et al., 2009) and consortia for collective management of security (Gupta & Zhdanov, 2007).

A recognized way to mitigate risks and enforce trust in B2B relationships is to formalize agreements via contract. For example, umbrella agreements (also called framework agreements) are an often chosen type of contract as the complexity of such relationships increase (Mouzas & Ford, 2002). They provide a framework of norms but "remain sufficiently flexible to respond to unforeseen contingencies and embrace new or emerging business opportunities" (Mouzas & Ford, 2012, p. 154). Quality of Service (QoS) thresholds, and corresponding penalties, may be established via Service Level Agreements (SLAs) to specify measurable standards of service, which complement umbrella agreements. However, QoS parameters are typically related to service performance, availability and reliability, while non-quantifiable security requirements for service assurance remain an open issue in SLAs (Jaatun et al., 2012; Morali & Wieringa, 2010) due to challenges already discussed in the late 90's (Henning, 2000) and only intensified by emerging B2B relationships. Security SLAs, often called Protection Level Agreements (Krabulut et al., 2007), must cover the protection of data during its whole lifecycle and must be negotiated between parties. This is our solution direction to counter the external insider threat.

We take the point of view of one company in an extended enterprise, which we call the *focal company* or *focal organisation*, through the

paper. The contribution of this paper is threefold. First, it provides an overview of challenges posed by external insiders, and discusses solutions currently available to counter the external insider threat. Second, it provides a systematic way to derive security requirements that supports the engineering of security agreements in B2B contracts (i.e., security SLAs) using the refined method first introduced in Franqueira et al. (2012). Finally, it elaborates on future research directions to allow organisations to better counter the external insider threat.

The method, improved based on feedback from a case study on a multinational manufacturer, now incorporates steps which lead to a better understanding of need-to-know requirements for external insider roles. More specifically, the method has two parts. Its first part aims at the identification of external insider roles for a specific part of the extended enterprise; this part comprehends three steps: (1) value modelling to limit the scope of the analysis and identify companies involved, (2) coordination modelling to understand the business processes involved, and (3) IT architecture modelling to provide an overview of systems and connections. The method second part aims at the analysis of external insider roles; this part also comprehends three steps: (4) identification of external insider roles and activities they have to perform to fulfill their duties in respect to the focal organisation, (5) access matrix for the elicitation of external insiders' need-to-know requirements, and (6) reverse engineering of security best practices, considering external insiders as source of threat and as enforcers of security in the behalf of the focal organisation, for the elicitation of security requirements.

BACKGROUND

This section reviews the elements of trust, control and access in the context of extended enterprises, discusses the characteristics of outsiders, insiders and external insiders based on those elements, and provides background on value modelling, as used in our method.

Trust and Control

Trust is a core element in B2B relationships (Solhaug et al., 2007; Siegrist et al., 2005; Das & Teng, 1998; Jiang et al., in press). Relevant in the context of extended enterprises are both B2B trust and business-to-individual trust (between focal organisation, outsiders, insiders and external insiders).

Solhaug et al. (2007) discuss trust from two perspectives. From the perspective of the trustor (who is expected to trust), trust involves belief, hence, depends on the subjective probability attributed by the trustor that a trustee (who is expected to be trusted) will act as expected. From the perspective of the trustee, trust involves showing evidences of trustworthiness to allow the trustor to calculate a more objective, well-founded, probability. Because a sound measurement of trust is difficult to obtain and to verify, a possible alternative is to "reduce the need for trust by replacing it by assurance" (Solhaug et al., 2007), such as contractual trust (Karabulut et al., 2007). Assurance, implemented via controls, reduces the risk that an outcome will not turn out as expected by the trustor.

Some authors, such as Das & Teng (1998), however, question the view that trust and control should be regarded as complementary linked (i.e. the higher the trust, the lower the need for controls, and vice versa), and argue that they should rather be regarded as supplementary. Therefore, trust (or even contractual trust) and control should be considered as parallel concepts which, together, contribute to decrease risk.

For the purpose of this paper, *control* refers to mechanisms that provide a certain level of security to a focal organisation; it can consist of policies, procedures, organisational structure and technical controls (COBIT, 2012a). We distinguish between *external control*, enforced to protect private assets of a focal organisation from the outside, and *internal control*, enforced to protect private assets of a focal organisation from the inside. A *private asset* is regarded as an asset owned by the focal organisation and that depends on its authorisation to be accessed

legitimately, while a *public asset* is regarded as an asset owned by the focal organisation and made available for the general public. When the difference is not explicit, we use the term *asset* to refer to private asset.

Another important aspect of trust in extended enterprises is transitivity. Network theories from Social Sciences imply that trust is transitive among humans. For example, Granovetter's (1973) strength of weak ties theory argues that if A and B have a strong tie, and B and C also have a strong tie, than there is an increased chance that A and C will have at least a weak tie – e.g., A and C are acquaintances (Borgatti & Halgin, 2011). In inter-organisational relations, trust is not transitive (Karabulut et al., 2007). In an outsourcing relationship, for instance, an outsourcing company trusts a contractor company, and this contractor trusts its subcontractors; these B2B relationships are sealed by contracts. However, the outsourcing company has no contractual trust with subcontractors of its contractors. What is happening now is that transitive trust in extended enterprises is more and more imposed, giving rise to non-transparent chains of transitive trust to deliver a promised service (Bernsmed et al., 2011).

Identity and Access Management

Identity management and access management (IAM) complement each other. Identity management is concerned with the administration of digital identities throughout their lifecycle. It comprehends (Windley, 2005): provisioning (when the identity is created), propagation (when the identity is disseminated to multiple systems), usage (when the physical person authenticates using one valid identity to different systems), maintenance (when attributes of the identity are updated), and deprovisioning (when the identity is deactivated). Therefore, identity management involves correlation of data from Human Resources − to tightly couple a physical person to her digital identities, credentials management, user account and user profile management, role management, and users' privilege management (Witty et al., 2003).

Access management is concerned with the real-time enforcement of access policies. It comprehends the processes of authentication (when digital identities are verified and validated), and authorisation (when a decision is made about granting or not access for an authenticated digital identity to a system resource based on rights (also called permissions) established via access control policies (Ferraiolo et at., 2003).

CHARACTERISTICS OF OUTSIDERS, INSIDERS AND EXTERNAL INSIDERS

External insiders have been treated evasively in the literature. They are approached either simplistically as insiders from trusted business partners (Weiland et al., 2010) and partner agents (Verizon, 2012), or collectively as partners (Bhala et al., 2010) and third-parties (Davis, 2010). However, external insiders (Franqueira et al, 2010a) have their own characteristics and pose additional challenges, thus requiring specific mitigations, compared to insiders and outsiders. In this section we distinguish between outsider, insider and external insider considering trust, access and control. Table 1 summarises the core differences between these three classes of individuals.

Outsiders

We consider that outsiders have the following characteristics.

- **Trust:** Outsiders are individuals who are not trusted by the focal organisation.
- **Access:** Outsiders have either unauthorised access to the private assets owned by the focal organisation, or have by default authorised access to public assets owned by the focal organisation.
- **Control:** Outsiders are fully subject to external controls enforced by the focal organisation. For example, they are subject to rules enforced by firewalls facing the Internet in the network owned by the focal organisation, are subject to policies

Table 1. Distinction between outsiders, insiders and external insiders in repect to a focal organisation

	Outsiders	Insiders	External Insiders
Trust	Distrust	Trust	Contractual trust between focal organisation and external insider's employer
Access	Unauthorised to access private assets and authorised to access public assets	Authorised to access private assets	Authorised to access private assets
Control	Fully subject to external controls enforced by focal organisation	Fully subject to internal controls enforced by focal organisation	Partially subject to external and/or internal controls enforced by focal organisation

enforced by the focal organisation's public website, and by its online shop for end consumers.

Examples of outsiders are hackers, end consumers, and the general public.

Insiders

Different authors emphasize different characteristics of insiders. We consider that insiders have the following characteristics (Bishop, 2005; Brackney & Anderson, 2004; Hayden, 1999).

- **Trust:** Insiders are individuals who are trusted by the focal organisation that employs them.
- **Access:** Insiders are granted authorised access to the private assets owned by the focal organisation. Apart from authorised access, insiders also have legitimate reasons or need-to-know to perform their duties (Spitzner, 2003) which may involve sensitive tasks requiring authorisations not only the need to read, but also to write, execute and delete data. This combination of access and authorisations puts insiders in a position that can easily lead to misuse, either on purpose or by mistake. This happens when private assets (e.g., data, IT infrastructure and processes) are used with a different intent from what and how they were supposed to (Baker et al., 2008), causing a violation of security policies enforced by the focal organisation (Bishop, 2005).
- **Control:** Insiders are fully subject to internal controls enforced by the focal organisation, e.g., hierarchical controls, such as supervision and revision procedures, or access control policies, such as separation of duties and dual control enforcement.

Examples of insiders are employees, and interns (i.e. students' placement).

External Insiders

We consider that external insider have the following characteristics.

- **Trust:** External insiders are individuals who are *not* trusted by the focal organization. It means that the relationship between focal organisation and external insiders is only established if there is a certain level of B2B trust between the business parties involved, i.e. their employer and the focal organisation. This B2B relationship may be established by means of non-contractual agreements, contractual agreements or joint ventures (Jagdev & Thoben, 2001). Therefore, external insiders are an example of non-transitive trust relationship between them and the focal organisation.
- **Access:** External insiders have authorised access to the private assets owned by the focal organisation because they act in its behalf. Therefore, like insiders, they need access and authorisations to these private assets, and this should (in theory) be

established based on their need-to-know to perform duties. However, external insiders differ from insiders in terms of applicable controls.

- **Control:** External insiders are partially subject to external and/or internal controls enforced by the focal organisation. There are controls which are simply not applicable or are difficult to operationalise in the case of external insiders, and that is why they are *partially* subject to a mixture of internal and external controls. For example, external insiders are typically subject to social controls enforced by their employers but not by the focal organisation itself, there are issues involving the management of their identities by the focal organisation, and many more; these will be reviewed in the challenges section. There are also controls which apply exclusively to external insiders but not to outsiders or insiders such as B2B contracts containing security agreements.

Examples of external insiders are contractors, self-employed consultants, and any employee of other organisations participating in the focal organisation's extended enterprise who complies with the characteristics above.

THE E3VALUE TECHNIQUE

We review next the *e3value* modeling technique (Gordijn & Akkermans, 2003) used in the first step of our method. Figure 1 shows the e3value model of a simplified manufacturer-retailer B2B relationship.

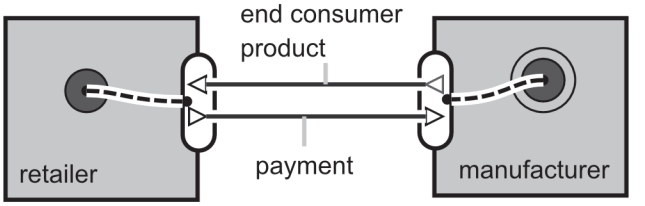
In the e3value model, manufacturer and retailer are actors, i.e. stakeholders with an economic interest. Actors have value interfaces represented by ovals that contains "in" and "out" ports (triangles) indicating the direction that a value object can be transferred from one actor to another. Value objects can be anything with value for the stakeholders involved such as money-related objects, products, services, or more intangible objects such as legal compliance. In the figure, the manufacturer transfers end consumer product to a retailer in exchange for payment transferred back by the retailer.

Value models are used to represent which economic exchanges take place when a business need occurs; a business need is represented by a filled circle. A dashed line, called a dependency path, connects all transactions performed to satisfy the need. In general, a dependency path is an acyclic and/or graph; it ends in one or more bull's eyes (filled circle with a halo). The path merely states which transactions have to occur, but not when they must occur, and so a value model is not a coordination process model (Gordijn et al., 2000). Paths in e3value allow the estimation of economic sustainability of the business model represented. We use e3value concepts to delimit a part of the extended enterprise for analysis of external insiders.

CHALLENGES CAUSED BY EXTERNAL INSIDERS

This section discusses challenges of the extended enterprise specifically related to external insiders. The analysis takes managerial and operational perspectives.

Figure 1. Value model of a simplified manufacturer-retailer relationship



Managerial Perspective

We selected five managerial challenges deemed more important; they are reviewed next.

- **Risk Management & Governance:** Security vulnerabilities and threats which impact a focal organisation have increased sharply with the expansion of organisational borders in an extended enterprise context. The external insider threat is one source of security risks, among many, to be considered. This situation calls for an extended-enterprise-wide risk management perspective away from an enterprise-wide perspective (Sutton, 2006; Starr et al., 2003) for a holistic view of (inter) dependencies and vulnerabilities. This represents a challenge because it requires a joint effort across different departments of the focal organisation – e.g., IT, legal, and business (Davis, 2010) – and beyond across different companies part of the extended enterprise. This need is constrained by potential conflicts of interests and the lack of visibility since transparency required for risk management is convenient for the focal organisation only.
- **Trust:** A company-trustor (who is expected to trust) has to rely on subjective indicators of trust to make decisions related to a B2B relationship. Such indicators are multi-dimensional and may involve factors related to *goodwill trust* (Jiang et al., in press) – benevolence, integrity, good faith – or *competence trust* − reputation, experience, statistics − (Karabulut et al., 2007). A calculation of trust is difficult to compute, and may give rise to complex structures like trust graphs (Wang & Wu, 2011). Another challenge about B2B trust is related to the fact that trust must be managed since the trustworthiness of a company-trustee (who have to be trusted) may deteriorate over time along the lifecycle of a B2B relationship.
- **Control:** There is no centralised control across an entire extended enterprise but rather distributed control mechanisms that may be spread across several organisations. For example, due to reduced and sporadic social interactions between insiders of the focal organisation and external insiders from another organisation, the chances of monitoring for detection of suspect behaviour by external insiders are limited. Note that there are some classes of external insiders, such as certain contractors and consultants, where this problem is reduced since they are usually socially embedded into the focal organisation. Moreover, the focal organisation has not necessarily visibility about internal controls enforced by other companies in its extended enterprise. For instance, screening prior to employment of external insiders may not happen.
- **Auditing and Monitoring:** In terms of auditing, audits provide snapshots at a particular point in time of processes carried out by a company within a certain scope, and may not reveal exactly how the company operates (Davis, 2010). In terms of monitoring, the focal organisation tends to have full access of fine-grained logged information about insiders and, in this case, monitoring and data aggregation for holistic auditing is possible. For a full overview of activities performed by external insiders, integration with information logged by other parties may be required for correlation to detect external insiders misuse; these other parties may keep this information confidential.
- **Expertise to Detect Threat:** In the case of insiders, there is internal expertise about the technologies used by the focal organisation. Likely, there are employees with know-how to detect misuse patterns and abnormal behavior. However, in extended enterprises, technology is often transferred, causing an evasion of expert knowledge; therefore, the focal organisation itself may lose the expertise to detect the threat that external insiders dealing with this technology may pose to its assets. Loss of knowledge or know-how is a recognised challenge in B2B partnerships (Beulen et al., 2006).

Operational Perspective

Numerous operational challenges arise from the external insider threat. Next we provide an overview of the challenges related to IAM (Identity and Access Management), and cascading risks in an extended enterprise.

- **Identity Management:** The problem that arises with external insiders' identities is the decoupling between who has visibility of physical persons and who has visibility of their digital identities. If the external insider is not embedded into the focal organisation (what often is the case), this decoupling becomes reality. As a consequence, the focal organisation has to rely on the timely and accurate communication of another organisation, which has visibility of external insiders as persons, to maintain identities and authorisations of its external insiders up-to-date. For example, a single organisation can have a very efficient interaction between the IT and the HR departments, to assure that access and privileges of terminated insiders are revoked quickly; this routine may even be automated. But if the insider is employed by another organisation, the event of termination involves the integration of the IT department of the focal organisation and the HR of another organisation, what makes the process more complex and subject to failures.
- **Access Management:** In security-conscious organisations, authorisations are granted on a need-to-know, individual basis and separation of duty policies are enforced to decrease the chance of assets being misused by insiders. However, in an extended enterprise setting, authorisations tend to be granted on a worst-case, partner basis (called shared identities (Baker et al., 2009)), i.e. higher-than-need-to-know authorisations are often granted, and separation of duty policies may not have guaranteed enforcement across the extended enterprise. Another issue of access management relates to consensus. Reaching agreements about the semantics of roles or authorisation attributes among business units of a same focal organisation is hard. Reaching such agreements across different organisational domains, as is the case in extended enterprises, is even harder (Karp et al., 2010).
- **Cascading Risks:** Extended enterprise typically have hundreds of bilateral relationships (Davis, 2010) forming a complex network of interdependent companies where each company can be seen as a node, and each relationship (which may represent a variety of concepts) as an arc (Jagdev & Thoben, 2001). Such representation allows the abstraction of extended enterprises and the modelling of important characteristics of such networks like their dynamic aspect and indirect connectivity established by subcontracting (Wiendahl & Lutz, 2002). However, it requires a holistic view of interdependencies, threats and vulnerabilities and this is challenging because: (i) organisations typically do not have enough information for this holistic assessment about external insiders, (ii) there is a need for a minimum level of security across all nodes of the network and this requires agreement on a number of aspects, e.g., on standards for enforcing and monitoring security across all of them, and (iii) highly connected nodes (i.e. hubs) need extra protection; this may be challenging because it requires incentives for the necessary extra spending.

SUMMARY OF CHALLENGES

Table 2 provides a cross-cutting overview of the discussed challenges related to the external insider threat problem.

So far, we have distinguished external insiders from outsiders and insiders, discussed challenges intrinsic to the problem of external insider threat, and concluded with a list of ten challenges. In the next sections we switch our focus to solutions.

Table 2. Summary of challenges related to external insiders and the threat they pose

Challenge	Description
1	Trust and risk management are important to counter the external insider threat, but they require a holistic view of interdependencies, and of threats and vulnerabilities to be effective.
2	Objective measurement of trustworthiness of other companies is fundamental for decision making (e.g., when engaging in new B2B contracts) and for a sounder trade-off analysis, e.g., between trust, risk and expected gain from a B2B relationship.
3	B2B contracts, when existent, are often broad and do not establish IT security agreements useful to counter the external insider threat.
4	Distribution of logging makes auditing and monitoring of external insiders hard to achieve.
5	Evasion of know-how related, e.g., to outsourced technology and IT infrastructure results in inability to detect external insider threat.
6	Some internal controls that work well for insiders do not work for external outsiders, e.g., behaviour monitoring.
7	Decoupling between who has visibility of external insiders as physical persons and who has only visibility of their digital identities in a B2B relationship results in mismanagement of authorisations for external insiders.
8	Higher-than-need-to-know authorisations for external insiders are difficult to detect and manage; this may be a consequence of challenges 4 and 7.
9	Consensus about semantics of roles and attributes for identity and access management across an extended enterprise requires reaching agreements that are difficult to achieve in practice; this may be aggravated by conflicting interests.
10	A minimum level of security has to be enforced across an entire extended enterprise and highly connected organisations need extra security to minimize the propagation of risks across a business network; this challenge has not only implications to security investments but also to counter external insider threat which may give rise to new cascading risks, such as the risk of knowledge sharing propagation.

POTENTIAL SOLUTION DIRECTIONS TO COUNTER THE EXTERNAL INSIDER THREAT

Organisational controls and security mechanisms that work to detect and prevent classical insider threat may not apply completely to counter the external insider threat; one example is user profiling and anomaly detection (for a survey of insider detection mechanisms, see Salem et al. (2008)). We review in this section three streams of research and practice proposed to deal with this problem; they partially address five of the identified challenges, namely challenges 1, 3, 4, 7 and 8 from Table 2.

First, the Jericho-Forum (n.d.) takes the view that the increasing connectivity of organisations can be solved by data-centric security, shifting security from complete systems or infrastructure to the data itself; i.e., storing the data centrally together with the applicable policies or allowing it to flow freely on a trusted infrastructure, where the policies stick to the data (van Cleeff & Wieringa, 2009). However, the feasibility of data-centric security is in doubt, because it may require classification of large amounts of data at a low level of granularity; moreover, it is hard to implement in extended enterprises. Therefore, data-centric security helps to improve challenge 8 (Table 2) but in cases where it helps, it may be prohibitively expensive.

Second, extended enterprises can opt for federated authentication architectures (Windley, 2005) to address challenge 7. In this case, each organisation keeps local control of its identities, and there is a higher-level mechanism to link these identities. This way, the focal organisation only deals with access management and is released from identity management regarding its

external insiders. However, although federated authentication can meet several levels of assurance (Burr et al., 2006), this architecture is only an alternative when there is a high level of B2B trust regarding identity management practices enforced by the other federated companies (e.g., no security vulnerabilities which may result in false identities (Smith, 2012)), agreed policies between all members of the federation, and consensus about identity attributes, such as roles (Karp et al., 2010). If there is no visibility over identity management of all other companies in the extended enterprise, the focal organisation cannot assess the external insider threat properly. To reduce this problem, the focal organisation has to opt for expensive assurance solutions, such as regular external auditing or, even more cost prohibitive, permanent internal auditing of the identity management of the other companies. Such audits to achieve certification check evidences that processes comply with best practices (e.g., with the security standard ISO/IEC 27001 (2005)) or test internal controls (e.g., the SAS70 (AICPA, 2000) type 2 audit) at a given point in time. However, successful audits do not necessarily translate to security (Valentine, 2010; Davis, 2010). External/internal audits and certification can only be partially effective to detect misuse by external insiders (Davis, 2010), and therefore to address challenges 1 and 4 (Table 2).

A third approach is to rely on third party agreements made explicit in the B2B contracts, e.g., via Security SLAs. The main problem is that B2B contracts are often very high-level, allowing each party to interpret the contracts in different ways, depending on the context, which does not help to understand and solve potential security issues, such as external insider threat. We take the perspective that improving IT security agreements in B2B contracts is a step forward to deal with the external insider threat, therefore, we propose improvements to a solution in this direction, i.e., the method first introduced in Franqueira et al. (2012) to support engineering of security agreements. The method partially addresses challenges 3 and 8 (Table 2) via the outcome of steps 5 and 6.

Other challenges are addressed by future research directions, as discussed later in the paper.

SOLUTION TOWARDS EXTERNAL INSIDER THREAT ANALYSIS

Existing standards, such as ISO/IEC-27002 (2005, Section 6.2), list *what* should be in place to promote security governance in extended enterprises but not *how* to identify external insiders in the first place and *how* to achieve security agreements. From case studies we performed, we have learned that this is a challenge in itself, and that even security-conscious organisations have problems identifying those individuals in their extended enterprise that might pose a threat. Our method shows how organisations can identify external insider roles and how they can analyse them to support the engineering of security agreements.

Rather than assessing the security of systems directly (as is often done in risk assessments) we take a top-down holistic approach for two reasons. First, we wish to understand the broader context of systems and the people involved, and avoid diving unnecessarily deep into technical details. Only when it is necessary or useful should organisations zoom into technical implementations of their systems. Second, in an extended enterprise setting, such technical details are often not available for review, because they are under the control of other organisations.

As such, our method is very distinct from the approach that one would take to identify insiders and mitigate their threat: insiders are part of the organisation, are on the payroll and their responsibilities and authorisations for applications can be checked much easier.

We refine and improve the method first introduced in Franqueira et al. (2012) for the analysis of external insider threat (Table 3). Although the number of steps has been maintained, steps 3, 4 and 5 have changed to provide a better analysis of external insider roles in terms

of activities and required access to IT-related assets, therefore, allowing the elicitation of need-to-know requirements which complement the outcome of step 6.

The first part of the method aims at the identification of external insider roles for a specific part of the extended enterprise; this part comprehends three steps: (1) value modelling to limit the scope of the analysis and identify companies involved, (2) coordination modelling to understand the business processes involved, and (3) IT architecture modelling to provide an overview of systems and connections to support the business process. The second part of the method aims at aims at the analysis of external insider roles; this part also comprehends three steps: (4) identification of external insider roles and activities they have to perform to fulfill their duties in respect to the focal organisation, (5) access matrix for the elicitation of external insiders' need-to-know requirements, and (6) reverse engineering of security best practices, considering external insiders as source of threat and as enforcers of security in the behalf of the focal organisation, for the elicitation of security requirements.

Our motivation for the use of value models as the starting point of the proposed method derives from the fact that extended enterprises are economic networks, where each actor performs an economic role. Value models allow us to represent these business roles: who provides something of value to whom, and which reciprocal value is obtained in return. From the value model, each model provides motivation for the content of the next one. For instance, the processes depicted in the coordination model are needed to create value, as per the value model. The same way, the IT resources depicted in the IT architecture model are needed to support the processes depicted in the coordination model. However, the last two steps of the method are complementary rather than sequential as the previous steps. They both provide input for security agreements.

In the next section, the method is illustrated with a realistic retailer-manufacturer example.

METHOD APPLIED TO A RETAILER-MANUFACTURER EXAMPLE

Step 1: Value Modelling

Figure 2 shows a detailed *e3value* model of the manufacturer-retailer relationship presented earlier in a simplified form in Figure 1.

The simplified view (Figure 1) only showed the retailer need being satisfied by the manufacturer, and the economic exchange between them. The detailed view (Figure 2) shows that there are other companies involved in satisfying this basic need. For example, the manufacturer has to collect taxes when selling products and, as a consequence, the manufacturer has an economic exchange with the tax office for legal compliance. In addition, the manufacturer itself has its needs in order to fulfill the retailer and

Table 3. Steps in the method and their output (extended from Franqueira et al. (2012))

Step	Description	Output
1	Value modelling	Scope delimited and companies involved identified
2	Coordination modelling	High-level business processes identified
3	Architecture modelling	Relevant systems and connections identified
4	External insider roles	External insider roles & activities performed for the focal organisation identified
5	Access matrix	Need-to-know requirements for external insider roles identified
6	Reverse engineering of best security practices	Security requirements related to external insiders from the perspectives of pose-threat and enforce-security identified
		The output of Steps 5 and 6 provides input for engineering of IT security agreements

government needs; these are fulfilled by service providers which manage the ERP system (SAP), the business transactions (EDI) and the call center, in exchange for payment. The logistics partner (warehouse & carrier) has also been modelled as an actor which fulfills the manufacturer's need to fulfill, itself, the retailer's need. This modelling choice implies that logistics are considered an indirect cost (Porter, 1985) for the purpose of this example.

Value modelling provides a rationale to set the scope of the analysis of external insiders by delimiting one part of the extended enterprise that realises a main business interaction, in this case, between manufacturer and retailer. However, it does not provide an overview of sequencing of activities among those business parties. But, since this information is essential to identify business processes involved in satisfying the value exchanges, coordination modelling is the next step of our method.

Step 2: Coordination Modelling

We assume EDI (Electronic Data Interchange) documents are the basis upon which trading partners cooperate, and therefore, coordinate their operations. Coordination between different parties of the value chain is a key aspect for the order process fulfillment (Croxton, 2003). Figure 3 shows the main coordinated interactions between the trading parties of the example in a simple sequence diagram. The other three service providers not present in the diagram (call center, data center and EDI-managed providers) are implicitly represented by the manufacturer, and therefore not visible, in the coordination model.

The process starts when a retailer issues an EDI-based Purchase Order (PO) to the manufacturer (item 1 in Figure 3). The order specifies which products the retailer wants to purchase and in which quantities. This triggers activities on the manufacturer side related to the approval of the PO. After approval, an EDI-based Shipment Advice is sent from the manufacturer to the warehouse (item 2). In general terms, this is an indication for the warehouse to get ready to release the products listed on the PO from stock. It triggers activities related to the replenishment of the manufacturer stock, such as those related to resource planning and purchase orders to suppliers. The manufacturer also sends an EDI-based Shipment Order (item 3) to the carrier. This document alerts the carrier to be ready to transport the products to the retailer, again triggering activities related to the manufacturer inventory management. Next, the manufacturer usually sends an EDI-based Shipment Notice to the retailer with details related to the delivery of the products (item 4), followed by an EDI-based invoice (item 5). The invoice triggers the update of accounts receivable on the manufacturer side. The next two steps involve the delivery of products (item

Figure 2. Value model showing a detailed manufacturer-retailer relationship (expanded from Figure 1)

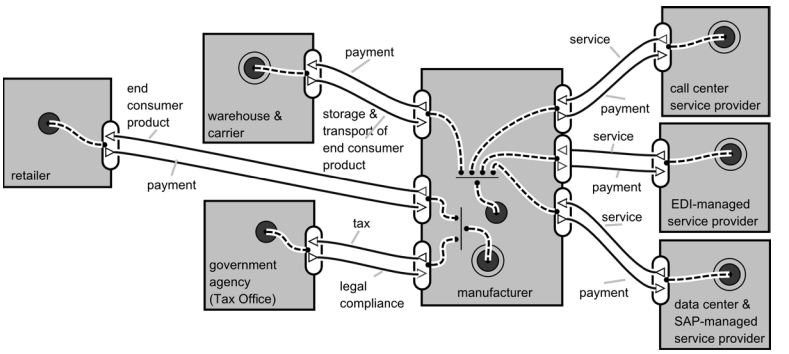
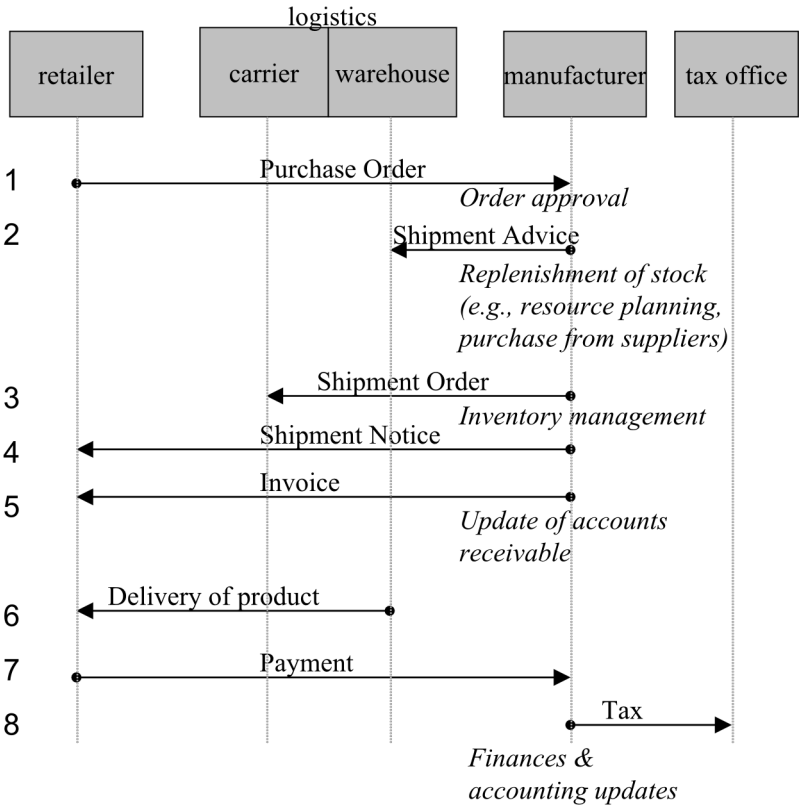


Figure 3. Model showing the main coordination activities among the trading parties



6) executed by the carrier that transports them from the warehouse to the retailer address, and the actual payment of the products received to the manufacturer (item 7). The last step (item 8) refers to the payment of taxes to the tax office by the manufacturer, triggering finance and accounting back-office activities.

The coordination model increases understanding about the part of extended enterprise modelled but is not enough to identify the external insider roles and to assess their capabilities to pose threat. For that, we need to model the IT architecture that supports this coordination including the activities triggered. We do this in the next step of our method.

Step 3: IT Architecture Modelling

Figure 4 shows the IT architecture used by our example manufacturer. It is consistent with both the value and the coordination models presented previously in the sense that the companies with this IT architecture can perform the coordination process described in the sequence diagram of Figure 3 and, doing so, can perform the transactions represented in the value model of Figure 2. Our method does not prescribe an architecture (or coordination process notation) and any architecture notation understandable by the stakeholders is acceptable. The diagram in Figure 4 essentially shows different parties (organisational boundaries), communication channels linking these parties (and thus crossing those boundaries), users' functionalities and IT infrastructure supporting these. Security officers and IT architects are familiar with this kind of diagram and find them easy to use.

One interesting aspect to notice is the fact that the trading partners and service providers represented in the value model (Figure 2) are

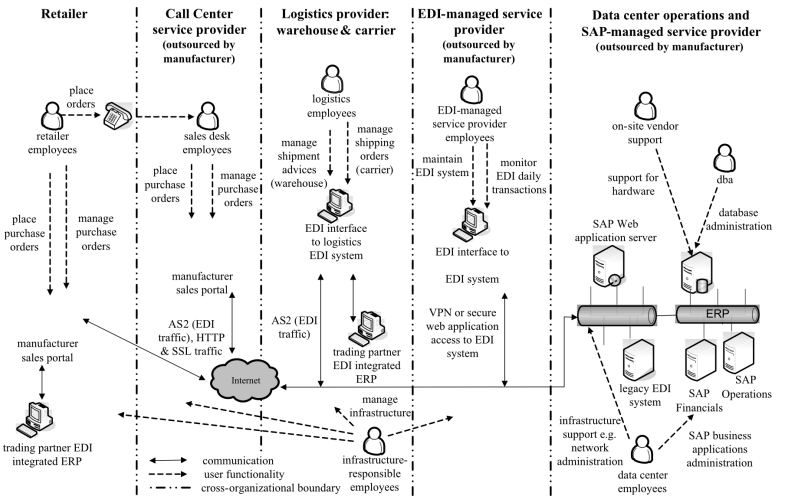
also part of the IT architecture diagram, but not the manufacturer itself. This is because the front- and back-office activities of the coordination model (Figure 3) are performed by service providers on behalf of the manufacturer.

As indicated earlier, the starting point is a Purchase Order (PO). Employees of the retailer can place and manage POs in two ways. They can use the manufacturer sales portal; alternatively, they can use the manufacturer call center and ask a sales desk employee to place and manage their orders. The EDI-based documents, such as POs, are usually transmitted via Applicability Statement 2 (AS2, n.d). AS2 is a standard which defines secure transmission over HTTP, used to send and receive EDI files over the Internet. AS2 connections require certificates issued by a Certificate Authority (Bishop, 2003) from both parties involved and use encryption for data transmission. A PO transmitted by the retailer or the sales desk employee is therefore sent via an AS2 connection to the EDI system located in the manufacturer's data center. The EDI system basically processes EDI files, and is integrated with the manufacturer's ERP (Enterprise Resource Planning) infrastructure. In our example, the manufacturer has a SAP ERP (http://www.sap.com/solutions/business-suite/erp), and this integration occurs via an interface based on SAP IDoc (Intermediate Document) technology; via this interface, documents are transferred from the EDI system to ERP systems and vice versa.

After a PO is approved, several exchanges of EDI-based files occur between the ERP infrastructure of the retailer, warehouse/carrier and the manufacturer, as shown in Figure 4. For example, employees from the logistics partner, i.e. the warehouse and carrier employees will have an EDI interface to access their logistics EDI system, used to manage shipping advices and orders. The activities triggered at each step of the whole process are performed by different business applications part of the manufacturer ERP infrastructure. For example, item 5 in Figure 4 involves SAP Financials to issue an invoice and send it automatically to the retailer, and to update the receivable accounts.

The manufacturer's legacy EDI system (located in its data center) is managed remotely by a service provider, as often happens in practice and illustrated in the diagram in Figure 4. Employees at the EDI-managed service provider perform tasks related to: (i) maintenance of the EDI system and (ii) monitoring of EDI daily transactions (AS2, n.d.). The manufacturer's

Figure 4. Model showing an IT architecture that realises the value and the coordination models presented in Figures 2 and 3, respectively



ERP (platform and applications), including databases (data) and the sales portal (SAP web application and web server), as well as the IT infrastructure, are all managed, in our example, by the data center provider. Next, we identify the external insider roles that support the activities described in this section.

Step 4: External Insider Roles

All the roles represented in the IT architecture diagram in Figure 4 refer to external insider roles with respect to the focal company, i.e. the manufacturer. Therefore, this diagram provides a list of external insider roles and activities in the manufacturer-retailer example, as shown in Table 4.

Interesting to observe is the fact that external insiders, on the one hand, pose security threats to the manufacturer but, on the other hand, they can also be in a position to enforce security on behalf of the manufacturer. We look at access required by external insider roles to fulfill their activities in the next section.

Step 5: Access Matrix

We identify sensitive data using the IT architecture shown in Figure 4. Table 5 shows a non-exhaustive list of IT-related assets on the vertical axis and external insider roles, identified in step 4, in the horizontal axis; each cell contains an "X" if the role requires access to the asset. The matrix represents a way to understand need-to-know requirements for different external insiders roles from the business perspective.

Acknowledging need-to-know requirements for external insider roles is important for two reasons. First, it helps to draw more specific IT security agreements as a proactive security measure against external insider threat. Second, it helps to audit those requirements as a reactive security measure during the lifetime of a B2B relationship. The next step complements this step by taking a broader view of external insider prompted by best practices.

Step 6: Reverse Engineering of Security Best Practices

In order to further analyse external insider threat, we propose a backward reasoning process from security best practice that provide security requirements to be fulfilled. In this case, we use the PCI DSS (Payment Card Industry Security Standards Council, 2010) standard, which defines 12 broad security requirements for companies dealing with cardholder payment data. Again, our method does not prescribe specific best practices to be used, e.g., HIPAA (2003) security standard is an alternative, or even the

Table 4. Output of the step 4, i.e., external insider roles and activities they perform

External insider role	Activity performed
Retailer employee	Places and manages purchase orders
Sales desk employee	Places and manages purchase orders on the behalf of the retailer
Logistics employee	Manages shipping advices and shipping orders involved with the delivery of products for the retailer
EDI-managed employee	Maintains the manufacturer EDI system and monitors EDI daily transactions
Network administrator	Manages network at data center
Infrastructure-responsible employee	Manages IT infrastructure at retailer, call center, logistics & EDI-managed
SAP administrator	Manages SAP business applications at data center
Sales portal master	Manages the manufacturer sales portal
Database administrator	Manages databases at data center
On-site vendor support	Manages data center specific hardware

Table 5. Output of step 5, i.e., access matrix for external insider roles

Assets vs. Roles	Manufacturers' price lists	Trading EDI-based documents	Payment details	Credentials to transmit EDI docs	Passwords to log on servers	Credentials to update sales portal	Passwords to configure IT infrastruct.
Retailer employee		X	X	X			
Sales desk employee	X	X	X	X			
Logistics employee		X		X			
EDI-managed employee		X		X	X		
Network administrator					X		X
Infrastructure-responsible employee					X		X
SAP administrator					X		
Sales portal master					X	X	
Database administrator					X		
On-site vendor support					X		X

controls from ISO/IEC-27002 (2005) for a more comprehensive analysis of external insiders.

PCI requirements represent possible mitigation to be included in an IT security agreement. However, they are too generic and not tailored to external insiders. Therefore, we evaluate each requirement from two perspectives: external insiders as security threat and external insiders as security enforcers, considering the external insider roles identified in step 4. Results are shown in Table 7 in the Appendix.

The outcome of Tables 5 and 7, overall output of the method, provides additional support for negotiation of IT security agreements as addendum to B2B contracts.

Note that the proposed method defines a rationale for the identification of external insider roles (step 4) and of need-to-know requirements for those roles (step 5). It also defines a rationale for the analysis of the external insider threat (step 6). Unlikely full risk assessment however, its coarse grained result does not provide a list of risks and mitigation.

DISCUSSION

Steps 4-6 complement rather than feed each other, as it happens with steps 1-3. Table 5 provides an overview of access required for external insider roles to perform their duties from the point-of-view of the business needs of the focal organisation. Together with Table 4, we obtain the basic elements of access control in respect to the focal organisation (Ferraiolo et al., 2003): *subjects* are the external insider roles (Tables 5 and 6), *objects* are the different assets (Table 6), *operations* are of the type "access" to perform different activities (Table 5), i.e., to perform their duties; *permission* (or

privileges) derives from the combination of object and operation. For example, one need-to-know requirement we can derive from Tables 4 and 5 is: "The sales desk employee" should have "access to the manufacturer's price list" to "place and manage purchase orders (to the manufacturer) on the behalf of the retailer". The analysis in Table 5, however, pointed to the threat of having sales desk employee performing the same tasks for different customers, e.g., accessing price lists of competitors' manufacturers. Therefore, apart from the set-up of the need-to-know requirement, there is a need to negotiate security requirements to mitigate this threat, such as the review of the actual access control list, and even restrictions in the use of USB ports, restrictions about emailing price lists. Therefore, this is the how the outcome of our method helps the engineering of security agreements.

The analysis proposed in step 6 also complements step 4 in the sense that more external insider roles that should perform other activities become visible. For instance, Table 7 mentions in the "external insiders as security enforcers" column, several instances of "external insider responsible… should be appointed at contracted parties". Such activities need to be further investigated and refined to generate further security agreements.

RELATED WORK

Modelling organisations, inter-organisational relations and IT architectures can be done using several modelling techniques, each focusing on specific aspects. Well-known modelling frameworks include UML and ArchiMate (The Open Group, n.d.). ArchiMate, for example, models three perspectives of enterprise architecture, i.e. business, application and IT layers, and their interrelations to support the alignment among them (Steen et al., 2004). Our method also models three perspectives, namely value, coordination and IT architecture, but to achieve a completely different goal: to identify external insider roles. The perspectives we use have been proposed by Gordijn and Akkermans (2003) and Wieringa et al. (2008), and provide a systemic way to delimit and explore the context in which external insiders act, providing the basis for the analysis of external insider threat. Nevertheless, we assume that other frameworks can be used for the same purpose, depending on the techniques adopted by the focal organization or the preferences of the modeller.

For extended enterprises, IT security agreements are prescribed as best practice to counter risks related to the extended enterprise by the ISO/IEC-27002 (2005, Section 6.2.3). However, the guidelines are generic and must be complemented by techniques to implement them, i.e., for the specification of such agreements, and our method fills this gap. Another important difference between ours and the ISO 27000 family approach is that we focus on threats rather than risks. In extended enterprises it is difficult to get information to assess risks because it involves knowledge of existing vulnerabilities. The IT Information Library (ITIL, 2011a; ITIL, 2011b) for IT Service Management includes processes for security management prescribing a security section in Service Level Agreements (SLAs) between B2B service providers and customers. According to ITIL, SLAs should be further specified in Operational Level Agreements in the format of security plans covering: personnel security to prevent crime and fraud, security policies and access security. Again, these are generic best practices and our method helps to achieve such security agreements in respect to external insiders.

The Control Objectives for Information and related Technology (COBIT, 2012a) supports IT governance via processes and controls driven by the alignment between business and IT objectives. COBIT 5 for Information Security (COBIT, 2012b) specifically focuses on information security governance. The processes described in COBIT are too broad and must be complemented by other standards, techniques and good practices such as the HIPAA (2003) Security Rule and the PCI DSS (Payment Card Industry Security Standards Council, 2010). The COSO (1994) framework provides an internal control model that allows organisations

Table 6. Mapping between challenges summarized in Table 2 and solution directions

Challenge	Solutions and research directions
1	Present: Certifications/auditing Future: Holistic View of Security Risks
2	Future: Reputation Systems for B2B Decision Making
3	Present: Proposed method for engineering security agreements
4	Present: Certifications/auditing
5	No solution direction identified in this paper
6	Future: Holistic View of Security Risks
7	Present: Federated Authentication Architecture Future: New Access Control Paradigms
8	Present: Data Centric Security Present: Proposed method for engineering security agreements Future: New Access Control Paradigms
9	Future: New Access Control Paradigms
10	Future: Extended Enterprise from a Network Perspective

to check their own controls to achieve, for example, financial reporting compliance with the Sarbanes-Oxley Act (Sarbanes & Oxley, 2002). Control activities related to security of assets and segregation of duties are part of the model, and may be used as best practices for reverse-engineering in step 6 of our method as an alternative to the PCI DSS analysis of external insider threat.

Our method is not a full risk assessment methodology such as the ones proposed in frameworks like the CRAMM (Insight Consulting, 2005), OCTAVE (Alberts & Dorofee, 2002), CORAS (den Braber et al., 2007) and ISO/IEC-27005 (2011). A full risk assessment is very expensive, and might not even be possible at all, to perform in an extended enterprise context because of incomplete information available from other organisations which prevent to assess vulnerabilities. We do use a model-based approach, as in CORAS, but with the difference that CORAS' models are used to assist in risk assessment; e.g., they use diagrams to analyse causal relationships between threat, vulnerability, risk, unwanted incident (consequence), and asset potentially affected. We use models that have a different purpose and represent other types of relations. Our models are useful to (i) zoom-in on a relevant part of the extended enterprise from a value perspective, help to understand (ii) the B2B coordination involved and (iii) the supporting IT architecture, with an ultimate purpose: identify external insider roles and engineer security agreements to counter the external insider threat.

Since our method concerns security threat analysis, we turn to this topic now. Threat concerns the potential for a *threat agent* to exploit a particular vulnerability (NISTIR-7298, 2006), either intentionally or accidentally, resulting in a risk. There are three main approaches for security threat analysis. The first approach for threat analysis is to focus on agents' attack potential determined by factors such as motivation, abilities (e.g., skills, expertise, and resources) and strategies to comprise or misuse an asset. For example, the Threat Agent Library by Intel (Casey et al., 2010) classifies threat agents in terms of the following characteristics: intent, access, outcome (i.e., goal), limits (i.e., constraints), resource level, skill level, objective (i.e., attack strategy), and visibility. The eTVRA method (Rossebo et al., 2006; ETSI-TS-102-165-1, 2011) evaluates attack potential based on threat agents' knowledge about an asset to be compromised, time required to suc-

cessfully launch an attack, expertise required, opportunity window in terms of required access for a period, and equipment required to launch an attack (i.e., hardware and software). The second approach for threat analysis is to focus on types of attack. One typical example is the STRIDE threat model (Microsoft, 2002). It provides six classes of threat (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and the threat analysis consists of evaluating whether these threats affect a specific IT asset. The third approach for threat analysis is to focus on profiles or taxonomies of threat agents. Profit-driven and fame-driven are profiles of threat agents based on their intention and goals (Leeson and Coley, 2006). Profit-driven agents are motivated by financial greed and typically target assets with high perceived value, while fame-driven agents are motivated by notoriety (e.g., peer recognition and media attention) as a function of inventiveness and severity, and typically aim at maximum disruption and impact. Another example of threat agent profiling is the taxonomy by Anderson (1980). He classifies the threat agent *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. These three threat analysis approaches are hardly applicable to external insiders because of the large landscape of threat agents and the variety of their characteristics (Davis, 2010), added to the extent of their potential to compromise the focal organisation IT assets. Therefore, our method first provides a rationale to scope and understand the context which allows pinpointing external insider roles, then it concentrates specifically on their access requirements and finally on their ability to cause threat or enforce security based on security best practices with the ultimate goal of engineering security B2B agreements.

FUTURE RESEARCH DIRECTIONS

This section suggests three directions for future research. Table 6 maps these future directions, as well as potential solutions directions identified and the proposed method to the challenges summarized in Table 2. Potential solutions to challenge 5 are not addressed in this paper.

New Access Control Paradigms

One research direction to overcome the identity and access management challenge mentioned in the challenges section is the use of an alternative access control model which avoids the inherent problems of centralised and federated identity architectures. One step forward in this direction is the authoriZation Based Access Control (ZBAC) model proposed by Karp et al. (2010). It shifts the paradigm of access control from authentication-based (such as in Role Based Access Control), where access decisions are made *after* the authentication of the requester, at request time, this way determining the authorisations the requester has, to authorisation-based, where access decisions are made *before* the request is made based on authentication of the requester; authorisation tokens are submitted along with the access request.

ZBAC has three features of interest: (i) it allows distributed access control where identity and access management are locally controlled, (ii) it allows accountability of responsibility for the access granting process, and (iii) it allows delegation of a sub-set of authorisations that a user has, decreasing the need for password sharing.

Extended Enterprise from a Network Perspective

One research direction towards better dealing with cascading risks in extended enterprise is to increase understanding of business networks from a network perspective. This calls for studies of real cases to gain insights in their structure, size, connectivity and other characteristics related to the external insider threat.

Results may potentially push development on the conceptual front, allowing more accurate modelling and automatic reasoning about business networks. Results may also allow the confirmation of some hypothesis, such as that business networks are scale free (Huang et al., 2008), triggering further research to answer in which circumstances they are scale free or not, and whether scale-free network properties (Barabási, 2002) apply to them.

Holistic View of Security Risks

Several challenges related to the external insider threat have their cause grounded in the lack of a holistic view of security risks. However, because the spectrum of threat posed by external insiders is so large, one way forward is to scale down on one very specific aspect of this threat while still aiming for its holistic view across the extended enterprise. For example, Aljafari and Sarnikar (2009) proposes a method to assess knowledge sharing risks in inter-organisational networks, while Jiang et al. (in press) address the risk of knowledge leakage in inter-organisatonal networks. Our method can also help in this direction by providing a rationale for the analysis of one specific aspect related to external insider roles such as risks related to knowledge sharing, knowledge leakage, or high-privilege access. Such methods, combined with the network perspective of extended enterprises (discussed above), represent an interesting research direction which could be expanded to draw conclusions about the expected propagation of confidentiality and integrity-related risks.

Reputation Systems for B2B Decision Making

One research direction that supports a more objective evaluation of business trustworthiness is the use of online reputation-based systems. Such systems are very common in B2C (e.g., amazon.com) and C2C (e.g., ebay.com) relationships, but are underexplored in B2B relationships. Although they have the potential to provide a measure of trustworthiness about companies which the focal organisation has not interacted before (as opposed to internal evaluation systems), it involves a number of issues. For instance, the target business needs to be evaluated on a number of criteria and different people from the source business are in a best position to evaluate subsets of criteria depending on their department, their involvement with the target business, or their competence or position. One step forward in this direction is the work by Dikow et al. (2013). They tackle the issue of low raters' expertise, which can negatively influence the accuracy of reputation systems' output, and propose an algorithm to infer expertise and filter out sub-criteria evaluated by non-experts. As a complementary solution direction, B2B reputation systems can be enhanced with trade-off engines for the aggregation of different aspects (e.g., trustworthiness, risk and benefit criteria) to support B2B decision making, as proposed by Franqueira et al. (2010b).

CONCLUSION

The external insider threat is a growing problem which is becoming ever more complex as transitive trust is imposed in inter-organisational networks. One recognised way to address this threat is to negotiate security agreements in B2B contracts (e.g., in SLAs). However, these contracts are typically too broad, generic and do not cover non-quantifiable security requirements. This paper contributed towards the engineering of such security agreements to improve the governance of external insiders. Based on feedback from a case study on a multinational manufacturer, we described an improved version of our method to identify external insider roles in a delimited part of the extended enterprise, to analyse their need-to-know requirements from a business perspective and to analyse security requirements from a pose-threat and security-enforcement perspectives. The method leverages from conceptual modelling, access matrix and reverse-engineering reasoning. The paper also reviewed challenges posed by external insiders, solutions available, and indicated four streams of future research to address some of the challenges identified.

REFERENCES

AS2. (n.d.). *AS2 processing for EDI*. Retrieved March 2010, from http://www.dcs-is-edi.com/AS2.html

AICPA. (2000). *Auditing standards board. Statement on Auditing Standards No. 70, Service Organizations. Professional Standards* (Vol. 1). American Institute of Certified Public Accountants.

Alberts, C., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach* (1st ed.). Boston, MA: Addison-Wesley.

Aljafari, R., & Sarnikar, S. (2009). A framework for assessing knowledge sharing risks in inter-organizational networks. In *Proceedings of the AIS Americas Conference on Information Systems (AMCIS 2009)*. AIS Electronic Library (AISeL).

Anderson, J. P. (1980). *Computer security threat monitoring and surveillance*. Fort Washington, PA: James P. Anderson Co.

Baker, W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., et al. (2009). *2009 data breach investigations report*. Verizon Business Security Solutions. Retrieved September 2009, from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp .pdf

Baker, W. H., Hylender, C. D., & Valentine, J. A. (2008). *Data breach investigations report*. Verizon Business Security Solutions. Retrieved September 2008, from www.verizonbusiness.com/resources/security/databreachreport.pdf

Barabási, A.-L. (2002). *Linked: How everything is connected to everything else and what it means for business and everyday life*. Cambridge, MA: Perseus Publishing.

Baraldi, E., Gressetvold, E., & Harrison, D. (2012). Resource interaction in inter-organizational networks: Introduction to the special issue. *Journal of Business Research*, *65*, 123–127. doi:10.1016/j.jbusres.2011.05.010

Bernsmed, K., Jaatun, M. G., Meland, P. H., & Undheim, A. (2011). Security SLAs for federated cloud services, In *Proc. of the Sixth International Conference on Availability, Reliability and Security (ARES'2011)* (pp. 202-209). IEEE Press.

Beulen, E., Ribbers, P., & Roos, J. (2006). *Managing IT outsourcing, governance in global partnerships*. Abingdon, UK: Routledge.

Bhala, S., Christodoulides, M., Cornwell, L., Jones, R., & Morris, B. (2010). *UK security breach investigation report - An analysis of data compromise cases*. 7Safe Limited. Retrieved March 2010, from http://7safe.com/breach_report/Breach_report_2010.pdf

Bishop, M. (2003). *Computer security: Art and science*. Boston, MA: Addison-Wesley.

Bishop, M. (2005). Position: Insider is relative. In *Proceedings of the 2005 New Security Paradigms Workshop (NSPW'05)* (pp. 77–78). ACM Press.

Borgatti, S. P., & Halgin, D. S. (2011). On network theory. *Organization Science*, *22*, 1168–1181. doi:10.1287/orsc.1100.0641

Brackney, R. C., & Anderson, R. H. (2004). *Understanding the insider threat: Proceedings of a March 2004 workshop*. Retrieved March 2010, from www.rand.org/pubs/conf_proceedings/2005/RAND_CF196.pdf

Burr, W. E., Dodson, D. F., & Polk, W. T. (2006). *NIST special publication 800-63: Information security. Version 1.0.2*. National Institute of Standards and Technology.

Casey, T., Koeberl, P., & Vishik, C. (2010). Threat agents: A necessary component of threat analysis. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research* (pp. 56:1-56:4). ACM Press.

COBIT. (2012a). *Control objectives for information and related technology - version 5*. Information Systems Audit and Control Association.

COBIT. (2012b). *COBIT 5 for information security*. Information Systems Audit and Control Association.

COSO. (1994). *Internal control - Integrated framework by committee on sponsoring organizations of the treadway commission*.

Croxton, K. L. (2003). The order fulfillment process. *The International Journal of Logistics Management*, *14*(1), 19–32. doi:10.1108/09574090310806512

Das, T., & Teng, B.-S. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review*, *23*(3), 491–512.

Davis, A. (2010). Managing third parties − An information security perspective. *Network Security*, (5): 13–15. doi:10.1016/S1353-4858(10)70057-X

den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps - a guided tour to the CORAS method. *BT Technology Journal*, *25*(1), 101–117. doi:10.1007/s10550-007-0013-9

Dikow, H., Hasan, O., Kosch, H., Brunie, L., & Sornin, R. (2013). *Improving the accuracy of business-to-business (B2B) reputation systems through rater expertise prediction (Tech Report)*. Lyon, France: University of Lyon.

ETSI-TS-102-165-1. (2011). *Part 1: Method and proforma for threat, risk, vulnerability analysis*. European Telecommunications Standardisation Institute (ETSI), v 4.2.3.

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003). *Role-based access control*. Norwood, MA: Artech House Press.

Franqueira, V. N. L., Houmb, S. H., & Daneva, M. (2010b). Using real option thinking to improve decision making in security investment. In *Proceedings of the 2010 International Conference on On the Move to Meaningful Internet Systems (OTM'10)* (pp. 619−638). Springer Press.

Franqueira, V. N. L., van Cleeff, A., van Eck, P. A. T., & Wieringa, R. J. (2010a). External insider threat: A real security challenge in enterprise value webs. In *Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES'2010)* (pp. 446–453). IEEE Press.

Franqueira, V. N. L., van Cleeff, A., van Eck, P. A. T., & Wieringa, R. J. (2012). Securing the extended enterprise: A method for analyzing external insider threat. In Gupta, M., Walp, J., Sharman, R. (Eds.), Strategic and practical approaches for information security governance: Technologies and applied solutions (pp. 195-222). Hershey, PA: Information Science Publishing (IGI Global). ISBN 978-1-46660-197-0.

Gordijn, J., Akkermanns, J. M., & van Vliet, J. C. (2000). Business modelling is not process modelling. In Conceptual modeling for e-business and the web (pp. 40–51), LNCS 1921. Springer Press.

Gordijn, J., & Akkermans, J. (2003). Value-based requirements engineering: Exploring innovative e-commerce ideas. *Requirements Engineering Journal*, *8*, 114–134. doi:10.1007/s00766-003-0169-x

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, *78*(6), 1360–1380. doi:10.1086/225469

Gupta, A., & Zhdanov, D. (2007). Growth and sustainability of managed security services networks: An economic perspective. In *Proceedings of the 7th Workshop on the Economics of Information Security (WEIS'07)*. Retrieved March 2010, from http://weis07.infosecon.net/papers/65.pdf

Hakansson, H., & Ford, D. (2002). How should companies interact in business networks? *Journal of Business Research*, *55*, 133–139. doi:10.1016/S0148-2963(00)00148-X

Hayden, M. V. (1999). *The insider threat to U.S. government information systems*. Advisory Memoranda NSTISSAM INFOSEC 1-99.

Henning, R. R. (2000). Security service level agreements: Quantifiable security for the enterprise? In *Proc. of the 1999 Workshop on New Security Paradigms (NSPW'99)* (pp. 54-60). ACM Press.

HIPAA. (2003). *HIPAA security rule.* Retrieved June 2013 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Huang, C. D., Behara, R. S., & Hu, Q. (2008). Managing risk propagation in extended enterprise networks. *IT Professional*, *10*, 14–19. doi:10.1109/MITP.2008.90

Insight Consulting. (2005). *CRAMM user guide. Risk analysis and management method*. Version 5.1.

ISO/IEC-27001. (2005). *Information technology. Security techniques. Information security management systems. Requirements*.

ISO/IEC-27002. (2005). *Information technology. Security techniques. Code of practice for information security management.*

ISO/IEC-27005. (2011). *Information technology. Security techniques. Information security risk management.*

ITIL. (2011a). *ITIL service design*. The Stationery Office Edition.

ITIL. (2011b). *ITIL service transition*. The Stationery Office Edition.

Jaatun, M. G., Bernsmed, K., & Undheim, A. (2012). Security SLAs – An idea whose time has come? In *Proc. International Cross-Domain Conference and Workshop (CD-ARES'2012)* (pp. 123-130). Springer Press.

Jagdev, H. S., & Thoben, K. D. (2001). Anatomy of enterprise collaborations. *Production Planning and Control*, *12*(5), 437–451. doi:10.1080/09537280110042675

Jericho-Forum. (n.d.). *The what & why of de-perimeterization*. Retrieved from http://www.opengroup.org/jericho/deperim.htm

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*.

Karabulut, Y., Kerschbaum, F., Massassi, F., Robinson, P., & Yautsiukhin, A. (2007). Security and trust in business outsourcing: A manifesto. *Electronic Notes in Theoretical Computer Science*, *179*, 47–58. doi:10.1016/j.entcs.2006.08.030

Karp, A. H., Haury, H., & Davis, M. H. (2010). From ABAC to ZBAC: The evolution of access control models. *ISSA (Information Systems Security Association)*. *Journal*, *8*(4), 22–30.

Kumar, K., & van Dissel, H. G. (1996). Sustainable collaboration: Managing conflict and cooperation in interorganizational systems'. *MIS Quartely*, *20*, 279–300. doi:10.2307/249657

Leeson, P. T., & Coyne, C. J. (2006). The economics of computer hacking. *Journal of Law*. *Economic Policy*, *1*(2), 511–532.

Microsoft. (2002). *The STRIDE threat model.* Retrieved August 2013, from http://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx

Morali, A., & Wieringa, R. J. (2010). Risk-based confidentiality requirements specification for outsourced IT systems. In *Proc. of the 18th IEEE Int. Requirements Engineering Conference (RE'10)* (pp. 199-208). IEEE Press.

Mouzas, S., & Ford, D. (2002). Managing relationships in showery weather: The role of umbrella agreements. *Journal of Business Research*, *59*(12), 1248–1256. doi:10.1016/j.jbusres.2006.10.001

Mouzas, S., & Ford, D. (2012). Leveraging knowledge-based resources: The role of contracts. *Journal of Business Research*, *65*, 153–161. doi:10.1016/j.jbusres.2011.05.015

NISTIR-7298. (2006). *Glossary of key information security terms*. National Institute of Standards and Technology.

Payment Card Industry Security Standards Council. (2010). *PCI quick reference guide to the payment card industry (PCI) data security standard (DSS)*, version 2.0. Retrieved June 2013, from https://www.pcisecuritystandards.org/documents/PCI SSC Quick Reference Guide.pdf.

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance* (1st ed.). New York, NY: Free Press. doi:10.1108/eb039075

Rossebo, J. E. Y., Cadzow, S., & Sijben, P. (2007). eTVRA, a threat, vulnerability and risk assessment method and tool for eEurope. In *Proceedings of the 2nd International Conference on Availability*, Reliability and Security (pp. 467-471). IEEE Press.

Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. In Advances in information security: Vol. 39. Insider attack and cyber security (pp. 69–90). Springer Press.

Sarbanes, P. S., & Oxley, M. (2002). *U.S. public law 107-204*. 30 July 2002.

Siegrist, M., Gutscher, H., & Earle, T. (2005). Perception of risk: The influence of general trust, and general confidence. *Journal of Risk Research*, *8*(2), 145–156. doi:10.1080/1366987032000105315

Smith, K. T. (2012). Mitigating risks associated with transitive trust in service-based identity propagation. *Information Security Journal: A Global Perspective, 21*(2), 71-78.

Solhaug, B., Elgesem, D., & Stolen, K. (2007). Why trust is not proportional to risk. In *Proceedings of the The Second International Conference on Availability, Reliability and Security (ARES'07)* (pp. 11–18). IEEE Press.

Spitzner, L. (2003). Honeypots: Catching the insider threat. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC'03)* (pp. 170–179). IEEE Press.

Starr, R., Newfrock, J, & Delurey, M. (2003). Enterprise resilience: Managing risk in the networked economy. *Strategy+Business, 2003*(30), 1-10.

Steen, M. W. A., Akehurst, D. H., ter Doest, H. W. L., & Lankhorst, M. M. (2004). Supporting viewpoint-oriented enterprise architecture. In *Proceedings of the Eighth International Enterprise Distributed Object Computing Conference (EDOC'2004)* (pp. 201-211). IEEE Press.

Sutton, S. G. (2006). Extended-enterprise systems' impact on enterprise risk management. *Journal of Enterprise Information Management*, *19*(1), 97–114. doi:10.1108/17410390610636904

The Open Group. (n.d.). *ArchiMate.* Retrieved from http://www.opengroup.org/subjectareas/enterprise/archimate

Thoben, K. D., & Jagdev, H. S. (2001). Typological issues in enterprise networks. *Production Planning and Control*, *12*(5), 421–436. doi:10.1080/09537280110042666

Thorgren, S., Wincent, J., & Örtqvist, D. (2009). Designing interorganizational networks for innovation: An empirical examination of network configuration, formation and governance. *Journal of Engineering and Technology Management*, *26*, 148–166. doi:10.1016/j.jengtecman.2009.06.006

Valentine, J. A. (2010). Compliance complacency: How 'check-box' compliancy remains a pitfall for many organizations worldwide. *Information Security Technical Report*, *15*(4), 154–159. doi:10.1016/j.istr.2011.02.002

van Cleeff, A., & Wieringa, R. J. (2009). Rethinking de-perimeterisation: Problem analysis and solutions. In *Proc. of the IADIS Int. Conf.* [IADIS press.]. *Information Systems*, *2009*, 105–112.

Verizon (2012). *2012 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

Wang, G., & Wu, J. (2011). Multi-dimensional evidence-based trust management with multi-trusted paths. *Future Generation Computer Systems*, *27*, 529–538. doi:10.1016/j.future.2010.04.015

Weiland, R. M., Moore, A. P., Cappelli, D. M., Trzeciak, R. F., & Spooner, D. (2010). *Spotlight on: Insider threat from trusted business partners*. Carnegie Mellon University: Software Engineering Institute. Retrieved from http://www.cert.org/archive/pdf/TrustedBusinessPartners0210.pdf

Wiendahl, H.-P., & Lutz, S. (2002). Production in networks. *CIRP Annals - Manufacturing Technology, 51*(2), 573–586.

Wieringa, R., Pijpers, V., Bodenstaff, L., & Gordijn, J. (2008). Value-driven coordination process design using physical delivery models. In *Proc. of the 27th Int. Conference on Conceptual Modeling* (pp. 216–231). LNCS, Springer Verlag.

Windley, P. J. (2005). *Digital identity* (1st ed.). Sebastopol, CA: O'Reilly Media, Inc.

APPENDIX

Table 7 contains the output of step 6 of our method.

Table 7. Output of step 6, i.e., security requirements to counter external insider threat via reverse-engineering of the PCI DSS (Payment Card Industry Security Standards Council, 2010).

Security Goal	Adapted from PCI DSS best practice requirements	External Insiders as threats	External Insiders as security enforcers
Protect sensitive data in motion	Firewalls should be installed and maintained to filter traffic of sensitive data; this involves management of inbound & outbound traffic of network firewalls, personal firewalls, and virtual machines firewalls (e.g., when the data center uses a shared hosting environment)	Unmanaged firewalls at one or more of the parties involved (i.e. retailer, call center, logistics, EDI-managed provider and data center) at the level of network, desktop or virtual machine are a source of threat	Infrastructure-responsible employees at data center and at each party should be hold accountable for configuring and managing such firewalls
	Encrypt transmission of sensitive data traveling over open, public networks.	Use of communication channels such as unencrypted email, peer-to-peer or wireless connections for intentional or unintentional transmission of sensitive data	Infrastructure-responsible employees at each party need to restrict the availability of unsafe connections, e.g. for sales desk employees
	Logs should be collected and analyzed not only at the OS and network levels but also at the level of application, anti-virus, database; analysis may involve correlation of information from different logs	Logs collected but not managed is a common practice; logs not analysed at different parties cause threat of undetected unauthorised access and misuse of sensitive data	Infrastructure- and application-responsible employees at the data center and infrastructure-responsible employees at each other party should be held responsible for that
Protect sensitive data at rest	Sensitive data should be stored in an unreadable way, i.e. encrypted and decryption keys should be locked in a safe, not logically nearby location	Certificates for EDI transmission and decryption keys stored at the retailer, call center and logistics organisations could be source of threat; passwords to sales portal and VPN kept unsafe by employees involved in their manipulation at every party including by the data center employees is also source of threat	Strict policies should be enforced at each party; external insider responsible should be appointed at contracted parties
	Up-to-date anti-virus should be present and regularly updated not only on client desktops but also on servers hosting applications	Anti-virus are usually installed at users desktops/laptops but often not installed at servers for performance reasons; threat may come from every party involved	Infrastructure-responsible employees at data center and at each party need to manage it
	Vulnerability patches and software updates should be managed	Vulnerable desktops used by retailer, call center, logistics & EDI-managed employees can be source of malware that exposes sensitive data; EDI system is a special threat because legacy systems are known to be difficult to patch	Infrastructure-responsible employees at data center and at each party need to manage it

continued on following page

Table 7. Continued

Security Goal	Adapted from PCI DSS best practice requirements	External Insiders as threats	External Insiders as security enforcers
Protect sensitive data in use	Vendor-supplied defaults for system passwords and other security parameters should be changed; such passwords and security parameters span across the infrastructure level and the business application level	Weak passwords are a source of threat from data center employees, retailer, call center, logistics and EDI-managed employees	Strict policies should be enforced at each party; external insider responsible should be appointed at contracted parties. Peer review could help to make sure infrastructure- and applications-responsible employees at the data center enforce it
	Individuals should only have the authorisations they need to perform their duties (need-to-know security principle)	A same sales desk employee handling the same tasks for different customers, and separation-of-duty conflicts between tasks handled by a same employee, e.g. retailer employee that places purchase orders and approves payment of invoices represent threats	Requires enforcement & periodic review of access control policies including separation of duties policies; measures to restrict information sharing
	Every individual should be hold accountable to her actions; this means that actions should be traceable	The use of functional logins (same user ID) or shared password (same password for different ID) often happens in practice; retailer, logistics and call center employees may cause this threat	Requires supervision and review of access control lists; external insider responsible should be appointed at contracted parties
	Physical access to sensitive data should be restricted; this also involves protecting distribution of data, e.g., via email, hardcopy, portable devices	Retailer and logistics employees that handle EDI-based documents and call center employees that handle customer-specific data often print and archive information, and this is a source of threat; vendor support employees with physical access to hardware parts are also threats	Requires supervision at each party; external insider responsible should be appointed at contracted parties
	A policy that addresses information security, security awareness and training should be enforced, as well as strict selection and recruitment procedures	Poor security culture among employees, low level of security training, deficient screening practices; employees from retailer, call center and logistics are potential source of threat	Requires auditing at each party
Protect sensitive data disposed	Data disposed should be rendered unusable, unreadable or undecipherable; this involves physical or electronic data that should either be destroyed or disposed encrypted	Retailer, logistics and call center employees may dispose hardcopy of sensitive data; vendor support employees that replaces hardware parts are also a source of threat	Requires supervision at each party; external insider responsible should be appointed at contracted parties