Value-driven Security Agreements in Extended Enterprises

Virginia N. L. Franqueira*, Roel Wieringa
University of Twente
Enschede, The Netherlands
Email: {franqueirav, r.j.wieringa}@ewi.utwente.nl

***Abstract*—Today organizations are highly interconnected in business networks called *extended enterprises*. This is mostly facilitated by outsourcing and by new economic models based on pay-as-you-go billing; all supported by IT-as-a-service. Although outsourcing has been around for some time, what is now new is the fact that organizations are increasingly outsourcing critical business processes, engaging on complex service bundles, and moving infrastructure and their management to the custody of third parties. Although this gives competitive advantage by reducing cost and increasing flexibility, it increases security risks by eroding security perimeters that used to separate insiders with security privileges from outsiders without security privileges. The classical security distinction between insiders and outsiders is supplemented with a third category of threat agents, namely external insiders, who are *not* subject to the internal control of an organization but yet have some access privileges to its resources that normal outsiders do not have. Protection against external insiders requires security agreements between organizations in an extended enterprise. Currently, there is no practical method that allows security officers to specify such requirements. In this paper we provide a method for modeling an extended enterprise architecture, identifying external insider roles, and for specifying security requirements that mitigate security threats posed by these roles. We illustrate our method with a realistic example.**

***Keywords*-Extended Enterprise Architecture, Governance, Security Agreement, External Insider Threat, Value Modeling.**

I. Introduction

Today, organizations are highly interconnected with other organizations, creating business networks variously called value constellations, value webs, value chains or *extended enterprises*. This is mostly facilitated by outsourcing activities that used to be performed in-house, by new economic models based on pay-as-you-go billing and IT-as-a-service, by new technologies such as virtualization, and by fast and reliable communication over the Internet. Although outsourcing has been around for a couple of decades, what is now new is the fact that organizations are increasingly outsourcing critical business processes, engaging on complex service bundles, and moving infrastructure to other private, shared or even public networks under the custody of third-parties. Extended enterprises provide competitive advantage by allowing cost savings and increasing business flexibility; each participant in an extended enterprise specializes on its core competencies and takes advantage of other organizations' specialities to deliver its business mission.

However, as observed by the Open Group's Jericho Forum,[1] extended enterprises erode organizational boundaries and therefore security perimeters. Data storage, management and processing migrates to the custody of other organizations in the extended enterprise, but the organization that owns the data remains accountable for its protection, regardless of where and by whom it is handled. This creates a governance problem, that we will call the *external insider threat problem.*

In a single enterprise, people either are insiders, who have an employment contract with the organization and accordingly have some privileged access to the organization's resources, or they are outsiders without such privileged access. Insiders are trusted and have access permissions, but also fall under the internal control of the organization in which the proper exercise of these permissions is verified, for example by monitoring behavior and by log analysis; outsiders are not trusted and have no access permissions, and they do not fall under the internal control of the organization. Organizations protect themselves against outsiders by erecting a so called security perimeter, based on firewalls, and by using security mechanisms such as Intrusion Detection Systems and Vulnerability Scanners.

If an organization is embedded in an extended enterprise, as most organizations nowadays are, they must deal with a third category of people, that we call external insiders [1], who are not employed by the organization and do not fall under the internal control of the organization, but nevertheless have some privileges just like insiders. Examples are employees of business partners, and outsourcing service providers. Classical internal control is not possible here, because these employees work with IT that is monitored or logged by another organization, and classical protection against outsiders is not sufficient, because external insiders have legal access privileges.

The solution is to specify *security agreements* with other companies in an extended enterprise in which particular security risk mitigation measures are demanded from the other party. For example, ISO 27002 requires specification of security agreements [2]. However, there currently is

*Supported by the research program Sentinels (www.sentinels.nl).

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

no method for identifying the security requirements to be included in such agreements. For several reasons, identifying such requirements is complex. First, modern companies may deal with hundreds of other organizations, and the complete extended enterprise in which the company operates is simply too complex to model. Not only is it too complex, information about which companies are part of the extended enterprise is hard to find. So a method to identify security agreements must not rely on a model of the entire extended enterprise.

Second, if we restrict our extended enterprise model to the few companies involved in providing a particular business service, we must deal with the problem of finite budgets: Any company has only a finite security budget and therefore only some of the necessary security mitigations can be taken. If a company requires another company that it does business with to take a security measure, then that company will raise the price of whatever it is providing, which negates the major reason to participate in an extended enterprise: reducing cost. But if a company does not require the other company to take a security measure, then it will simply have to *trust* that company. This increases the security risks in transactions with that company if some employees in that companies turn out not to be trustworthy after all, and in addition it may be a source of non-compliance with governance regulations such as the Sarbanes-Oxley Act. Security risk and non-compliance are also costs. Therefore, a method for specifying security agreements in extended enterprises must be a method for supporting negotiations in which a company can trade off the cost of specifying a security requirement against the cost of trusting another company.

Third, the method must be usable by security officers against acceptable effort, which in the current cost-aware climate means that it must be easy to use. The solution that we propose in this paper relies on a multiperspective architecture model of the extended enterprise.

We will achieve complexity reduction by using value modeling to zoom in on the part of the network needed to satisfy a particular customer need (Section II). Using the value approach, we have made a catalog of common relationships between companies in extended enterprises of manufacturing companies (Section III). These relationships are our first step in identifying different kinds of external insiders. We then illustrate our method by analyzing one of these roles in detail, namely the manufacturer-retailer relationship (Section IV). Basically, we model an extended enterprise from a value perspective, coordination perspective and IT architecture perspective, and use this to identify external insiders, sensitive data, and confidentiality threats posed by this. We then show how to mitigate these risks by including mitigation requirements in a security agreement, and which role external insiders play in posing the threats as well as in implementing the mitigations.

II. Value Modeling of Extended Enterprises

In this paper we take the point of view of one company in an extended enterprise, which we will call the *focal company.* To avoid having to model an entire extended enterprise, we focus on a particular *need* of a customer of the focal company, and we make a high-level architecture model of only the companies that cooperate with the focal company to serve that need. This typically reduces the size of the network from a few hundred companies to only a handful.

We use value modeling to represent the part of the extended enterprise required to serve this need, using e3value [3]. An e3value model allows us to show how a customer need is served by the cooperation of a number of companies, and also includes the customer in the model. In this section we summarize the e3value modeling technique. Figure 1 shows a value model of a simplified manufacturer-retailer relationship.

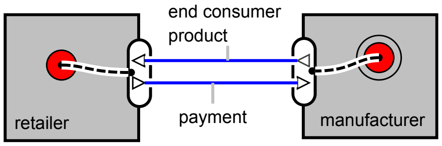

Figure 1. Value model of a simplified manufacturer-retailer relationship

Manufacturer and retailer are actors, i.e. stakeholders with an economic role. Actors have value interfaces represented by the bean-like shape which contain in and out ports (triangles) indicating the direction that a value object is transferred from one actor to another. Value objects can be anything with value for the stakeholders involved such as money-related objects, deliverables, or more intangible objects such as legal compliance. In the figure, the manufacturer transfers end-consumer product in exchange for payment transferred back by the retailer.

Value models should also contain at least one start-stimulus (filled circle) and one end-stimulus (filled circle with a halo). In the example, retailers have a need (start-stimulus) to be fulfilled by another actor in the model: manufactures. However, this is only accomplished if the stimulus is connected through a dependency path (dotted line) to an actor's value interface. Sometimes it may be important to show on a value model that an actor is a broker-like actor; it means that its strength is to transfer value objects between other actors via a dependency path. Dependency paths can also contain "and" (a line with dots) and "or" (a triangle with dots) constructs to represent choice or joint connections, as we will see later.

The underlying principle behind a value model is *reciprocity*, that sustains the delivery of each actor mission. As shown in Figure 1, on the one hand, the manufacturer will only deliver end-consumer products upon an agreement of payment via an invoice to the retailer. On the other hand, the retailer will only pay (the invoice) if the end-consumer products specified on its purchase order have been delivered accordingly. This reciprocity is more visible between profitable driven actors, and less visible when it involves governmental actors, for example.

III. Business Roles in Extended Enterprises

Although our method is claimed to be general, we will consider only the case where the focal company is a manufacturing company. Analysis of a number of existing manufacturing extended enterprises has revealed a small number of frequently occurring roles of companies. This is our entry point for identifying external insiders who play a role in this part of the extended enterprise. In this section we list these roles, and as an illustration provide an e3value model for one of them.

A. *Trading Partners*

Trading partners are organizations the manufacturer trades with to perform the value-adding primary activities of its value chain, in Michael Porter's terminology [4]. One characteristic of such partners is the exchange of business transactions via Electronic Data Interchange (EDI) [5]. EDI are formatted messages that represent documents necessary to coordinate trading between two parties. We will see some examples of EDI documents when we model our running example, the manufacturer-retail relationship in Section IV.

The value model in Figure 2 shows three types of manufacturer trading partners, described next. These are broad views of the value relationships; we will see in Section IV, for example, that the relationship manufacturer-retailer in fact involves many other organizations and also directly involves another type of trading partner (i.e. warehouse & carrier) to realize the relationship seen in this model.

1) **Customers**
   Customers are organizations that buy products from the manufacturer. They can basically be of two types:
   a) *Retailers (or dealers)* are organizations that act as a broker in the sense that they buy from the manufacturer for resale. The relationships between manufacturer and retailer, and between retailer and end consumer are explicit in the value model in terms of the value objects "end consumer product" and "payment".
   b) *Professional customers* are organizations that buy from the manufacturer for the benefit of its own end consumers. For example, a car manufacturer can trade with car dealers that resell family cars to end consumers, but can also trade utility vehicles, such as ambulances, with healthcare institutions. In the value model shown in Figure 2, we make the distinction between these two classes in terms of the value objects they buy, i.e., "end consumer product" and "professional product".
2) **Suppliers**
   Suppliers are organizations that provide the manufacturer with bill-of-material[2] goods. Therefore, in this case the manufacturer is the buyer while suppliers are the sellers. In the value model shown in Figure 2, we see that the payment flows from manufacturer to supplier in exchange for bill-of-material goods.
3) **Warehouse and carriers**
   Warehouse and carriers are the main components of logistics, in this case, outbound logistics [4]. The commercial relationship between manufacturer and warehouse & carrier is explicit in the value model shown in Figure 2. The manufacturer pays in exchange for storage and transport of its products.

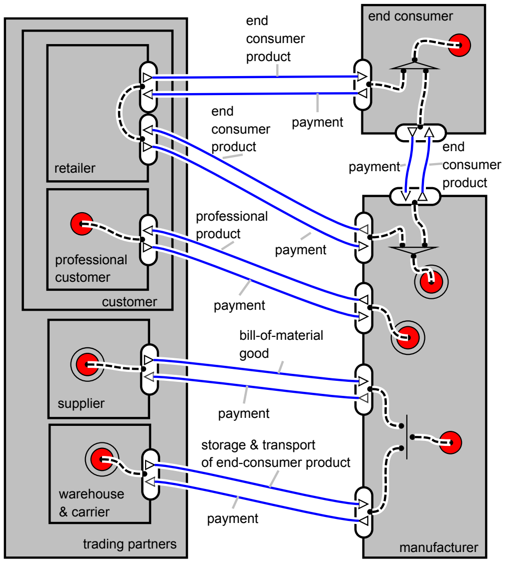

Figure 2. Typical trading partners of a manufacturer

The trading partners value model also shows that end consumers and professional customers have start-stimuli, i.e., they have consumption needs. End consumers, as represented, can choose from alternative paths, either buy at retailers or buy directly from the manufacturer web store, for example. Retailers play the role of brokers, and suppliers and logistics fulfill the customer needs of the manufacturer itself.

B. *Service Providers*

Part of a manufacturer extended enterprise are service providers; in this case the manufacturer is mainly a services client. However, a manufacturer can also play the role of service provider. For example, Xerox[3], a manufacturer of copiers, printers, and supplies such as toner cartridges and

[2] Products essential for building the products sold by the manufacturer.
[3] http://www.xerox.com

paper, provides a number of business services to organizational clients such as enterprise print services and document management services.

There are two main types of service providers: business process providers and support service providers. Although it may seem this distinction relates to Porter's distinction between primary and support activities in a value chain [4], such relation does not exist. A business process can be related either to a primary activity (e.g., sales) or to a support activity (e.g. human resource management).

Regardless of the service provider type, in all cases the value exchange between service provider and client is the same: payment is transferred from client to provider in exchange for service, transferred from provider to client.

1) **Business process providers**
   Business process providers deliver an entire business process, i.e., a series of related tasks with a specific purpose delivered as a service. Business processes can be related to front-office or to back-office processes. The former are processes externally visible either to the outside world or to the extended enterprise; examples are call centers, and recruitment & selection services. On the contrary, back-office processes are not visible externally; examples are accounting, finance and salary administration.
2) **Support service providers**
   These service providers deliver services that support business processes, or involve facilities and infrastructure. These services can be related to Information Technology (IT) or not. Examples of *IT support services* are network management, data center operations, and software maintenance. While examples of *non-IT support services* are cleaning, catering, physical security, telephone/water/power supply.

C. Business Partners

Another class of B2B relationship that happens on the extended enterprise of a typical manufacturer refers to business partners. We identify basically two types of business partners, described next.

1) **Co-development partners**
   This type of business partner relationship appears when a product is manufactured; this includes software development organizations that *manufacture* software-products. In this case, the partner receives a payment in exchange for a design or specification. Most of the times, customers and consumers of the manufacturer products do not become aware of such partnerships.
2) **Business complementary partners**
   This type of business partner relationship complements each others' products to deliver a combined solution or product to customers and consumers. A typical example is the more apparent partnership between hardware manufacturers and software developers to deliver, for example, laptops and desktops with operating system already installed and licensed.

D. Administration

A manufacturer extended enterprise also comprehends a class of B2B relationship that we call generically "administration". We identify three types of business-to-administration relationships:

1) **External auditors**
   External auditors fulfil a customer need from a manufacturer; the value objects they exchange are auditor statement for payment. A SAS 70 (Types 1 and 2, for Service Organizations) [6][4] statement issued by independent auditors is an example.
2) **Regulatory bodies**
   Regulatory bodies also fulfil a customer need from a manufacturer; they issue certifications of legal compliance in exchange for payment. For example, manufacturers are only able to trade their products in the European market if their products have a CE marking. Depending whether these products are of high risk for public safety, then they have to be assessed by a Notified Body. As such, certain medical devices need to be assessed by notified inspection bodies against the Council Directive 93/42/EEC [7] before they can receive a CE marking.
3) **Government agencies**
   Manufacturers have to comply with local and federal governmental agencies needs in exchange for legal compliance. For example, manufacturers have to pay taxes such as VAT (Value-Added Tax), and have to provide data (e.g., statistics and reports) to agencies such as the Bureau of Economic Analysis (U.S. Department of Commerce[5]) used for governmental statistics [8].

E. Competitors

Competitors represent the last class of B2B relationships identified from the perspective of a manufacturer. In this case, customers such as retailers and professional customers as well as end consumers have the choice of buying from the manufacturer or its competitors to fulfil the same customer needs.

IV. A Method for Identifying External Insider Threat Mitigations

A security agreement between the focal company and some other company consists of a specification of security risk mitigations to be taken by the other company. This

[4] SAS 70 [6] 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.

[5] http://www.bea.gov/

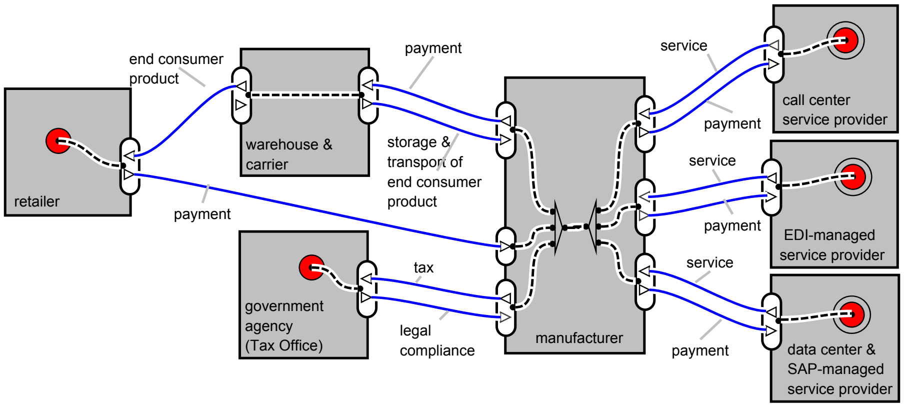
end consumer product
payment
service
payment
call center service provider
retailer
warehouse & carrier
storage & transport of end consumer product
payment
service
payment
EDI-managed service provider
government agency (Tax Office)
tax
legal compliance
manufacturer
service
payment
data center & SAP-managed service provider

Figure 3. Model showing the value exchanges among parties

mitigation specification is a requirement; the security agreement states that the other company must comply with this requirement.

In order to identify mitigations of risks posed by external insiders, we first need to identify these external insiders. In the method proposed here, we do this by first making a value model of the part of the extended enterprise that cooperates to serve a particular customer need of the focal company. This reduces the network to a manageable size, and also shows between which pairs of companies a security agreement may be needed. Next, we make a model of coordination activities needed to serve the need, and of the IT architecture required to support these activities. This allows us to identify external insiders in this part of the network, the activities that they legitimately must perform in order to do their job, and the sensitive data they have access to. This also allows us to provide a list of threats posed by these external insiders, and of mitigations of these threats. We illustrate our method with the manufacturer-retailer business relationship presented in Section II, where we incorporate the additional roles that we have identified so that we get a realistic model.

A. *Value Modeling*

Figure 3 shows the value model of a manufacturer-retailer relation where five other actors (organizations) are involved. We see (i) two trading partners of the manufacturer (the retailer itself and the logistics partner), (ii) three service providers of the manufacturer (the call center business process provider and two IT support service providers), and (iii) one administration organization (the Tax Office).

The retailer transfers a payment to the manufacturer in exchange for the products ordered. However, the delivery of these products happens via a logistics partner (warehouse & carrier) of the manufacturer. Therefore, the manufacturer transfers a payment to the warehouse/carrier in exchange for storage & transport of products. The manufacturer has to collect taxes when selling products and, as a consequence, the manufacturer has to transfer taxes to the Tax Office in exchange for legal compliance. Moreover, the manufacturer transfers payments to service providers in exchange for different types of services. Hence, the model shows exchanges of payment by service between the manufacturer and the call center, the EDI-managed and the data center & SAP-managed service providers.

Although the value model provides an overview of B2B relationships that play an important role in realizing the main business interaction between manufacturer and retailer, it does not provide an overview of sequencing that those parties have to follow. That is why we also need to model the coordination perspective; we do that next.

B. *Coordination Modeling*

As already mentioned when trading partners were discussed in Section III-A, EDI (Electronic Data Interchange) documents are the basis upon which trading partners cooperate, therefore coordinate, their operations. Coordination between different parties of the value chain is a key aspect for the order process fulfilment [9]. Figure 4 shows the main coordinated interactions between the trading parties involved in a simple sequence diagram. We omitted the activities of the three service providers since there is no coordination involving those parties.

The whole process starts when a retailer issues an EDI-based Purchase Order (PO) to the manufacturer (step 1 in Figure 4). 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 (step 2). In general terms, it is an indication for the warehouse to get ready to release the products listed on the PO from stock. This 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 (step 3) to the carrier. This document alerts the carrier to be ready to transport the products to the retailer, again triggering

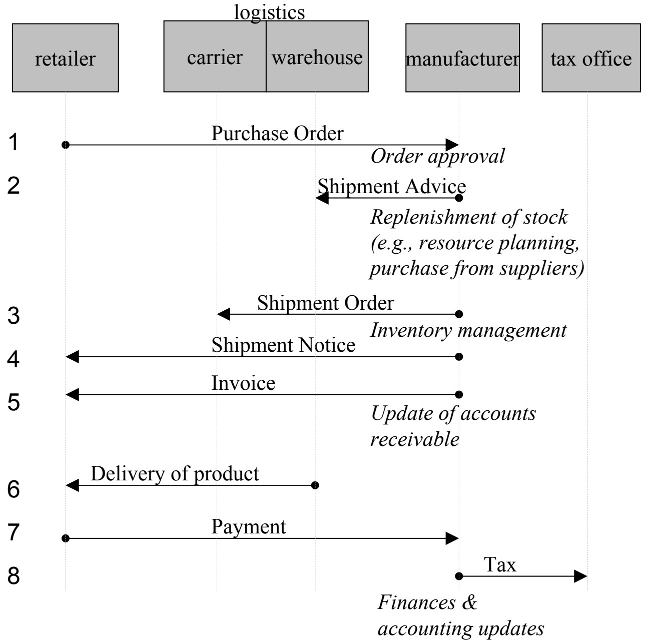

Figure 4. Model showing the main coordination activities among the trading parties.

activities related to the manufacturer inventory management. Inventory may aggregate, for example, stock information from more than one warehouse, and from the final stage of production. Next, the manufacturer usually sends an EDI-based Shipment Notice to the retailer with details related to the delivery of the products (step 4), followed by an EDI-based invoice (step 5). The invoice triggers the update of accounts receivable on the manufacturer side. The next two steps involve the delivery of products at the retailer address (step 6) executed by the carrier that transports these products from the warehouse to the retailer, and the actual payment of the products received to the manufacturer (step 7). The last step (step 8) refers to the payment of taxes to the Tax Office, performed by the manufacturer, and triggers finance and accounting back-office activities for the manufacturer.

The coordination model shows the main sequence of interactions between the trading partners and the manufacturer. However, several back-office activities are triggered on the manufacturer side that are still not visible on the coordination model. Also, in order to assess external insider threat, we need to know which IT resources are involved in these activities. Therefore, in the following section we model the IT architecture that supports this coordination including the activities triggered.

C. IT Architecture Modeling

Figure 5 shows an IT architecture that realizes both the value and the coordination models presented previously. Any architecture notation understandable by the stakeholders is acceptable here. The diagram in figure 5 essentially shows different parties (organizational boundaries), communication channels linking these parties, and user functionalities.

One interesting aspect to notice is the fact that the trading partners and service providers present on the value model (Figure 3) are also part of the IT architecture diagram, but not the manufacturer itself. This is because the front- and back-office activities mentioned on the coordination model (Figure 4) are performed by IT support service providers and by a business process provider on the behalf of the manufacturer.

As seen before, the starting point is a Purchase Order (PO). Retailer employees can place PO in two ways. They can use the manufacturer sales portal, not only to place but also to manage their orders. Alternatively, they can use the manufacturer call center and ask a sales desk employee to place and manage their orders; in this case, the retailer employees have to manage their orders through the call center. The EDI-based documents, such as a PO, are usually transmitted via AS2 (Applicability Statement 2). 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 [10] from both parties involved and use encryption for data transmission. The PO transmitted by the retailer or the sales desk employee is therefore sent via AS2 connection to the EDI system located on the manufacturer data center. The EDI system basically processes the EDI files, that has to be integrated with the manufacturer ERP (Enterprise Resource Planning) infrastructure. In this example, we assume (quite reasonably) that the manufacturer has a SAP ERP[6]. The integration between EDI system and SAP ERP requires an interface based on SAP IDoc (Intermediate Document) technology; via this IDocs interface documents are transferred from EDI system to ERP systems and vice-versa.

After the 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 3. For example, employees from the logistics partner, i.e. the warehouse and carrier employees, will have an EDI interface to access their EDI system (logistics EDI system) used to manage shipping advices and shipping orders, respectively. The activities triggered at each step of the whole process are performed by different business applications part of the manufacturer ERP infrastructure. For example, step 5 in Figure 3 involves SAP Financials to issue the invoice and send the EDI-based invoice automatically to the retailer, and to update the receivable accounts.

The manufacturer's legacy EDI system (located on its data center) is managed remotely by a service provider, as often happens in practice and illustrated in the diagram in Figure 5. Therefore, their employees basically perform tasks related

[6] http://www.sap.com/solutions/business-suite/erp

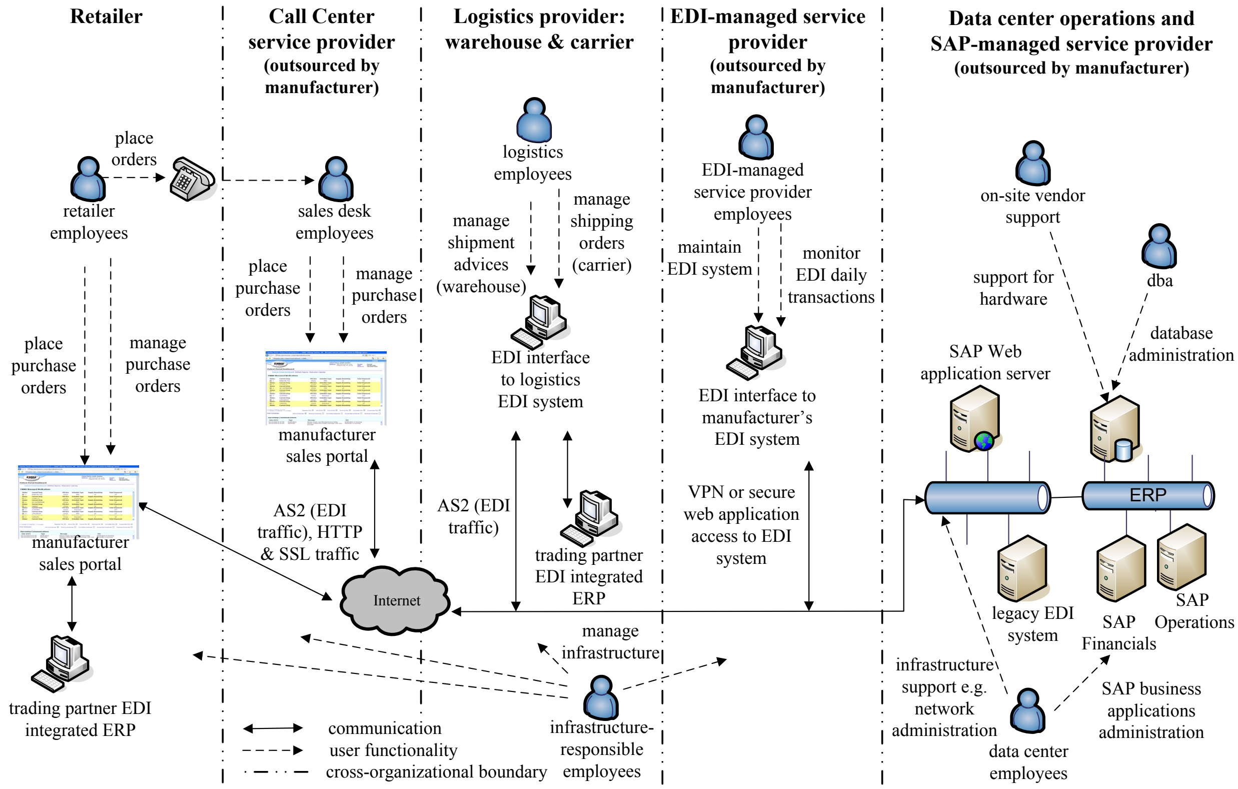
Retailer
Call Center service provider (outsourced by manufacturer)
Logistics provider: warehouse & carrier
EDI-managed service provider (outsourced by manufacturer)
Data center operations and SAP-managed service provider (outsourced by manufacturer)
place orders
retailer employees
sales desk employees
place purchase orders
manage purchase orders
place purchase orders
manage purchase orders
manufacturer sales portal
manufacturer sales portal
trading partner EDI integrated ERP
AS2 (EDI traffic), HTTP & SSL traffic
Internet
logistics employees
manage shipment advices (warehouse)
manage shipping orders (carrier)
EDI interface to logistics EDI system
AS2 (EDI traffic)
trading partner EDI integrated ERP
manage infrastructure
infrastructure-responsible employees
EDI-managed service provider employees
maintain EDI system
monitor EDI daily transactions
EDI interface to manufacturer's EDI system
VPN or secure web application access to EDI system
on-site vendor support
support for hardware
dba
database administration
SAP Web application server
ERP
legacy EDI system
SAP Financials
SAP Operations
infrastructure support e.g. network administration
data center employees
SAP business applications administration
communication
user functionality
cross-organizational boundary

Figure 5. Model showing an IT architecture that realizes the value and the coordination models presented in Figures 3 and 4, respectively

to: (i) maintenance of the EDI system and (ii) monitoring of EDI daily transactions. EDI maintenance involves tasks related to disaster recovery such as archive of EDI data and backup of EDI software; while EDI daily monitoring involves tracking EDI error messages and repair or resume transmission [11]. The manufacturer's 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 assumed to be managed, in this example, by a same service provider. We identify in the diagram a *few* actors that play a role on the tasks that such provider has to perform. For example, we identify data center employees responsible for network administration, and SAP experts responsible for monitoring daily SAP operations; we also identify the role of dba (database administrator). Additionally, it becomes clear when we think about on-site vendor support for hardware that the data center operations service provider also has its own extended enterprise.

D. *Identifying External Insiders*

All the actors in the IT architecture diagram are *external insiders* with respect to the focal company, the manufacturer. The diagram also illustrates why external insiders can be a security problem: For example, the manufacturer cannot know whether call center employees who have left their job have had their digital identity and access revoked or not, and how quickly. This represents a threat because a detected incident can bring consequences not only for the service provider in terms of liability but can also bring consequences to the service client organization. An illustration is the Citibank fraud revealed in 2005 [12]. Investigation showed that Citibank account holders were affected when their money were transferred by three former employees of its call center provider, raising questions not only about identity and access management, but also about the rate of turnover and screening procedures at outsourced call center providers.

Our IT architecture model provides a list of external insiders in the manufacturer-retailer example.

1) retailer employees that place and manage purchase orders
2) sales desk employees that also place and manage purchase orders on the behalf of the manufacturer's customers
3) logistics employees that manage shipment advices and manage shipping orders sent by the manufacturer for coordination involved with the delivery of products for the retailer
4) EDI-managed service provider employees that maintain the manufacturer EDI system, and monitor EDI daily transactions
5) infrastructure-responsible employees at the retailer, call center, logistics, and EDI-managed service provider

6) data center employees that perform basically two roles: network administration and SAP business applications administration
7) database administrators also from the data center
8) on-site vendor support individuals that manage data center specific hardware

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 be in a position to enforce mitigations on the behalf of the manufacturer. This happens when the activity they perform has been outsourced. We look at threats and mitigations next.

E. Specifying Threat Mitigations

What threats do these external insiders pose? The main security attribute at risk is confidentiality. Therefore, we take a data-centric approach for the analysis of threats and mitigations, and classify the threats according to the data states recognized by the Health Insurance Portability and Accountability Act (HIPAA) [13], that applies to organizations handling health data. According to HIPAA, there are the four data states: (i) data in motion, i.e. data in transit through a network, (ii) data at rest, i.e. data stored, (iii) data in use, i.e. data in process of being created, retrieved, updated or deleted, and (iv) data disposed, i.e. data discarded or recycled. Protecting sensitive data in each of these states becomes security goals, and this is our starting point for identifying threats.

Next, we identify sensitive data using the IT architecture shown in Figure 5. Sensitive data, in this particular example, includes:

- customer-specific price lists for manufacturer products,
- trading EDI-based documents,
- customer personal data, and
- credentials such as certificates to transmit EDI documents,
- decryption keys,
- passwords to log on the sales manufacturer portal, and
- administrative passwords to manage infrastructure and business applications (e.g. ERP environment, database, legacy EDI system) at the data center.

In order to identify realistic mitigations (using technology currently in use by companies) we follow a backward reasoning from best practice mitigations to threats that they can mitigate. Our starting point here is the Payment Card Industry Data Security Standard (PCI DSS) [14] (also a data-centric standard), which we apply to sensitive data rather than to credit card holders data. Each PCI requirement is a possible mitigation to be included in a security agreement, and we analyze whether external insiders listed in the previous section would pose threat, and would be responsible to mitigate that threat. The results are shown in Table I. We support this analysis by recent investigations on cases of data breaches reported by 7Safe (2010) [15] and Verizon (2009) [16].

The outcome of Table I is twofold. First, it provides mitigations against external insider threat, useful for addressing security in third party agreements, as mandated by ISO 27002 [2]. Second, it lists not only the external insiders who pose threats, but also the external insiders that must implement mitigations. This provides additional support for negotiating about inclusion of mitigation measures in security agreements.

V. Related Work

The three perspectives (value, coordination, IT architecture) used in this paper to identify classes of external insiders has been proposed by Gordijn and Akkermans [3] and Wieringa et. al [17]. We have no particular choice of coordination and IT architecture modeling techniques and assume that companies using this method have their own preferred modeling techniques.

The need for security agreements in extended enterprises is a best practice listed in the ISO 27002 [2] code of practice for information security management (Section 6). However, ISO 27002 does not provide guidelines for doing so, and this paper is the first to provide such a method. An important difference between our approach and ISO 27002, though, is that we focus on threats rather than risks because in extended enterprises it is difficult to get information to assess risks, because it involves prior knowledge of existing vulnerabilities.

Enterprise governance frameworks are also related to our work. For example, the Control Objectives for Information and related Technology (COBIT) [18] contains controls for IT management. It contains a process under the domain of “Delivery and Support” that covers *Manage Third-party Services*, but again it is too broad and aims at monitoring of service delivery, not really on the security aspect. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [19] focus on management in more general terms, and related to financial reporting. Here too our method can be used to satisfy these requirements.

Our work uses data-centric security standards that organizations have to be compliant with, depending on the type of data they handle. The Health Insurance Portability and Accountability Act (HIPAA) [13] and Payment Card Industry Data Security Standard (PCI DSS) [14] are the basis for our security goals and mitigations considered when reasoning about external insiders threats, in Section IV-E.

Our work contributes to the specification of Service Level Agreements (SLAs). However, SLAs address the delivery of services in terms of measurable indicators that guarantee the quality of services (QoS) delivered. While some attributes of security can be specified in an SLA, such as availability of services, others cannot not, such as confidentiality and integrity. Confidentiality requirements must be specified in the form of mitigation measures in security agreements that can be appended to SLAs.

VI. Summary and Further work

We have provided and illustrated a method for modeling an extended enterprise from three perspectives, namely the commercial value, the coordination, and the IT architecture perspective, and to identify external insider threats and mitigations in this network. This provides useful information for security officers who must negotiate security agreements with other companies in an extended enterprise, because it shows the source of threats as well as the sources responsible to mitigate these threats. Use of value modeling allows us to restrict modeling to a manageable small part of the extended enterprise, which is the first requirement of the method listed in section I. Motivating the threats and mitigations in terms of the extended enterprise architecture provides support for making trade-offs between mitigating the threat, increasing the price of cooperation, and trusting the threat not to materialize, increasing the risk of sensitive data disclosure and non-compliance. Finally, our third requirement is ease of use. This is notoriously difficult to validate. E3value modeling has been used mostly by researchers (www.e3value.com), so this is the biggest obstacle to transferring this method to practice. More realistic is the use of this technique by a trained consultant to support a security officer.

In order to validate the method in practice using an action case study approach [20], we will use it to perform insider threat analyses using other scenarios from manufacturing companies. Initial experience with real-world cases has indicated that the usability of the method would be enhanced if support for access path analysis would be provided. Moreover, to generalize the method, we will use it in economic sectors other than manufacturing, for example, in the healthcare domain.

References

[1] V. N. L. Franqueira, A. van Cleeff, P. A. T. van Eck, and R. J. Wieringa, "External Insider Threat: a Real Security Challenge in Enterprise Value Webs," in *Proc. of the Fifth Int. Conf. on Availability, Reliability and Security (ARES'2010).* IEEE Computer Society Press, February 2010, pp. 446–453.

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

[3] J. Gordijn and J. Akkermans, "Value-based requirements engineering: Exploring innovative e-commerce ideas," *Requirements Engineering Journal*, vol. 8, pp. 114–134, 2003.

[4] M. E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance*, 1st ed. New York, NY, USA: Free Press, 1985.

[5] M. A. Emmelhainz, *EDI: Total Management Guide*. New York, NY, USA: John Wiley & Sons, Inc., 1992.

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

[7] "Council Directive 93/42/EEC of 13 June 1993 concerning medical devices," Official Journal of the European Union, directive amended by the Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007.

[8] D. D. Kim, B. M. Lindberg, and J. M. Monaldo, "Annual Industry Accounts, Advance Statistics on GDP by Industry for 2008," Bureau of Economic Analysis (U.S. Department of Commerce, May 2009.

[9] K. L. Croxton, "The Order Fulfillment Process," *The International Journal of Logistics Management*, vol. 14, no. 1, pp. 19–32, 2003.

[10] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley, 2003.

[11] "AS2 Processing for EDI," Online, http://www.dcs-is-edi.com/AS2.html, last visited on March 2010.

[12] J. Ribeiro, "Twelve arrested, including three ex-employees of outsourcing company," Online, April 2005, http://www.computerworld.com/s/article/100900/Indian_call_center_workers_charged_with_Citibank_fraud, last visited on March 2010.

[13] HIPAA, "Health Insurance Portability and Accountability Act, enacted by Senate and House of Representatives of the United States of America," 1996, http://www.legalarchiver.org/hipaa.htm.

[14] Payment Card Industry Security Standards Council, "Payment Card Industry Data Security Standard, version 1.2," October 2008.

[15] S. Bhala, M. Christodoulides, L. Cornwell, R. Jones, and B. Morris, "UK Security Breach Investigation Report - An Analysis of Data Compromise Cases," 7Safe Limited, January 2010, http://7safe.com/breach_report/Breach_report_2010.pdf, Last visited on March 2010.

[16] 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, Last visited on September 2009.

[17] R. Wieringa, V. Pijpers, L. Bodenstaff, and J. Gordijn, "Value-driven coordination process design using physical delivery models," in *Proc. of the 27th Int. Conference on Conceptual Modeling*, ser. LNCS. Springer Verlag, 2008, pp. 216–231.

[18] IT Governance Institute, "CobiT 4.0 - Control Objectives for Information and related Technology," 2005.

[19] COSO, "Internal Control - Integrated Framework by Committee on Sponsoring Organizations of the Treadway Commission," 1994.

[20] R. J. Wieringa, "Design science as nested problem solving," in *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, Philadelphia*. New York: ACM, 2009, pp. 1–12.

Security Goal	External Insiders that Pose Threat	Mitigation Best Practice	External Insiders that Mitigate Threat
Protect sensitive data in motion	Unmanaged firewalls such as personal firewalls on desktops used by retailer, sales desk and logistics employees are a source of threat	Firewalls should be installed and maintained to filter traffic of sensitive data; this involves management of inbound and outbound traffic of network firewalls, personal firewalls, virtual machines firewalls, when the data center uses a shared hosting environment	Infrastructure-responsible employees at data center and at each party
	Use of communication channels such as unencrypted email, peer-to-peer, and wireless connections for intentional or unintentional transmission of sensitive data such as customer-specific price lists and customer data by sales desk employee are a source of threat	Encrypt transmission of sensitive data across open, public networks	Infrastructure-responsible employees at each party need to restrict the availability of unsafe communication channels, e.g. for sales desk employees
	Logs collected but not managed is a common practice (according to Verizon investigation); logs not analyzed at different parties cause a threat from all parties of undetected unauthorized access and misuse of sensitive data	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	Infrastructure-responsible and applications-responsible employees at data center and infrastructure-responsible employees at each other party
Protect sensitive data at rest	Certificates for EDI transmission and decryption keys are stored at the retailer, call center and logistics organizations could be source of threat; passwords to sales portal and VPN e.g., should not be stored but could be kept unsafe by employees involved in their manipulation at every party including by the data center employees	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	The same external insiders that may cause threat
	Anti-virus are usually installed at users desktops/laptops but often not installed at servers for performance reasons, according to 7Safe investigation; threat comes from every party involved	Up-to-date anti-virus should be present and regularly updated not only on client desktops but also on servers hosting applications	Infrastructure-responsible employees at data center and at each party
	Vulnerable desktops used by retailer, call center, logistics, and EDI-managed employees can represent source of malware that exposes sensitive data; EDI system is a special threat because legacy systems are known to be difficult to patch	Vulnerability patches and software updates should be managed	Infrastructure-responsible employees at data center and at each party
Protect sensitive data in use	Guessable login/passwords are a source of threat from data center employees, retailer, call center, logistics and EDI-managed employees	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	The same external insiders that may cause threat, but specially infrastructure-responsible employees at each party, and applications-responsible employees at data center
	A same employee handling the same tasks for different customers, e.g. sales desk employees; 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	Individuals should only have the authorizations they need to perform their duties (need-to-know security principle)	Requires supervision and review of access control lists; external insider responsible should be appointed at contracted parties
	The use of functional logins (same user ID) or shared password (same password for different ID) often happens in practice, according to Verizon and 7Safe investigations; retailer, logistics and call center employees may cause this threat	Every individual should be hold accountable to her actions; this means that actions should be traceable	Requires supervision and review of access control lists; external insider responsible should be appointed at contracted parties
	Employees that handle EDI-based documents (e.g. retailer and logistics employees) and call center employees that handle customer personal data & customer-specific price list often print and archive information, and this is a source of threats; vendor support employees with physical access to hardware parts are also threats	Physical access to sensitive data should be restricted; this also involves protecting distribution of data, e.g., via email, hardcopy, portable devices	Requires supervision at each party; external insider responsible should be appointed at contracted parties
	Poor security culture among employees, low level of security training, deficient screening practices; retailer, call center and logistics are potential source of threat	A policy that addresses information security, security awareness and training should be enforced, as well as strict selection and recruitment procedures	Requires auditing at each party
Protect sensitive data disposed	Retailer, logistics and call center employees may dispose of hardcopy of sensitive data such as customer-specific price list, customer personal data, trading documents; vendor support employees that replaces hardware parts are also a source of threat	Data disposed should be rendered unusable, unreadable or undecipherable; this involves physical or electronic data that should either be destroyed or disposed encrypted	Requires supervision at each party; external insider responsible should be appointed at contracted parties

Table I

ANALYSIS OF EXTERNAL INSIDERS IN TERMS OF WHO POSES THREATS AND WHO IS RESPONSIBLE FOR ENFORCING MITIGATIONS TO COUNTER THESE THREATS ON THE BEHALF OF THE MANUFACTURER