IT Confidentiality Risk Assessment for an Architecture-Based Approach

Ayşe Morali*, Emmanuele Zambon*, Sandro Etalle* † and Dr. Ir. P.L. (Paul) Overbeek RE‡
*University of Twente
Email: {emmanuele.zambon, ayse.morali, sandro.etalle} (at) utwente.nl
†Eindhoven Technical University
Email: s.etalle (at) tue.nl
‡Partner OIS Information Risk & Security Management
Email: Paul.Overbeek (at) Ois-NL.EU

***Abstract*—Information systems require awareness of risks and a good understanding of vulnerabilities and their exploitations. In this paper, we propose a novel approach for the systematic assessment and analysis of confidentiality risks caused by disclosure of operational and functional information. The approach is based on a model integrating information assets and the IT infrastructure that they rely on for distributed systems. IT infrastructures enable one to analyse risk propagation possibilities and calculate the impact of confidentiality incidents. Furthermore, our approach is a mean to bridge the technical and business-oriented views of information systems, since the importance of information assets, which is leading the technical decisions, is set by the business.**

I. Introduction

The World-Wide Web [4] has fueled the deployment of a plethora of electronic services of increasing complexity, like on-line banking, cross organization interconnections to support supply chains, etcetera. In some countries, health insurance cards are replaced by digital patient IDs.

To exploit these possibilities, organizations have to store valuable confidential information (like patient records, bank account information, credit card details or client profiles) in IT infrastructures that are usually exposed to malicious activities such as hacker attacks via the Internet and insiders misuse, raising the problem of dealing with the risks related to the possible loss of confidential data.

The consequences of confidentiality breaches for an organization range from financial loss, to loss of market shares in the private sector as well as to compromise national security in the public sector. According to McAfee Virtual Criminology Report'2005, information theft is today the most costly form of cybercrime.

To deal with possible losses of confidential data (i.e. unauthorized disclosure), companies follow by now largely standardized risk management (RM) methodologies, like NIST 800-30 [16], AS/NZS4360:2004 [13], OCTAVE [14], COBIT [7], ISO/IEC 27002 [10] (ISO 17799). One of the first basic step of any RM methodology is always the *risk assessment* (RA), which - following the terminology of SP800-30 [16] - is "the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact".

When it comes to the management of confidentiality risks, we argue that the main drawbacks of present mainstream risk assessment and mitigation methodologies is that they do not take the IT architecture of the system under examination. To give an intentionally oversimplified example of how the IT architecture can greatly affect the resistance of the system w.r.t. confidentiality breaches, consider the IT system of a hospital: if its web-server is on the same sub-network of the patient database, then a hacker could work her way to the patient database via the web-server, while if the two systems were not directly interconnected, then this would be much harder. Indeed, the IT architecture determines to a great extent how resilient a structure is to confidentiality breaches and also in case of breaches how much of the information asset it will disclose (the damage is of a different magnitude weather a breach leads to the disclosure of only a few of the stored credit card numbers or all of them).

Since present RM methodologies do not take the architecture directly into account, they completely delegate the issue of distinguishing a solid architecture from a less solid one to the specialist carrying out the RA.

The problem of distinguishing between solid architectures and less solid ones arises also during the *engineering* of a new system that has to deal with confidential information; also in this case there exist no tools able to assess how good an architecture is, given the fact that it should preserve the confidentiality of the data stored in one or more of its subsystems.

In this paper, we introduce the Distributed Confidentiality Risk Assessment (DCRA) Model. By modeling how confidentiality breaches can propagate through an organization, the DCRA-Model can be used as a tool for quantitatively measuring their actual impact (if needed, also in monetary terms).

Also, the DCRA Model can be used to compare different architectures and identify the best one to cope with the

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

confidentiality risks, given the (business-driven) value of the data stored in it.

Furthermore, by including in the DCRA an estimate of the risk the IT infrastructure is exposed to and of their likelihood, we can use it to calculate the global operational risks related to confidentiality an organization is exposed to. The added value of the DCRA is that it can be integrated with other methodologies in order to allow them to consider the underlying IT architecture.

We argue that the DCRA-Model assesses the IT confidentiality risk intrinsically better than other RA methods and allows one to measure how robust the system is to confidentiality risks.

The rest of this paper is structured as follows: In Section II an over view of the related research in the field of IT risk management is given; in Section III the risk management methodologies are provided; in Section IV the framework for modelling information assets is introduced; in Section V the framework for modelling incidents and the formalization of their propagation is introduced; in Section VI two applications examples of the model for telecommunication and research domain are given; in Section VII the feasibility for required information in building the model is argued; in Section IX conclusions and required future work is given.

II. Related work

AS/NZS4360-2004 [13] states that risk management can be applied at many levels within an organization and recommends embedding risk management into operational and strategic planning. IT related risks are classified as: strategic and operational [5].

Operational risk is defined in BASEL-II as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". Compliance with BASEL requires banks to quantify IT related operational risks [11], including legal risk and risks related to business processes of the organization.

Strategic risks are related to the high-level goals of an organization. They may be quantified by setting them equal to loss of market share, which depends on the monetary volume of the market and potential loss of market share in case of a confidentiality breach. Strategic risks are especially important by calculating the impact of confidentiality incidents.

There exist various academic frameworks for carrying out risk assessments, but they all differ from our proposal in that they do not model the propagation of incidents across an organization as precisely as we do. Furthermore, they do not differentiate between methods of analysing different security goals. We believe that differentiating between security goals allow us to determine risks more accurately. From this perspective we limit ourselves in this paper on confidentiality related risks.

For instance, Lenstra and Voss [11] present a quantitative approach to IT risk management to determine the optimal risk management, strategy given a limited budget. Their approach requires performing a risk assessment on all the applications supporting business processes and identifying the (monetary) loss due to each threat on the business process they support, thus the risk is evaluated in terms of the likelihood and the loss. Since this approach is designed to deal with threats to all the three aspects of information security (CIA), to keep it feasible it lacks in a complete representation of the constituents of an IT infrastructure (machines, applications, etc.) and in modelling the functional dependencies between them, which is essential for properly modelling the confidentiality risks. Our model, on the other hand, being specifically tailored for confidentiality risks, considers the IT infrastructure on which the confidential information relays on and the interdependencies among them.

Another proposal is that of Aagedal et al. [1], who developed the CORAS framework to produce an improved methodology for precise, unambiguous, and efficient risk analysis of security critical systems. CORAS focuses on the tight integration of viewpoint-oriented visual modelling in the risk assessment process, using an UML-based approach in the context of security and risk assessment. Although, both our approach and CORAS are asset oriented, our approach distinguishes by considering the IT Infrastructure in modelling the risk propagation.

A further approach to risk modelling is proposed by Arnes et al. [3]. They use Hidden Markov Models to evaluate the risks of intrusion, and present risk depending on IT assets, as well as define the risk level of a network as the composition of risks of individual hosts. Our approach is more mature then, in the sense that it also models the propagation of risks.

Furthermore, our model is designed to be used with standard risk assessment methodologies. Ciechanowicz [6] states a number of requirements for a risk analysis methods. These requirements are group in 6 categories: common sense requirements, business requirements, functional requirements, security, audit and control requirements. Our model is compatible with Ciechanowicz's requirements.

In our approach we model the relations among the system components using so-called layers. The motivating idea is that layers enable concentrating on different attributes of assets, studying the interrelations between assets on different abstraction layers, meanwhile remaining expressive. Eck et al. [20] present GRAAL to provide a conceptual framework to describe an ICT architecture in a business. It differentiates between Business Layer (Events, communication channels and stimulus), Software Layer (system transactions, software library) and Physical Layer (Network topology, machines) layers. Our approach is orthogonal to GRAAL, since we use the layered architecture of GRAAL for modelling IT related confidentiality risks.

Another layered approach to risk management is introduced by Innerhofer-Oberperfler and Breu [9]. Differently from our approach, they consider the enterprise architecture, to model the interrelations between stake-holders, business processes and information assets. They use the model to drive security requirements that are linked to the threats and integrated in the risk management process. Instead, our approach is based on

the IT Architecture and on the propagation of confidentiality breaches. Therefore the two approaches may be used in a complementary way.

Finally, our model is designed for supporting the dynamic risk management process, as the authors did in [21] in the field of availability risk management and business continuity. As for the availability model presented in [21], this one is meant to be implemented by a tool and used to assess the risks in a continuously changing environment. This approach is especially suitable for organizations where it is important that the level of risk is constantly kept under control.

III. Present Methodologies for Risk Management

There exists a number of standards and methodologies for Risk Management, among which COBIT (Control Objectives for Information and related Technology) [7] and NIST SP800-30 [16] are of particular relevance to our work. COBIT is the *de facto* standard for information control and IT Risk Management, addressing IT Governance and control practices. It provides a reference framework for managers, users and security auditors. COBIT is mostly based on the concept of *control* (be it technical or organizational) which is used to assess, monitor and verify the current state of a certain process (that may refer to procedures, human resources, etc.) involved in the information system. To implement COBIT, the organization must benchmark its own processes against the control objectives suggested by the framework, using the so-called *maturity models* (derived from the Software Engineering Institute's Capability Maturity Model [15]). Maturity models basically provide: (1) a measure expressing the present state of an organization, (2) an efficient way to decide which is the goal to achieve and, finally, (3) a tool to evaluate progress toward the goal. Maturity modelling enables gaps in capabilities to be identified and demonstrated to management. Key Goal Indicators and Key Performance Indicators are then used to measure, respectively, when a process has achieved the goal set by management and when a goal is likely to be reached or not. Since COBIT does not suggest any technical solution but only organizational solutions, organizations combine COBIT and ISO 17799, applying the controls suggested in the part *Code of Practice for Information Security Management* of the standard.

As we mentioned before, current methodologies are not sufficiently taking into account how information assets are linked together and the way a single confidentiality breach could propagate and affect other related assets. The fact that COBIT and ISO 17799 do not consider dependencies between IAs has even greater impact in the mitigation phase of confidentiality risks: it is standard practice to protect the information assets whose confidentiality has a greater *direct impact* on the organization goals, while a more accurate analysis in many cases reveals that it is more cost effective to protect some of the information assets that have an *indirect impact* as well.

IV. Modelling Architecture

In this section we propose the DCRA-Model. We follow notable architecture frameworks, such as TOGAF [17], Zachman [18] and ArchiMate [2] as well as IT Governance solutions (IBM [8] and ISACA [7]), to determine the elements, which may directly or indirectly be involved in leakage of confidential information.

The DCRA-Model consists of: (1) A representation of the IT infrastructure of an organization, consisting of a set of Information Assets, of the IT Assets that they depend on, and a set of relationships between them. (2) A representation of estimated values assigned to the Information Assets. This can be integrated with set of possible incidents affecting the confidentiality of Information Assets, annotated with the expected frequency estimation, measured in times per year (See Section V).

The DCRA-Model is divided in 3 layers: The Business Layer, The IT Layer, and The Physical Layer. The *Business Layer* consist of business related events and communications. This is the layer where the value of information assets is defined[1]. The *IT Layer* is the layer where the interconnections between IT assets are defined. This layer consists of the applications, the middleware and the operating systems. The *Physical Layer* contains the hardware, on which the components of the IT Layer runs. Here we follow [19] in calling information assets the semantic components of an information system that "an organization must have to conduct its mission or business".

A. IT&I-Model

The IT&I-Model is the core of the DCRA-Model. In it, we represent an IT infrastructure of an organization using a graph, where nodes represent IT Assets and labelled edges between nodes represent their relationships. The presence of an edge from node a to node b indicates that the information stored in b depends on the information stored in a in a way that, the disclosure of confidential information in a may propagate to the linked assets (in this case b), and cause the confidential information stored in b to become disclosed as well. To model this correctly, we refer to a measure (likelihood) of this propagation occurring: we annotate each edge with the "propagation likelihood", i.e. the estimated likelihood that an attacker that has intruded in a is able to use the outcome of this attack for attacking b.

We model this probability in a qualitative way, as it is commonly done in many risk assessment methodologies, such as [16], as well as in academic works, such as [11]. We refer to the following set of likelihood values $\mathbb{L}$ = {*High, Medium-high, Medium, Medium-low, Low, Null*}, and to the binary operator $\bullet$ on $\mathbb{L}$ whose behaviour is defined in Table I.

Then, assuming that $\mathbb{R}^+$ indicates the set of positive real numbers, $\mathbb{L}$ is defined above and $\mathbb{V}$ is the domain of asset values, the IT&I-Model is defined as follows.

[1]We address this in Section IV-B in more detail

TABLE II
IT ASSETS OF THE IT LAYER.

ID	Description
a_1	domain controller
a_2	doctors PC at home
a_3	doctors PC
a_4	nurse PC
a_5	admin PC
a_6	patient database

TABLE III
INFORMATION ASSET - IT ASSET MAPPING.

ID	Description / Value	Location	→	Percentage
i_1	patient data / 5	a_2	→	5%
		a_3	→	15%
		a_4	→	10%
		a_6	→	100%
i_2	user credentials / 1	a_1	→	100%
		a_2	→	10%
		a_3	→	30%
		a_4	→	30%
		a_5	→	10%

Definition 4.1: An IT&I-Model is a tuple $\langle \mathbf{P}, \mathbf{I}, \xrightarrow{l}, v \rangle$, where $\mathbf{I}$ is a set of information assets, $\mathbf{P}$ is a set of IT assets, $\xrightarrow{l}$ is a mapping $\mathbf{P} \times \mathbf{P} \rightarrow \mathbb{L}$, and v is a mapping $\mathbf{P} \cup \mathbf{I} \rightarrow \mathbb{V}$.

We write $a_i \xrightarrow{l} a_j$ as shorthand for $(a_i, a_j, l) \in \rightarrow$. $a_i \xrightarrow{l} a_j$ indicates that an attacker which discloses the asset a_i may directly disclose the confidential information stored on asset a_j with likelihood l. Furthermore, $v(a)$ indicates the operational value of the confidential information stored on a. We should mention that dependency relationships are typically AND relationships: an asset depending on two or more other assets may be hacked even if just one of them is affected by an incident. For the sake of simplicity, in this work we do not consider OR relationships, even though it would be simple to include them in our model.

From now on, we support the exposition of the model by means of a running example.

Running example - Part 1: We present here an example (oversimplified, to fit in the format of the paper) of the IT infrastructure of a clinic, whose assets are listed in Tables II and III. The IT&I-Model is reported on Figure 1. The edges that connect the assets on the IT Layer and the Physical Layer express the dependencies, and are annotated with the likelihood of propagation of incidents between assets. The edges connecting the Information assets of the Business Layer to the IT assets on the IT Layer express that a given Information Asset is contained in some IT assets, and are annotated with the percentage of information stored on each IT asset.

Assuming that Alice, who is logged on to the Nurse PC without authorization, scans the temporary files and finds a doctors credentials. With *Low* probability she is then able to use this information to log onto the doctors PC. Furthermore, once she has penetrated the doctors PC, she has *Low* probabilities to disclose the confidential patient information stored in the patient database.

B. The impact of information assets disclosure

To be effective, our model requires a value to be set that to each information asset which should be kept confidential (e.g. medical records, etc.). There are organizations which are able to express this value in terms of money, e.g. banks, insurance companies; for other organizations this can be harder. In such cases the value can be specified in a more qualitative way, e.g. using a linear value. The important thing to bare in mind when using the qualitative approach is that these figures should reflect the relative values of the information.

Finally, the model includes the percentage of each information asset that is stored on each IT component (this is necessary to establish the *local impact* of the disclosure of a physical or information asset). The percentage of each information asset $i \in \mathbf{I}$ stored in each asset $a \in \mathbf{P}$ is modelled with a $M \times N$ matrix $\mathcal{P}$, where $N = \mid I \mid$ and $M = \mid P \mid$. For instance according to Table III 15% of patient data is stored in PC-Doc.

Assuming that, the vector ψ of length N consists the value of Information Assets, the local impact vector v defines the value of each asset, such that

$$v = \mathcal{P} \cdot \psi \tag{1}$$

Running example - Part 2: According to Table III, the value of Information Asset "user credentials" is set equal to 1, and the value of "patient data" to 5. Table III shows also the percentage of confidential information stored in each asset. According to (1), the local impact of the disclosure of the assets in the clinic example are as follows: v_{a_1} = 1, v_{a_2} = 0.35, v_{a_3} = 1.05, v_{a_4} = 0.8, v_{a_5} = 0.1 and v_{a_6} = 5.

Using the IT&I-Model in Isolation The IT&I-Model is meant to be used within a RA (as it is shown in the next section). However, it can also be used in isolation, to do the following:

TABLE I
BEHAVIOR OF THE • OPERATOR.

•	High	Medium-high	Medium	Medium-low	Low	Null
High	High	Medium-high	Medium	Medium-low	Low	High
Medium-high	Medium-high	Medium-high	Medium	Medium-low	Low	Medium-high
Medium	Medium	Medium	Medium	Medium-low	Low	Medium
Medium-low	Medium-low	Medium-low	Medium-low	Medium-low	Low	Medium-low
Low	Low	Low	Low	Low	Low	Low
Null	High	Medium-high	Medium	Medium-low	Low	Null

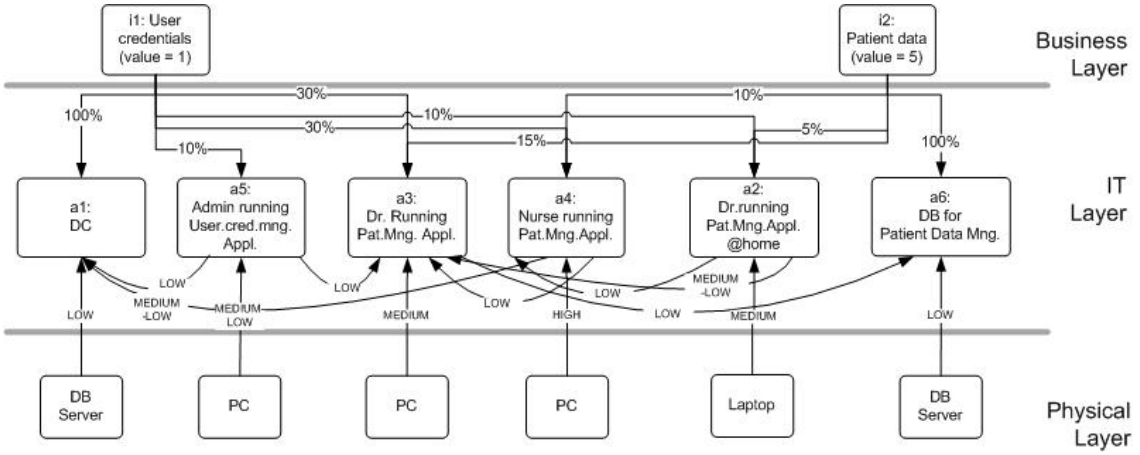

Fig. 1. Architecture of DCRA-Model example.

1) Evaluating, for each component of the IT infrastructure, which is the global impact resulting from a confidentiality violation. As a consequence, it is also possible to find which are the most critical among the IT components, i.e. the components with the highest associated global impact.
2) Comparing how robust two different IT architectures are with respect to confidentiality of information stored in it.

We now indicate how we can achieve both points.

1) Global impact: First we need to define the global impact of an asset a, which is the cumulative loss caused by disclosure of confidential information stored in a, and the disclosure of confidential information stored in assets depending on a.

Definition 4.2: Let v_p be the local impact of asset $p \in P$, the global impact of p is defined as:
$gImp(p) = v_p + \sum_{i=1}^{k} l_i \bullet gImp(p_i)$
where $\{p_1 - p_k\}$ are the assets of P directly depending on p (i.e. for which $p \xrightarrow{l_i} p_i$) and l_i is the likelihood associated to the edge $p \xrightarrow{l_i} p_i$.

Since the IT&I graph is acyclic the concept of global impact is well defined.

Running example - Part 3: In case PC-Nurse is cracked, the confidential information stored on it gets disclosed. Accordingly, the local impact of this confidentiality violation on "PC-Nurse" is 0.8 and on PC-Admin is 0.1. According to this, PC-Nurse a more critical component then PC-Admin.

Looking at the global impact, compromising PC-Nurse can lead to compromising a_1 and/or a_3 (and – iteratevely – a_6) corresponding to the following sequences of attacks: $Seq_1 = a_4, a_1$ and $Seq_2 = a_4, a_3, a_6$. The global impact of (exploiting) PC-Nurse is then:
$gImp(a_4) = 0.8 + Medium - low \bullet 1 + Low \bullet 6.05$.

2) Architecture comparison: For comparing the robustness of different architectures (w.r.t. confidentiality risks), we calculate the average and standard deviations of global impact values of disclosing the confidential information stored on each asset of the two architectures. The standard deviation tells us how widely spread the global impacts are. If the standard deviation is small, then the potential impact is almost equally distributed on many assets. Otherwise, there are few critical components in the system with high potential impact.

Due to space reasons, we are not providing any further details here.

V. Modelling Risk

In this section we introduce the concept of "incident" and we show how to integrate it in the DCRA model to carry out a complete risk assessment.

Incidents are security related events affecting one or more assets on which some confidential information is stored. Incidents can happen several times a year, and Risk Assessment methodologies [7], [16] always require to make an inventory of possible incidents, together with their expected frequencies. This information (type and expected frequency of incidents) is thus available after carrying out a standard RA, though it is usually expressed in qualitative terms (e.g. likely, moderate-likely, unlikely).

Definition 5.1: Let **P** be a set of IT assets, an *incident* is a mapping $i : \mathbf{P} \rightarrow \mathbb{R}^+$.

In particular, $i(p)$ indicate how often (per year) the incident i is expected to affect the IT asset p. If $i(p) = 0$ then the incident i does not affect p. On the other hand, by setting $i(p) \neq 0$ we model the situation in which an occurrence of i would cause the disclosure of all the confidential data on p; in this case we say that i directly affects p. Of course, an incident can cause an indirect damage by propagation, as described in the previous section. To measure thus the *global* impact of an incident we have to refer to the $gImp()$ function (Definition 4.2). With it, we can compute the *risk level* of a system

Definition 5.2: Let **I** be a set of incidents and **P** be the set of IT assets in the system. The risk level of the system is

calculated with the following formula:

$$\sum_{p \in P, i \in I} i(p) * gImp(p) \quad (2)$$

We now apply this definition do calculate the level of risk of the clinic example.

Running example - Part 4: Let us assume that we have two incidents effecting the "PC-Nurse" directly; an attacker could break directly into the employee mail (i_1) or get the nurses authentication information by masquerading herself as system administrator (i_2). The expected frequency of these incidents are respectively "moderately likely" (which corresponds to an expected frequency of twice a year) and "unlikely" (which corresponds to an expected frequency of once every three-four years). The global impact for "PC-Nurse" is presented as multiplication of the local impacts of assets (see Running Example - Part 2) and of incident propagation likelihoods: $gImp(PC - Nurse) = 0.8 + Medium - low \bullet 1 + Low \bullet 6.05$. Furthermore, the asset "PC-Nurse" is affected by two incidents, and according to Definition 5.2 the global impact of incident i_1 is $moderately - likely * (0.8 + Medium - low \cdot 1 + Low \cdot 1.05 + Low \cdot 5)$, while the global impact of incident i_2 is $unlikely * (0.8 + Medium - low \cdot 1 + Low \cdot 1.05 + Low \cdot 5)$.

Integrating the IT&I model in RA methodologies: Most RA methodologies currently in use require assessing the impact of incidents (intended as threats exploiting vulnerabilities). For instance, [16], [5] recommends to use FIPS 199 [12] to categorize the impact level as Low, Moderate, High, according to a standard description of the effects of the incident itself.

IT&I-Model is designed to be used together with standard Risk Assessment methodologies to provide a more specific and architecture-dependant approach to evaluate the impact of incidents, and it can be easily integrated in those methodologies by using as input the incident information and providing the global impact of those incidents as output. To make possible a full integration we need to translate the output of our system (which is given in term of a sum of likelihood-value products) in term of the usual LOW, MODERATE, HIGH notation. Although we believe that our approach is more suitable for RA than this, since it allows a more fine-grained analysis of the effect of a confidentiality incident, it is simple to flatten our global impact into a single value. For the purpose of our running example we adopt this mapping: if the impact value is higher than the 10% of the total value of all the information assets, than it is mapped as HIGH, if it is higher than 0.1% then it is considered as MODERATE, otherwise LOW.

Running example - Part 5: Let us assume that the clinic is using NIST SP 800-30 for Risk Assessment purposes. The risk related to incident i_1 on "PC-Nurse" is $moderately - likely * (0.8 + Medium - low \cdot 1 + Low \cdot 1.05 + Low \cdot 5)$.

Furthermore, IT&I-Model delivers a further simplified version of the semi-quantitative risk value by assigning quantitative values to qualitative ones. Respectively, the quantitative risk related to "PC-Nurse is: $(0.1 + 0.05) \cdot (0.8 + 0.1 \cdot 1 + 1.05 \cdot 0.05 + 0.05 \cdot 5) = 0.18$.

Since the total value of the information assets in the clinic example is 6, and 0.18 is between 0.1% and 10% of the total value, the risk level of incident i_1 is therefore MODERATE.

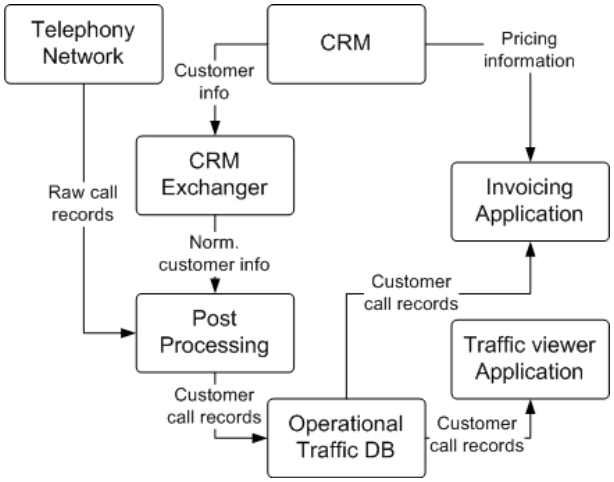

Fig. 2. Telecommunication company invoicing process

VI. Application of DCRA-Model

To show how to use and which are the outcomes of the DCRA model, we apply our approach to a segment of the IT infrastructure of a real-world telecommunication company. The source of the information in this example comes from the past working experience of one of the authors.

Part of the core business of a telecommunication company consists of generating proper invoices for the customers of the company by counting the calls they did. The invoicing process is composed by a number of steps, which we summarized in Figure 2: at first, the raw call records are provided by the physical network infrastructure. The record does not contain any information about the customer, but only a reference to the physical telephone line. These records are then enriched by the Post Processing application with the customer information provided by the Customer Relationship Manager (CRM) application. Since the data format used by CRM application is too complex for the Post Processing application, the customer information is first normalized by the CRM Exchanger application. After the post-processing phase, the enriched call records are then stored in the Operational Traffic Database, where they are readily accessible for inspection by means of the Traffic Viewer application. Finally, the invoicing application uses the complete call records, together with the pricing information from the CRM, to calculate the exact amount of each customer invoice. Furthermore, the infrastructure includes other components, such as a complete test environment for the Post Processing, Operational Traffic, Traffic Viewer and CRM Exchanger applications, the file and e-mail servers used by the developers, as well as the laptop used by the employees of the company and of the external consultants.

TABLE IV
INFORMATION ASSETS

Asset	Loss (Eur)
Customer call records	100,000,000
Raw call records	10,000,000
Phone contract info	20,000,000
Phone line info	500,000
Test data sets	0
Application design specification	0
SW Test documentation	0
Encryption keys	0
Employee mail	70,000

Since applications run on different hardware components, the data is transferred from one to the other by means of encrypted flat files. Part of the information, such as the source and destination phone numbers and the customer ID are kept partially encrypted inside the Operational Traffic Database. Access to this database is also controlled by strong authentication mechanisms and logs are generated for each read operation. Encryption keys are kept inside a key repository, and applications can access the repository to retrieve the keys and use the encrypted flat files.

A. Building the model

To build our model we start from the business layer: Table IV reports the information assets that we identified, together with the estimated (monetary) loss due to their disclosure. The most important information assets are the customer call records, the raw call records, the phone contact information and the phone line information which have to be kept confidential because of laws and liability issues. The disclosure of the employees mail has a lower but still significant impact, while the disclosure of the other assets is judged to have no direct impact.

The IT layer is composed by the custom applications used in the invoicing process and general purpose software components providing services to the users or to other software components. Table V reports the applications (top part of the table) and infrastructure components (bottom part of the table) supporting the invoicing process, together with the information assets they contain and their percentage. The call records, which are among the most valuable pieces of information, are contained, in different percentages, in the following applications: post processing, traffic viewer and invoicing. Furthermore, we observe that the CRM exchanger test application contains part of the production phone line information. This is due to the fact that generating fake data sets to test the CRM exchanger application is too time consuming, and some real phone lines are used for testing purposes. Moreover, the mail client application contains both the employees mail and the application specification and test documentation, because employees are used to share documents by means of the e-mail service. Finally, as expected, the Oracle server used to implement the operational traffic database contains the whole user call records; moreover, since some employees need to regularly control the formal quality of the call records shared between the various applications, some call record files are stored also on the FTP cache of the employees laptops.

TABLE V
COMPONENTS OF THE IT LAYER AND THE INFORMATION ASSETS THAT THEY USE

Component	Information asset	Perc.
Telephony network database	Raw call records	100%
Post processing	Raw call records	5%
	User call records	5%
	Phone line info	100%
Operational traffic procs	-	-
Traffic viewer	User call records	100%
CRM	Phone contract info	100%
	Phone line info	100%
CRM Exchanger	Phone line info	100%
Invoicing	User call records	20%
	Phone contract info	100%
Post processing test	Test data sets	100%
Operational traffic test	Test data sets	100%
Traffic viewer	Test data sets	100%
CRM Exchanger	Test data sets	100%
Mail client	Application design spec.	4%
	SW Test documentation	3%
	Employee mail	1%
FTP Service	-	-
Operational traffic Oracle	User call records	100%
Traffic viewer app. server	-	-
Employee FTP client	User call records	0.5%
SAMBA server	Application design specifications	100%
	SW Test documentation	100%
MS Exchange server	Employee mail	100%
	Application design specification	70%
	SW Test documentation	60%
Encryption key server	Encryption keys	100%

TABLE VI
PROPAGATION PROBABILITIES

Source	Destination	Probability
Traffic Viewer Server	Traffic DB	H
Key Server	FTP Service	M-H
MS Outlook Mail Client	FTP Client	M
MS Outlook Mail Client	Post Processing App.	L
MS Outlook Mail Client	Traffic View App.	L
MS Outlook Mail Client	CRM Exchanger App.	M-L
MS Exchange Server	FTP Client	M
MS Exchange Server	Post Processing App.	M-L
MS Exchange Server	Traffic View App.	L
MS Exchange Server	CRM Exchanger App.	M-L
Samba Server	FTP Client	M-H
Samba Server	Post Processing App.	M-L
Samba Server	Traffic View App.	L
Samba Server	CRM Exchanger App.	M-L

The physical layer is composed by the hardware components on which the software runs. These are: Telephony network, post processing server, operational traffic server, traffic viewer server, CRM exchanger server, CRM server, invoicing server, employee laptop, file server, network segment, test server and mail server.

Figure 3 gives a complete outlook of the DCRA model for this telecommunication company example.

To complete the DCRA model, we also need to assess how the disclosure of information can propagate within the organization. Some propagations are quite intuitive: compromising

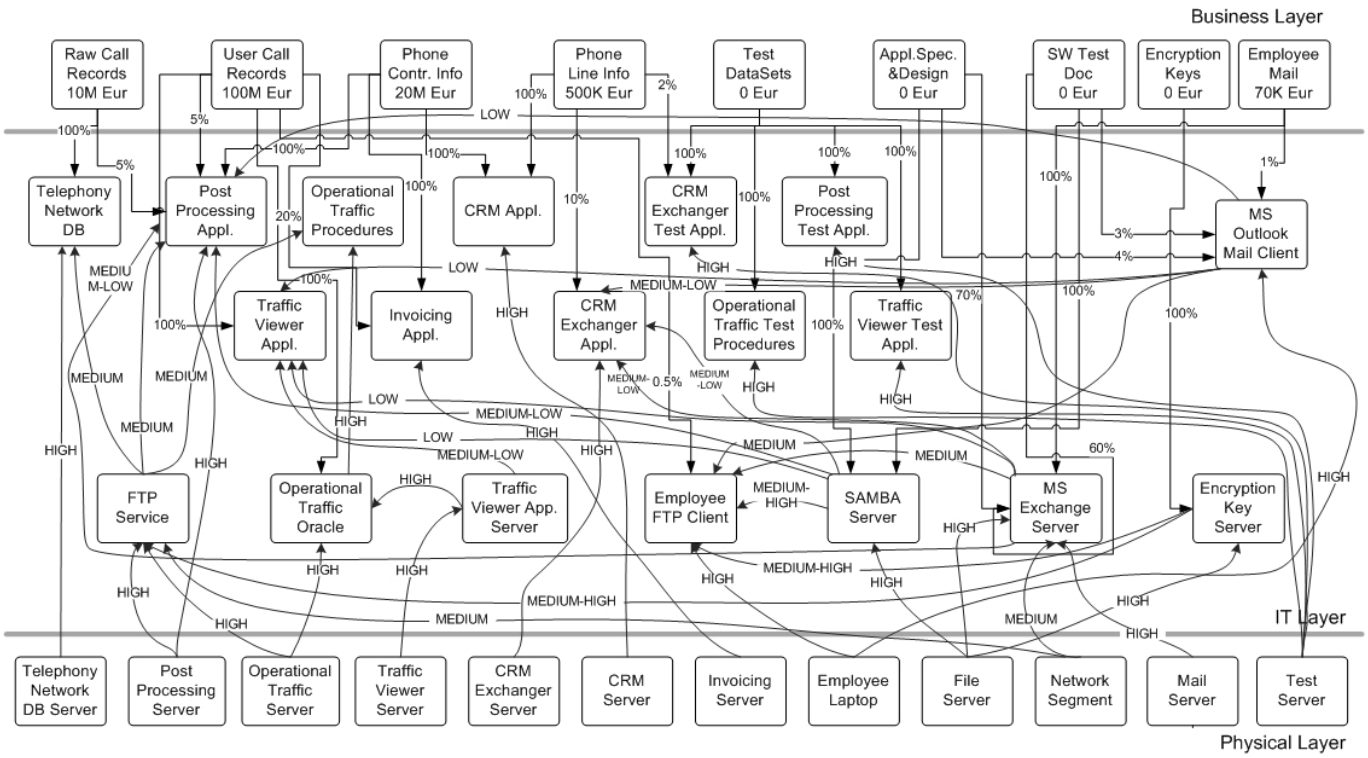

Fig. 3. DCRA model for telecommunication company invoicing process

a physical asset such as a machine implies that with high probability the information contained on it will be disclosed. Table VI reports the other, non-trivial cases, we have found in this scenario, together with their estimated probability. The first propagation scenario assumes someone has the control of the traffic viewer application server: since the configuration of the application server also includes the credentials to access the Oracle traffic database, with a high degree of probability it will also be possible to obtain the user call records stored on the database. The second scenario assumes someone has broken the key server and owns some of the keys stored on it: with this information, one can access the user call records by sniffing the FTP traffic transiting on the network and then trying to decrypt them; the probability of this event (medium-high) is evaluated by considering both the skill level needed to perform this operation and the number of tries necessary to use the right key to decrypt the sniffed file. The subsequent scenarios assume someone gets access to the test software documentation, this can be achieved by either breaking the SAMBA server or the employee mail. In this case the attacker can use the information stored in those documents, such as the test credentials, the application behaviour (and bugs), for different purposes. He or she can break the FTP service to retrieve the call record flat files, or use a back-door on the post processing, traffic view and CRM exchanger applications to get sensible information. The remaining two scenarios are similar, and assume someone has access to the specifications documentation of some applications and can exploit this information to bypass the security controls on the post processing and traffic view applications, to obtain the user call records.

B. Using the model

After building the DCRA model we are ready to use it to assess the robustness of the IT architecture of the telecommunication company with respect to confidentiality of information. The first step towards the assessment of the architecture is to derive the local impact of each component. To do this we build the $\mathcal{P}$ matrix containing the percentage of each information asset contained in each IT component with the values from Table V; we also build the value vector ψ containing the value of each information asset as reported on Table IV. Table VII reports the resulting v vector, corresponding to the total direct impact due to the disclosure of information contained on each IT component with respect to all the information assets it contains. Despite it contains many different information assets, the Post Processing application is not the IT component with the highest associated amount, since it contains small percentages of the most valuable assets (the call records) at one time. On the other hand, as expected, the Traffic Viewer application and the Oracle database containing the whole user call records are the two most valuable components of the entire IT infrastructure. One unexpected outcome from this first analysis is that the CRM Exchanger test application, which should be expected to have no importance, is worth 50,000 Euro. This is due to the choice of using production data to test the application, as we discussed in the previous section.

The second step to complete the assessment of the architecture is to evaluate the global impact to the disclosure of the information contained in each component of the IT infrastructure. This way we can find which are the most critical components of the architecture, evaluate the global impact distribution of the architecture, and subsequently check if the IT components are protected accordingly to their real importance. To evaluate the global impact we apply the *gImp()* function, which takes into account also that incidents propagate from one asset from the other. Table VIII reports the results; when applying the *gImp()* function we use the following rule: if two components of the resulting impact vector refer to the same information asset and have comparable values, then we only include the one with the highest likelihood. If both the values and the likelihood are different we keep both. As expected, some of the IT components, such as the Mail client and the SAMBA server, which at a first look may seem to be of secondary importance, are more critical due to the possible propagation of information disclosure.

The last step of our assessment is now to calculate the average level of the global impact and its standard deviation, to be able to calculate such values from a semi-qualitative notation, we apply the following translation of the probability values into numerical ones: High = 0.9, Medium-high = 0.5, Medium = 0.3, Medium-low = 0.1, Low = 0.05. In this way we are able to flatten the impact vectors and obtain a single value. The resulting average global impact is $\sim 23,000,000$, while the standard deviation is $\sim 33,000,000$ which is relatively high, due to the fact that some IT assets have a global impact equal to zero, while other assets have a very high potential impact.

Concluding, the result of using the IT&I model in isolation shows that the IT infrastructure of the telecommunication company is quite heterogeneous: some components are at high risk, while some others are almost safe. On the other hand, the amount of critical components in this infrastructure is very high with respect to the amount of non-critical ones. This may suggest that the architecture does not present a graceful degradation with respect to confidentiality violations, because a big effort in protecting critical components must be applied to several ones.

VII. Constructing a DCRA-Model

In this section, we argue that building our model is feasible in practice. In particular, we show that organizations already have the majority of the input data we need, in the form of IT architecture documentation. For instance, the GRAAL framework [20] has been designed for architecture alignment of business requirements on IT systems and is structured in a form that is similar to our three-layered model. The GRAAL framework has been successfully adopted as case study in many organizations showing that the layered structure they adopted is understood inside organizations and that any similar model can be easily translated to the GRAAL notation.

Furthermore, specification documents provide us the information about where and in which fraction information assets are located in the physical assets, allowing us to compile the matrix $\mathcal{P}$ reporting the percentage of the information asset stored in each physical asset.

Finally, Risk Assessment methodologies already require to make an inventory of possible incidents, together with their frequency. We can find this data in the deliverables of Risk Assessments carried out following standard methodologies.

TABLE VII
Local impact of the IT components.

Component	Impact (Eur)
Telephony network database	10,000,000
Post processing	25,000,000
Operational traffic procs	0
Traffic viewer	100,000,000
CRM	20,500,000
CRM Exchanger	50,000
Invoicing	40,000,000
Post processing test	0
Operational traffic test	0
Traffic viewer test	0
CRM Exchanger test	10,000
Mail client	700
FTP Service	0
Operational traffic Oracle	100,000,000
Traffic viewer app. server	0
Employee FTP client	500,000
SAMBA server	0
MS Exchange server	70,000
Encryption key server	0

VIII. Conclusion and Future work

In this paper we present a confidentiality risk assessment model, which takes into consideration the interdependencies between information assets and the IT infrastructure that they relay on.

Although the necessity of considering the interrelations between information assets and components of IT infrastructure, as well as protection of seemingly uncritical data, is indicated in present methodologies (e.g. NIST SP 800-30 [16]), it is not specified how this can be realised. Furthermore, the research in this field is limited to assessing the risk for each asset separately. Hence, the interrelations among them and consequently the propagation of risk are not systematically analysed.

This yields to risk analyses which are not as accurate as they should be and which can not deal easily with changes in the infrastructure (dynamic risk management).

The model we present in this paper is a proposal to solve this problem and represents a first step towards dynamic management of confidentiality risks. In order to validate the model we are planning to integrate it to the case studies we are going to construct with industrial partners.

Acknowledgements

We thank Roel Wieringa for his suggestions.

TABLE VIII
GLOBAL IMPACT OF THE IT COMPONENTS.

Component	Global Impact
Telephony network database	10,000,000
Post processing	25,000,000
Operational traffic procs	0
Traffic viewer	100,000,000
CRM	20,500,000
CRM Exchanger	50,000
Invoicing	40,000,000
Post processing test	0
Operational traffic test	0
Traffic viewer test	0
CRM Exchanger test	10,000
Mail client	700 + L · 100,000,000 + M · 500,000
FTP Service	M · 25,000,000
Operational traffic Oracle	100,000,000
Traffic viewer app. server	H · 100,000,000
Employee FTP client	500,000
SAMBA server	M-H · 500,000 + M-L · 25,000,000 + M-L · 50,000 + L · 100,000,000
MS Exchange server	70.000 + M · 500,000 + M-L · 50,000
Encryption key server	M · 10,000,000 + M · 25,000,000
Telephony network database server	H · 10,000,000
Post processing server	H · 25,000,000
Operational traffic server	H · 100,000,000
Traffic viewer server	H · 100,000,000
CRM Exchanger server	H · 50,000
CRM server	H · 20,500,000
Invoicing server	H · 40,000,000
Employee laptop	H · 700 + L · 25,000,000 + L · 100,000,000 + M-L · 50,000,000
File server	M-H · 500,000 + M-L · 50,000 + L · 100,000,000 + H · 70,000 + M · 25,000,000
Network segment	M · 70,000 + M · 500,000 + M-L · 50,000 + M · 25,000,000
Mail server	H · 70,000 + M · 500,000 + M-L · 50,000
Test server	H · 10,000

REFERENCES

[1] J. Ø. Aagedal, F. den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stëlen. Model-Based Risk Assessment to Improve Enterprise Security. In *EDOC '02: Proc. 6th International Enterprise Distrubuted Object Computing Conference*, pages 51–63. IEEE Computer Society, 2002.

[2] The ArchiMate project. http://archimate.telin.nl.

[3] A. Arnes, F. Valeur, G. Vigna, and R. Kemmerer. Using hidden markov models to evaluate the risks of intrusions: System architecture and model validation. In *Proc. of the Int. Symp. on Recent Advances in Intrusion Detection (RAID)*, Hamburg, Germany, September 2006.

[4] T. Berners-Lee, R. Cailliau, A. Luotenen, H. F. Nielsen, and A. Secret. The world-wide web. *Communications of the ACM.*, 37(8), Aug. 1994.

[5] P. Bowen, J. Hash, and M. Wilson. Information Security Handbook: A Guide for Managers. Technical report, NIST, 2006. SP 800-100.

[6] Zbigniew Ciechanowicz. Risk analysis: requirements, conflicts and problems. *Computers & Security*, 16(3):223–232, 1997.

[7] CobiT: Control Objectives for Information and related Technology. http://www.isaca.org.

[8] R. Cocchiara. Beyond disaster recovery: becoming a resilient business. Technical report, IBM, 2005. http://ibm.com/services/its/resilience.

[9] F. Innerhofer-Oberperfler and R. Breu. Using an Enterprise Architecture for IT Risk Management. In *ISSA '06: Proc. Information Security South Africa Conference*, 2006. URL: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/115_Paper.pdf.

[10] ISO/IEC 27001:2005 Information techniques - Security techniques - Code of practice for information security management.

[11] A. Lenstra and T. Voss. Information Security Risk Assessment, Aggregation, and Mitigation. In *ACISP: Information Security and Privacy: Australasian Conference*, 2004.

[12] NIST - National Institute of Standards and Technology. Standards for Security Categorization of Federal Information and Information Systems. Technical report, 2004.

[13] Joint Technical Committee OB-007. Risk Management: AS/NZS 4360:2004, 2004.

[14] OCTAVE risk methodology. http://www.cert.org/octave/.

[15] M. C. Paulk, C. V. Weber, B. Curtis, and M. B. Chrissis. *The capability maturity model: guidelines for improving the software process*. Addison-Wesley Longman Publishing Co., Inc., 1995.

[16] G. Stoneburner, A. Goguen, and A. Feringa. Risk Management Guide for Information Technology Systems. Technical report, NIST, 2002. SP 800-30.

[17] The Open Group. TOGAF (The Open Group Architecture Framework), 2003. http://www.opengroup.org/architecture/togaf8-doc/arch/.

[18] The Zachman Institute for Framework Advancement. Zachman Framework, 2007. http://www.zifa.com/.

[19] H.F. Tipton and M. Krause. *Information Security Management Handbook*. Auerbach Publications, Boca Raton, New York, 2007.

[20] P. A. T. van Eck, H. M. Blanken, and R. J. Wieringa. Project graal: Towards operational architecture alignment. *International Journal of Cooperative Information Systems*, 13(3):235–255, 2004.

[21] E. Zambon, D. Bolzoni, S. Etalle, and M. Salvato. Model-based mitigation of availability risks. In *Second IEEE/IFIP International Workshop on Business-Driven IT Management, Munich, Germany*, pages 75–83, Munich, May 2007. IEEE Computer Society Press.