Journal of Information Security, **2013, 4, 33-41**
http://dx.doi.org/10.4236/jis.2013.41005 Published Online January 2013 (http://www.scirp.org/journal/jis)

A Socio-Technical Approach to Cyber Risk Management and Impact Assessment

Konstantinia Charitoudi, Andrew Blyth
Information Security Research Group, University of Glamorgan, Trefforest, UK
Email: kcharito@glam.ac.uk, ajcblyth@glam.ac.uk

Received September 17, 2012; revised Ocotber 22, 2012; accepted November 26, 2012

ABSTRACT

Technology is increasingly being used by organisations to mediate social/business relationships and social/business transactions. While traditional models of impact assessment have focused on the loss of confidentiality, integrity and availability, we propose a new model based upon socio-technical systems thinking that places the people and the technology within an organisation's business/functional context. Thus in performing risk management in a cyber security and safety context, a detailed picture of the impact that a security/safety incident can have on an organisation is developed. This in turn stimulates a more holistic view of the effectiveness, and appropriateness, of a counter measure.

Keywords: Impact Assessment; Risk Management; Socio-Technical Systems

1. Introduction

It is clear that, given the level of complexity of Information Systems Security (ISS) risk management's simple linear models as proposed in most of the existing approaches will not be able to capture such complexities [1]. To achieve a more complete picture of the risks that cyber attacks pose to safety and security a more social oriented model must be developed that views an organisation as a holistic construct comprising of people and technology; and allow for the relationships and interactions between them to be better modelled and understood.

The term socio-technical system is used to describe the function and form that people (individuals, groups, roles and organisations), physical equipment (buildings, surroundings, etc.), hardware and software, laws and regulations that accompany the organisations (e.g. laws for the protection of privacy), data (what data are kept, in which formats, who has access to them, where they are kept) and procedures (official and unofficial processes, data flows, relationships play in comprising an organisation [2]. From a risk assessment perspective the challenge is to understand that impact that a potential loss of cyber safety and security can have on the organisation.

Thus our target is to construct a framework that will allow us to reason about risk and impact assessment as a stateful model on a socio-technical systems level so as to better capture the dynamics of a cybernetic organization and its state of affairs. It is in the cybernetic organizations' nature that we can find the arguments for the need of a more social approach to cyber security and safety. The socio-technical systems (STS) have as a main target to blend both the technical and the social systems in an organization. This can be viewed as a necessary condition within a risk management framework as both aspects are of equal importance [3]. We will use stateful models to express the status quo of an organization, *i.e.* the current state of the systems, personnel and processes at each discrete moment before and after an event have occurred. This is going to give us a better perspective of the dependencies, responsibilities and finally reliabilities that run through the entire hierarchical chain of an organisation. Thus it will allow us to be able to run different threat scenarios and detect the potential vulnerabilities in a corporate network through forward and backward chaining.

2. What Is a Socio-Technical System

The socio-technical systems (STS) concept first appeared in the 1950s, as a project for the Tavistock Institute in London, in an attempt to focus on the group relations at all levels in an organization and come up with innovative practices in organizational development to increase productivity without the need for a major capital [3,4]. By socio-technical systems we mean people (individuals, groups, roles and organizations), physical equipment (buildings, surroundings, etc.), hardware and software, laws and regulations that accompany the organizations (e.g. laws for the protection of privacy), data (what data are kept, in which formats, who has access to them,

where they are kept) and procedures (official and unofficial processes, data flows, relationships, in general anything that describes how things work, or better should work in an organization) [5].

Socio-technical systems are focusing on the groups as working units of interaction that are capable of either linear "cause-effect" relationships, or non-linear ones more complex and unpredictable [4]. They are adaptable to the constantly changing environment and the complexity that lies in the heart of most organizations.

The concept of tasks, their owners, their meaningfulness and the entire responsibility modelling as well as the dependencies are also a big part of this theory. In this study we treat people and systems as actors of certain tasks over a state of affairs. They are agents that comply with the same rules and norms, when it comes to the way they operate and interact with other agents for the accomplishment of states of affairs, with a model we are introducing in another section below. By agents, we mean individuals, groups of people or systems that hold roles and thus responsibilities for the execution or maintenance of certain tasks with certain objectives; we expanded the classic definition used in Artificial Intelligence [5].

Along with the socio-technical systems approach we will use Role Theory on the agents as each one of them in an organization fulfils some roles in association with certain states of affairs. Role Theory emphasizes on the fact that roles are basically sets of rights and responsibilities, expectations, behaviours or expected behaviours and norms. People's behaviour in organizations is bounded by specific context subject to both social and legal compliance, depending on their position in the hierarchy.

The objective of this is to be able to assist the performance of Responsibility Modelling on the socio-technical systems [5] to analyse their internal structure, the responsibility flows and the dependencies. This will provide us with the necessary information and structure upon which we can apply scenarios that simulate behaveiours deviating from the expected (e.g. attack scenarios) [6], along with logical rules that best describe the organization at hand, its expected behaviour and targets, that will allow us to locate vulnerabilities in the supply chain and express cause and effect, in case anything changes to the environment beyond expectation.

Different types of threats and countermeasures, different exposures, the variety of information and the heterogeneous data make it hard to manage risk. "Thus, it is clear that, given the level of complexity of Information Systems Security (ISS) risk management, simple linear models as proposed in most of the existing approaches will not be able to capture such complexities [1]." For this reason, we suggest the socio-technical systems approach combined with Role Theory and eventually Responsibility and Dependencies Modelling, as we think it works much better than linear models and is far more capable to map down the complex relationships, that more realistically represent organizations of any size and it is the nature of the information they provide that makes them appropriate for impact assessment and vulnerability analysis.

3. Impact Assessment

More and more security breaches are taking place the last few years, with a major pick on the attacks in 2011. DoS attacks, Botnets, Ghostnet, Operation Aurora, Flame, Stuxnet, Duqu and the very recent Gauss virus are only some of the major attacks that took place since 2009 onwards. No matter what the measures and the controls though, the assets or the information an organization is managing are never fully secure.

Thus businesses and organizations are utilising in Risk Assessment and Risk Management methods as a tool to mitigate this threat. The reason being, they are trying to prevent those breaches and consequently damage or loss of assets and information. Impact assessment is a critical tool in understanding how a Computer network Attack can impact on an organisation and can this be used as both a planning tool to allow for structured arguments and business investment to be considered and as a post-incident mitigation tool. Key to this decision process is situational awareness.

ISO 27005 is an Information Security Risk Management guideline applicable to organizations of all types that is why we are going to follow its definitions for Risk Assessment (RA). It provides a Risk Assessment Framework without providing specific methodologies and within this framework, Risk Assessment is recognized as the overall process of Risk Analysis and Risk Evaluation. Risk Analysis itself, is further divided in Risk Identification and Risk Estimation [7], *i.e*. any systematic use of information to identify sources and estimate the risk.

Risk estimation is the process used to assign values to the probability and consequence of risk and usually that is where the results of the overall process come from. In the process of Risk Identification we can place the identification of assets, threats, existing controls, vulnerabilities and impact. In essence, it is the finding, listing and characterizing elements of risk.

According to the same standards, the definition to threat is a potential cause of an incident that may result in an adverse change to an asset, a group of assets or an organization. Vulnerabilities are weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Impact Assessment is defined as

adverse change to the level of business objectives achieved, *i.e*. the loss of productivity and market share, or brand deterioration, penalties etc. It is used as a factor, along with the likelihood of occurrence of an event, the vulnerabilities and threats, to calculate and evaluate the risk.

Over the past years, a lot of methodologies have been developed in order to manage Information Systems Security (ISS) and Information Assurance (IA) [7,8]. Usually in the literature review Risk Assessment methods are divided into three categories, the qualitative ones, the quantitative ones and those that are a combination of both. The quantitative ones provide probabilistic results as to what is the percentage of running the risk, while the qualitative ones present results in predetermined scales of High-Medium-Low levels of risk. All the methods that appear in the literature have certain limitations so far, according to our opinion, and very few focus on the impact assessment side to properly estimate the impact itself and not to use impact to estimate the risk. Our approach is not focusing on the risk and threats side like the current methodologies and frameworks; we focus on impact and the propagation of it in the entire supply chain. Trying to calculate the probability of an event happening and predict it might be one perspective.

There is great difficulty in estimating the probability of loss occurrence as most methods suggest that such information is obtained by discussions with the users in order to understand the threat propagation. The problem with this approach is that these discussions are limited and they rarely help the analysts to get complete awareness and estimate the risk correctly [1]. Even when there is a proper understanding of the risk propagation it is extremely hard to quantify this even in a probabilistic way. So we suggest that a more automated method is necessary without excluding the human factor out of the equation. This can be achieved via the utilisation of a socio-technical approach that maps down business processes and roles, responsibilities and dependencies of tasks and considering impact as failure in states of affairs.

The problem with using stochastic probabilistic approaches is the "correct" metrics and the probabilities to estimate the magnitude and the probability of loss. By the term "correct", we mean metrics accurate and descriptive enough to capture the organization's pulse and priorities, in order to take the right threats into consideration and calculate the appropriate risks that actually make sense for the particular organization. In addition to that, as stated by the Risk Assessment Review Group Report of the NRC in 1978, for methods like these it is conceptually impossible to be mathematically complete [9]. It is an inherent limitation due to Gödel's theorem and thus they will always be subject to review and doubt as to their completeness. Whilst the problem with the qualitative approaches is that they are not specific enough with the results they provide and not customized enough to make sense. So we think an approach using a stateful model and reasoning is needed, to be able to make forward and backward inferences about scenarios that have either happened or are trying to construct them.

Furthermore, most approaches do not capture the complex interrelationships of the corporations with very few exceptions. It is in those internal relationships and structures, that most of the uncertainty and risk is lying and not in the environmental uncertainty [10]. MIT argued that the chain-of-events concept that most current risk assessment methods use couldn't account for nonlinear and indirect relationships that describe most accidents in complex systems. For this reason, our approach as stated before is that of socio-technical systems and role theory with main focus on the responsibility and dependencies modelling part, along with a rule based framework capable of forward and backward inferences, to provide impact assessment. Socio-technical systems are scalable and adaptable, capable of mapping those complex nonlinear relationships in the organizations and thus we claim that they are capable of providing better incident and impact analysis.

4. The Framework

To perform risk management in a cyber security and safety context we must understand that relationship and interactions that technical and people have within an organisation. We have defined a responsibility with reference to a state of affairs and the ability of an agent to fulfil, or maintain, it. This definition gives rise to the question of how a given agent can achieve this within the context of a socio-technical system. **Figure 1** defines a framework within which responsibilities are mapped down into tasks that are executed by agents. A task is the primary vehicle through which the state of a sociotechnical system is changed and manipulated.

Within **Figure 2** we can see that a process of mapping responsibilities into set of tasks is achieved via the performance of a set of roles. The function of a role is to define the behaviour in terms of interactions that an agent engages in when executing a task. From a formal perspective we can define the following basic sets that will be used to model and express a socio-technical system.

The mapping from a responsibility to a role is achieved via obligations. Each responsibility will give rise to a requirement for a set of behaviours that maintain, and/or achieve a state of affairs. The requirement is termed as an obligation and hence an obligation may be said to be a relationship between a given single responsibility and a set of roles. The concept behind these functions is to al-

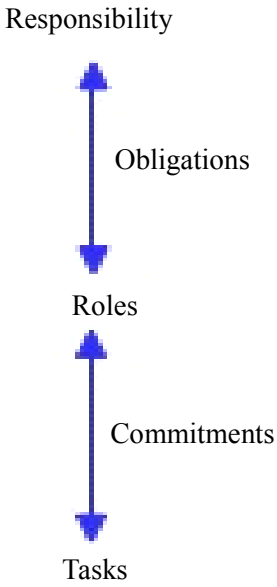

Figure 1. The framework.

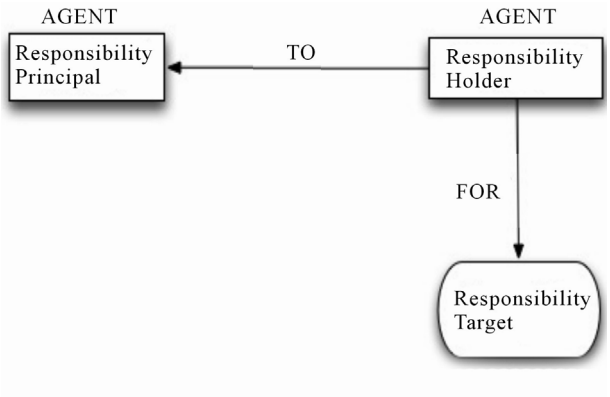

Figure 2. The responsibility relationship.

low us to express a set of necessary and sufficient conditions that must be achieved in order for a responsibility to be fulfilled.

These conditions take the form of requirements for the performance of a set of roles via a set of agents.Thus an obligation can be formally defined as a function that takes a responsibility as input and maps that responsibility to the set of roles that must be performed in-order for the responsibility to be fulfilled. For example, the doctor agent may be said to be responsible for the delivery of healthcare. This responsibility gives rise to a set of obligations for the doctor to perform a set of roles such as diagnoses illness and prescribe treatment.

The mapping from a role to a set of tasks, or actions is achieved via a series of commitments. From a philosophical perspective a commitment is to define those tasks that must be executed in order to the performance of the role to be true. Formally a commitment functions to define a mapping from a role to a set of tasks. The role of a task is to define a series of interactions that function to manipulate the state of the socio-technical system.

For example when a doctor performs the function of prescribe-treatment the doctor must first authenticate themselves to the medical patient information system, then select the patient, and finally select an treatment plan from a set of predefined intervention plans.

Within the specification of a responsibility, role and task is the concept of sequentiality. This can be used to express and represent the concept of dependability. Dependability is defined as the necessary conditions that must be achieved in order for a statement to be true. For example, in order for a doctor to perform the role prescribe-treatment, the doctor must first have made a diagnosis. In order for the action select intervention plan to be performed the action of selecting a patient must first be performed.

5. Responsibility Modelling

Responsibility modelling is the analysis and design technique of the responsibilities within an organization with purpose to explore the internal structure and the dependencies in the socio-technical systems [5,11]. It is one way of exploring the relationships amongst personnel, technical infrastructure, resources and business processes. What is interesting is that the risk associated with any deviation from the expected behaviour can be explored. In the event of an unanticipated change, a before and after analysis can determine what effect the event could have or had on the socio-technical system.

According to dictionary definitions, responsibility has two meanings:

1) The state of having a duty to deal with a certain state of affairs.

2) The state of being accountable or to blame for a certain state of affairs.

The first case has a causal connotation meaning the agent has the responsibility for doing something-making an event happen. The second case has a connotation of blame between the actual action and the results of it, but does not necessarily imply causality for the agent held accountable. For example, the parents are held responseble for the actions of their children. As a result, two types of responsibilities can be distinguished, a causal responsibility and a consequential responsibility [5,11]. For instance, each member of a crew of a ship or a plane is causally responsible for the performance of certain tasks but the captain or the pilot is always consequently responsible for the state of the ship or plane.

Responsibility is associated with agents, resources and tasks [11] as defined in the ART model later on and it is defined as the duty from one agent (the responsible) to another (the authority or principal) for the accomplish-

ment of a state of affairs, whether this is the execution, maintenance or avoidance of certain tasks, subject to conformance with the organizational culture (**Figure 1**: The Responsibility Relationship). Thus the characteristics of a responsibility consist of: who is responsible to whom, for what state of affairs, which are the obligations of the responsibility holder in order to fulfil his/her responsibility and what type of responsibility it is [5].

Causal responsibility lies effectively between one agent and a state of affairs, while the consequential responsibility is a three-way relationship between two agents and a state of affairs. In this case the agent who holds the responsibility can be held accountable, culpable or liable to the "authority" agent as seen in **Figure 1**. Apparently, the most important part of the diagram for the consequential responsibility is the relationship between two agents as the most important question to be answered is "who is responsible to whom and in what respect?". On the other hand, for the causal responsibility the most important part is the relationship between the agent and the task as the most important question to be answered is "who is responsible for this action?".

Causal responsibility is a dynamic functional relationship between an agent and a state of affairs, while consequential responsibility indicates the structural relationships within organisations and their objectives. Due to its nature, more than one agent may hold consequential responsibility; it could rest upon an entire organisation, whereas the causal usually lies upon one agent. However, the latest can also be delegated from one agent to another, while the first one is normally not capable of that although it can be transferred.

6. The Concept of Role

6.1. On the Nature of Roles

At its simplest level the concept of a role is used to define behaviour in terms of is a set of rights, duties, expectations, norms and behaviours that a person has to face and fulfil. When modelling a socio-technical system we distinguish between two major, and distinct, concepts of a role [8]. A structural role, which is a relation between agents, corresponds to the consequential responsebility aspect of role and functions to define the context of the behaviour. Examples of structural roles are supervisor-subordinate, supplier-customer, provider-consumer, and so on. This is in contrast to a functional role, which is a relation between agents, and corresponds to the behavioural and interactional aspect of role. The functions roles function to define the tasks that an agent must execute in collaboration with other agents in order to fulfil a responsibility. Hence our concept of role allows us to distinguish the following:

- Agencies and agents with associated responsibilities to other agencies and agents.
- Tasks that interact through the utilisation of resources and are structured into actions and operations.

This distinction between functional and structural roles enables us to represent and analyse the relations between functional and structural concepts and to express the way in which they operate in real organisations. A marked advantage of our socio-technical modelling technique is the way in which we can compose and decompose our models for the purposes of ascertaining requirements at various levels of agency (individual, group or organisation). Our use of the abstract term 'agency', for example, is deliberate so that we can discuss who or what corresponds to the agency.

While agents act as the primary manipulators of the systems state, agencies act as repositories for responsebilities, and structural roles act as their binding points [5]. A structural relationship serves as a means for the responsibilities to flow from one agency to another and thus responsibilities flow through an organisation.

6.2. Structural Role and Relationships

A structural role is defined by the set of responsibilities that bind to it. Each responsibility in the set in turn defines a set of roles. Each role in turn defines a set of tasks that the role holder is engaged in performing. The key to understanding the nature of structural roles and their relationships with each other is in understanding the primary purpose of the socio-technical model and the uses to which it will be put. The socio-technical model facilitates a problem solver to model, and to comprehend, how organisational attributes like responsibilities are established, flow through an organisation and are then fulfilled.

Structural relationships of the particular types and under a particular set of circumstances may be transitive in nature [5]. A requirement on the notation is that it allows us to express and describe the types of relationships and circumstances under which they are transitive. The set of structural roles that an agent can hold is divided into three types, a power relationship, a peer relationship and a service relationship. These relationships are described as follows:

- The Peer Relationships—The peer relationship is a far more subtle relationship than the power relationship, as this appears to be more social in nature than the power relationship. In a peer relationship two or more agents share a common power relationship with a third agent. It is important to note however that this power relationship should be of the same type. In a peer relationship there is no implication of enforcement, in fact, it is exactly the lack of this attribute that is characteristic of peer relationships and makes them

special. Consequently when two agents are in this relationship they may request that each other perform various services, but they lack the facility or the power to enforce execution. As a result agreement to perform a service is achieved by means of negotiation. An example of a peer relationship is that of the colleague relationship.

- The Service Relationships—In a service relationship one or both of the agents have the power to invoke the execution of a pre-defined and agreed task by another agent. This task will in some way relate to both the invoking and executing agents. An example of a service relationship is the consumer-supplier relationship, an example of which is the relationship that most people can be said to hold with an electricity board. In this relationship, one agent acts as the consumer of a service while another agent acts as the supplier of that service. The difference between a service relationship and a power relationship is that when the consuming agent is dissatisfied with the service provided by the supplying agent then the consuming agent may appeal to a third agent. It is this third agent that has the ability to enforce its judgements on both the supplying and consuming agents. A service relationship is in essence one agent invoking the performance of a predefined activity by another agent with predefined rules for the enforcement of the correct execution of that task.
- The Power Relationships—The essence of a power relationship is that one agency has the power to make and enforce demands on another agency. It is important to note however that the enforcement of these demands may be made via a third agency. An example of a power relationship is the supervisor-subordinate relationship that can exist in most organisations. There are however many different types of this relationship, for example master-slave. In this relationship the supervisor has the power to define the responsibilities and obligations that a subordinate is required to fulfil, and to judge whether or not the responsibilities were correctly discharged. The subordinate is not totally subservient to the supervisor in that the responsibilities and obligations that the subordinate is required to fulfil are defined by means of interaction between the two agencies.

6.3. Functional Roles and Interactions

Interactions link together two functional roles in different agents or agencies where each agent or agency is called a role holder. One of the purposes of Interactions is to define the behaviour that a role holder may engage in with another role holder within the context of a structural relationship. We may say that one of the purposes of a structural relationship is to define the context for a functional relationship. In defining and modelling the behaviour of a role holder, the problem solvers are in fact defining and modelling the set of allowable Interactions that can exist for that particular role holder.

Interactions aid in the identification of the organisational objects that are required to give meaning to the behaviour associated with a responsibility [12,13]. The purpose of an interaction from the perspective of its role holders is to facilitate the correct discharge of their responsibilities. The behaviour that one role holder may engage in with another takes the form of interactions. The context of these interactions is defined by the structural roles within which they are said to take place.

In the socio-technical systems model the interaction between two role holders defines how, when, where and under what circumstances responsibilities are established, flow through the organisation and are finally discharged or fulfilled. By modelling the life cycle of responsibilities we may attempt to answer a number of types of questions:

- The first type of question allows for the examination of the possible conflicts that could arise for any given role holder. The term conflict is used to denote a situation where a role holder is either obliged or responsible to perform an action, or bring about some state of affairs, whilst at the same time being obliged or responsible either not to perform the action, or not to bring about some state of affairs.
- The second type of question is concerned with the elucidation of the conditions under which an agent cannotfulfil a responsibility.
- The third type of question is concerned with the elucidation of what objects act as tokens of responsibilities.
- The fourth type of question is concerned with the delineation of the valid accesses to objects that act as tokens of either responsibility.
- The fifth type of question is concerned with the examination and comprehension of the correct creation and deletion of the objects that act as tokens of either responsibility.

7. The ART Model of Socio-Technical Systems

The core idea is to develop a rule [13]-based reasoning framework that will be able to identify the incoming threats viewing the organization from a cybernetic systems organism perspective.

The goal to be achieved is to use reasoning to bridge both the ICT infrastructure and the business processes, as a socio-technical approach, to assure that the business services are safely delivered as scheduled and the or-

ganization meets its objectives. This means that all resources/assets are available to all eligible agents, *i.e*. agents with the appropriate access rights on those resources/assets and all agents are able to execute all actions that have been assigned to them in order to fulfil their responsibilities.

In order to have a full perspective of the supply chain *i.e*. both the human factor and the complex ICT systems, we need taxonomic and ontological structures that are able to express the enterprise view in a socio-technical way, such as the one in **Figure 3**. The socio-technical model presented in **Figure 3** is comprised of a basic taxonomy and ontology of agents-resources-tasks.

The agents are the holders of responsibilities, they can be viewed as primary manipulators of the state or structure of the system and they are the only objects that can create, modify or destroy other objects, through the responsibilities that are associated with them. Actions are the operations that change the state of the system, and they are performed by agencies. All actions must induce state changes in the system that is visible to one or more agencies. The resources can be of two types: physical or logical, where physical resource are tangible objects such as servers, planes, tankers, and logical resources include information, time etc. When modelling organizations as a socio-technical system resources act either as tokens of responsibility signifying that an agency has a binding responsibility upon them, or as objects for which some agency is responsible.

The basic components of this architecture, like mentioned before, are three, Agents, Resources and Tasks:

- Agent: This is a name attached to a set of consequential responsibilities such as accountability, liability and culpability. It also allows for the expression of legal obligation.
- Resource: A Resource is an answer to "with", or "by-means-of-what" questions. For example, when a doctor makes a diagnosis they may do so by looking at an x-ray of a broken leg. Thus the x-ray functions as a resource over which the doctor has access rights.
- Task: A Task is to be distinguished from the doer of the task. Thus a task is a functional answer to "a what" question, and takes a verbal form of the specification of a functional role. For example, a doctor may perform the function role "Diagnosing Illness" when performing the task Delivery of Heath Care.

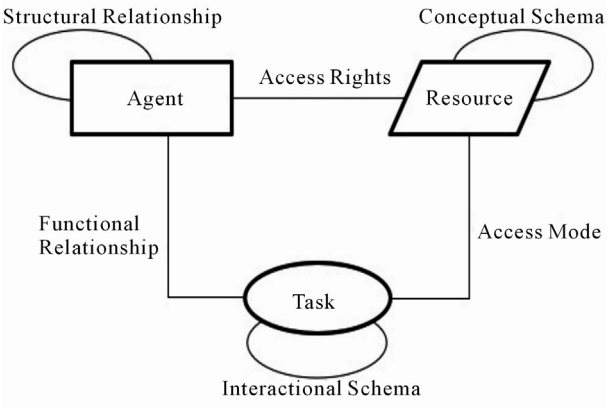

Figure 3. A socio-technical cybernetic enterprise model.

On those basic components, relationships are formed in order to describe the interactions between them:

- Task-Task: tasks interact with each other via interacttions. Such interactions are usually mediated by the exchange of resources; through direct interactions, such as interrupts, can also occur.
- Task-Resource: The relation between an task and an resource is an access mode, such as reads or writes (for information assets) or provides or consumes (for commodity assets).
- Resource-Resource: The relation between resource is what in information technology terms is called, the conceptual schema.
- Agent-Resource: The relation between an agent and an resource is an access right, such as the right: to-create, to-destroy, to-allocate, to-take-ownership-of.
- Agent-Task: The set of tasks with which an agent has some relation constitute the functional relationships of that agent and relates to the behaviour associated with that agent. For example, we can make some elementary distinctions between the functional relationships as follows:
  - The **Observer** of a task knows that it is taking place and may, or may not, know of any of the relationships which now follow.
  - The **Owner** of a task has the ability to destroy it; (the owner of an action may differ from the creator of an action, since ownership can be transferred).
  - The **Customer** of a task has the ability to change its specification.
  - The **Performer** of a task is the agent responsible for executing the tasks and performing the interactions.

By the *functional relationship* we mean two related things: a capability exists to perform the action and this capability by virtue of some legal instrument can be enforced by recourse to something outside the system (e.g. judicial)

- Agent-Agent: The set of agents with which an agent has some relation constitute the structural roles of that agent and relates to the responsibilities that bind agents together in webs that form structural schema.

The structural relationship diagrams that will be introduced in this section are normative. That is they attempt to explain what is required for a particular structural relationship in order for it to be such a relationship.

Therefore we term such a diagram an explication of

the structural relationship that it represents. When modelling the structural relationships that can exist within a socio-technical system there are two questions that the model should be able to answer. The first question is "what responsibilities are allowed to exist within the relationship?" The second question is what "socio-technical objects, *i.e*. resources etc., must exist in order to support and give meaning to the responsibilities?" It is important to note that these objects can act in several ways.

A structural relationship diagram is depicted in **Figure 3** and in this diagram there are a few things that should be pointed out. The first is that each object type is represented as a distinct shape, *i.e*. the agents are drawn as rectangles, the tasks as ovals and the resources as rhomboids. The arcs also have a condition associated with them. The task that is shown at the centre of **Figure 3** is derived from the responsibilities and obligations that a particular agency may hold. Responsibility is a three-place relationship between two agencies and a state of affairs. For this relationship we say that the agency A is responsible (in some way) to the agency B for bringing about or maintaining a state of affairs.

It is from this that the task definition is derived. A structural relationship diagram can be used in one of two ways by the problem owners. The first is to help them in their task of requirement elicitation by prompting them to ask certain questions.

For example "when and under what conditions is this relationship between two objects meaningful?" The second is in allowing them to explore the ramifications, implications and possible contradictions of policy statements.

The role and function of the responsibility dependency tree is to define the logical structures through which a responsibility is fulfilled within a socio-technical system. This graph/tree-based structure is represented in **Figure 4**. The responsibility dependency tree is a directed graph in which any two vertices are connected by exactly one simple path. In order words any connected graph without cycles is a free [14,15].

In addition, an undirected tree has the property that the path from any leaf node in the graph to the any other node in the graph is unique. This structure is a graph based formal semantic representation of dependence logic.

For the purpose of syntactic and semantic interoperability the following is a formal representation of the functional dependency between a responsibility depicted in **Figure 3** and its associated structural roles. Dependence logic is a logic of imperfect information and its semantics can be obtained from first order logic.

8. Summary and Conclusions

The methods and methodologies that have been deve-

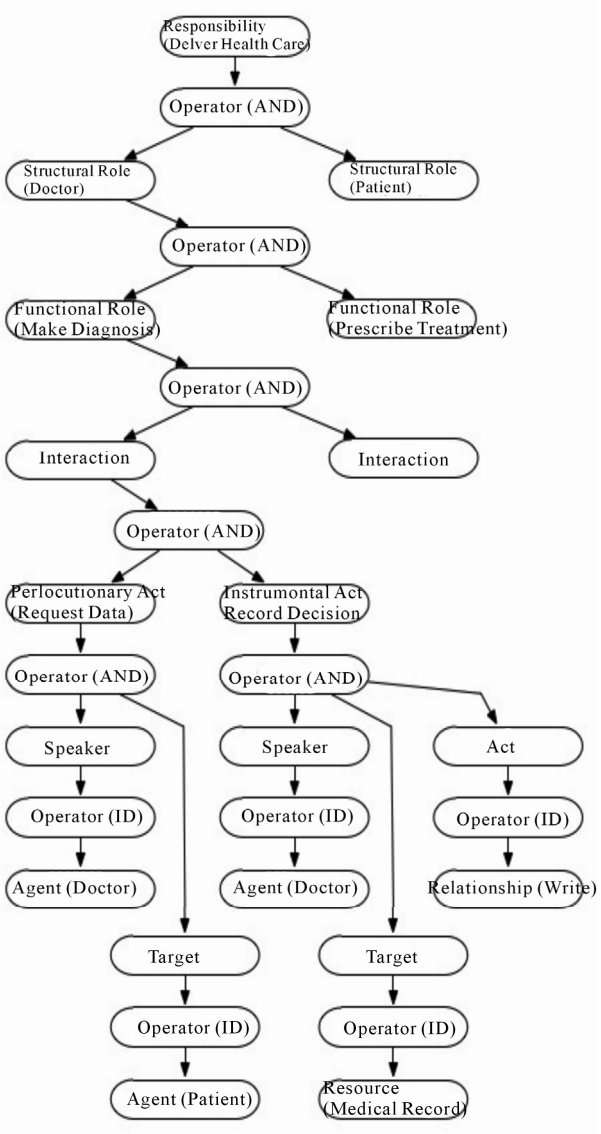

Figure 4. A responsibility dependency tree.

loped in order to manage Information Systems Security and Information Assurance have certain limitations so far, according to our opinion. They don't incorporate technology fully, but at the same time they don't include properly the human factor either [6]. They are focusing too much on probabilistic models with metrics that don't provide much help. The main target is risk analysis and predictions of events leaving out other equally important factors like impact and situational awareness. They are not complex enough or adaptable enough models to map all aspects of organisations not even the most important one the human personnel. They cannot reflect the interdependencies of assets or the correlations of data.

The RA methods were used in the past to evaluate situations or estimate the probability of an incident to occur and maybe disrupt the business processes or inter-

fere with the business objectives. The same methods are now used to evaluate the risk of security events to happen [16,17]. Those processes were designed to handle natural disaster events, accidents and anything that could make an organisation not to meet its objectives. We believe that more is needed than just an expansion of those frameworks to include security incidents and technology that was incorporated the past decades.

Our model focuses on impact; on the implications events can have on the supply chain and business processes and not on risk estimation and the prediction of events. The main objective is to be able to perform impact assessment, to provide situational awareness and feed in mitigation strategies. It provides a socio-technical stateful ontology capable to represent the complex models of organisations where humans and technology interact to achieve common objectives and it is adaptable and scalable enough to follow unpredictable evolvement. As a stateful model, it allows us to find a path between states so that we can make forward or backward inferences that will allow us to understand how to transit from a state to another and thus better analyse events, the impact, the dependencies and how to mitigate risk. The model will be executable since the engine will be running in real-time after bounding the search space with certain criteria and it supports some kind of temporality.

REFERENCES

[1] Lili Sun, R. P. Srivastava and T. J. Mock, "An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions," *Journal of Management Information Systems*, Vol. 22, No. 4, 2006, pp. 109-142. doi:10.2753/MIS0742-1222220405

[2] Collaboration, "Socio-technical Systems Engineering Handbook," St. Andrews University, St Andrews, 2011.

[3] W. M. Fox, "Sociotechnical System Principles and Guidelines: Past and Present," *Journal of Applied Behavioral Science*, Vol. 31, No. 1, 1995, pp. 91-105. doi:10.1177/0021886395311009

[4] E. Trist and K. Bamforth "Some Social and Psychological Consequences of the Longwall Method of Coal Getting," *Human Relations*, Vol. 4, No. 1, 1951, pp. 3-38.

[5] G. Dewsbury and J. Dobson, "Responsibility and Dependable Systems," Springer, Berlin, 2007.

[6] P. Periorellis and J. E. Dobson, "Organisational Failures in Dependable Collaborative Enterprise Systems," *Journal of Object Technology*, Vol. 1, No. 3, 2002, pp. 107-117.

[7] B. Aubert, M. Patry and A. Rivard, "A Framework for Information Technology Outsourcing Risk Management," ACM SIGMIS Database, New York, 2005.

[8] K. Padayschee, "An Interpretive Study of Software Risk Management Perspectives, SAICSIT'02," *Proceedings of the* 2002 *Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology*, 2002, Port Elizabeth, pp. 118-127

[9] H. W. Lewis, *et al*., "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission," National Technical Information Service, Technical Report, Alexandria, 1978. doi:10.2172/6489792

[10] R. Carvajal, "Systemic Netfields: The Systems' Paradigm Crises. Part I," *Human Relations*, Vol. 36, No. 3, 1983, pp. 227-246. doi:10.1177/001872678303600302

[11] A. J. C. Blyth, "Enterprise Modelling and Its Application to Organisational Requirements, Capture and Definition," Ph.D. Thesis, University of Newcastle, Newcastle, 1995.

[12] J.R. Searle, "Speech Acts: An Essay in the Philosophy of Languages," Cambridge University Press, Cambridge, 1984.

[13] J. J. Thomson, "Acts and Other Events (Contemporary Philosophy Series), Cornell University Press, New York, 1977.

[14] R. Nederpelt and F. Kamareddine, "Logical Reasoning: A First Course," College Publications, London, 2004.

[15] M. Blowfield and A. Murray, "Corporate Responsibility," Oxford University Press, Oxford, 2011.

[16] K. Brand and H. Boonen, "IT Governance CobiT 4.1—A Management Guide," 3rd Edition, Van Haren Publishing, Zaltbommel, 2008

[17] C Feltus, "Strengthening Employee's Responsibility to Enhance Governance of IT: COBIT RACI Chart Case Study," *Proceedings of the First ACM Workshop on Information Security Governance*, New York, 9-13 November 2009, pp. 23- 32. doi:10.1145/1655168.1655174

