Bridging the Gap between Business and Technology in Strategic Decision-Making for Cyber Security Management

Margus Välja[1], Robert Lagerström[1], Matus Korman[1], Ulrik Franke[2]
[1]KTH Royal Institute of Technology, Stockholm, Sweden
[2]SICS, Swedish Institute of Computer Science, Stockholm, Sweden

Abstract--**System architectures are getting more and more complex. Thus, making strategic decisions when it comes to managing systems is difficult and needs proper support. One arising issue that managers need to take into account when changing their technology is security. No business is spared from threats in today's connected society. The repercussions of not paying this enough attention could result in loss of money and in case of cyber physical systems, also human lives. Thus, system security has become a high-level management issue. There are various methods of assessing system security. A common method that allows partial automation is attack graph based security analysis. This particular method has many variations and wide tool support. However, a complex technical analysis like the attack graph based one needs experts to run it and interpret the results. In this paper we study what kind of strategic decisions that need the support of threat analysis and how to improve an attack graph based architecture threat assessment method to fit this task. The needs are gathered from experts working with security management and the approach is inspired by an enterprise architecture language called ArchiMate. The paper contains a working example. The proposed approach aims to bridge the gap between technical analysis and business analysis making system architectures easier to manage.**

I. INTRODUCTION

The interconnected digital world brings enormous benefits, but it is also vulnerable. For commercial entities that depend on the digital world for their everyday business activities, this means added uncertainty. Antagonistic or non-antagonistic information and communication technology (ICT) incidents could end up harming or destroying the business. This means that ICT risks must somehow be managed.

There are different ways of managing threats to ICT. Security decisions are made on different levels in an organization. High level management is responsible for setting a long term strategy and for funding activities, including budgeting resources for threat mitigation. On the operational level, employees are responsible for keeping their work environment functioning and secure, and designated employees author guidelines and procedures for how to best accomplish this (preventive security). Ex post, someone must be responsible to minimize the losses of an incident (responsive security).

In today's dynamic threat environment, cyber security decisions need to be made quickly and be based on real threat intelligence. There are many IT security risk assessment approaches available. Some of the internationally recognized risk determination standards and methods are CORAS [29], ISO 27000 [32] and Octave [8]. However, these approaches are not by themselves sufficient to guarantee an acceptable level of cyber security. First, the traditional risk determination approaches are expensive to use in terms of resources and thus tend to be repeated infrequently, despite an evolving threat landscape. Second, Taubenberger, Jürjens et al. [31] have found that internationally accepted standards like ISO 27000 suffer from decomposition problems where elements are evaluated in decomposed states and their dependencies and interlinks get neglected. Third, Taubenberger, Jürjens et al. also point out that uncertainty in risk management is assessed by the gut feeling or limited knowledge of a few people and that low impact risks get ignored. Fourth, there is an issue of the actual implementation and operation of safeguards. How can one be sure that the devices and software have been set up and are operated in an effective way? The approaches that Taubenberger, Jürjens et al. investigated did not assess the effectiveness of design and actual operation. Moreover, Posey, Robert, Lowry and Hightower [24] analyzed thought patterns of organizational insiders and found that job design, security expectations and social influence have an impact to information security. According to the authors, organizational insiders rely on each other for important information and knowledge. There is a loyalty bias towards other people from whom information is collected, for example for risk analysis, or who are involved in common business activities. There is a need for a new approach to address all these problems.

Depending on the investments made in the ICT security and monitoring architecture, the data about dependencies, interlinks and effectiveness of design and operation might be available on the operational level of an organization. There are a number of different ways in which this kind of data could be used for system security analysis. A well-known and popular cyber security analysis approach uses graph theory and can employ logical reasoning and be at least partly automated [7; 20]. This approach, called attack graph analysis, can be used to show possible attack actions for reaching single or multiple goals. According to a NIST report [28] attack graphs are a cost effective way to understand complex multistep cyber attacks. The method lets us find enterprise assets that provide certain attack opportunities. The ability of automatic logical reasoning is a clear benefit over other methods as it allows quantifying and automating security analysis. There are both commercial and free tools available for that purpose as described in [28].

While attack graph based and similar analyses that make use of operational IT data are useful, they often need a domain expert to interpret the results. This seriously limits their usefulness, particularly for communicating the results to strategic management. The attack graph-based approaches that we have seen focus on the technical level, and do not address prioritization of assets or the business processes that depend on them. This means there might be a gap between the risk management approaches that look at the business side of security (top down) and cyber security analysis that centers on technical security (bottom up).

The authors of this paper set out to investigate with a series of interviews whether there really is a gap between cyber security practices on different organizational levels and if that gap could be addressed in a data driven way, meaning extending operational level cyber security analysis to be suitable for strategic level.

This paper is divided into seven sections. Section 2 looks at related works and introduces important concepts. Section 3 describes the design of the overall study. Section 4 details the results from the interviews and the requirements for the proposed solution. A study using the requirements is introduced in section 5. Section 6 discusses the results and the study and the conclusion can be found in section 7.

II. RELATED WORK

Organizations tackle security issues in various ways. Some adopt procedures and guidelines described in standards such as ISO 27001, or methods like OCTAVE, others prefer IT governance frameworks like COBIT [15]. Then there are methods to analyze operational security, some organizations using qualitative approaches and some quantitative. Posey et al. [24] found that the beliefs of the organizational insiders can have a significant impact to the information security efforts.

A. Security management

The report about critical enterprise success factors from Caralli, Stevens, Willke et al. [6] recognizes enterprise security management as one of the important management tasks that is needed to accomplish organization's mission. The report claims that regardless of what is being secured, each organization should have a security strategy that is aligned with its business strategy. A risk based approach helps organizations to find critical areas and assets and to address the problems related to them. The report proposes adding critical success factors to the OCTAVE based risk analysis to align business drivers with security analysis, but tries not to resolve issues like accuracy and resource-wise expensive analyses.

Anderson and Choobineh [2] write that an organization needs to utilize its assets in a best possible way to accomplish its mission. Information technology assets are of high value, but also vulnerable to various threats. The authors write that as security decisions are being made at every level of organization, there must be a strategy to optimize costs and propose a method for finding an optimal security budget based on security related costs and acceptable losses. The authors investigate only how to balance ICT security budgeting.

Rowe and Gallaher [25] studied private sector security investment and implementation strategies and found that most organizations use qualitative information to decide the optimal level of cyber security investment. The drivers for the cyber security strategy originate from internal and external information sources. They found that a company could resort to a reactive strategy (as compared to a proactive one) if there is not enough information available from the public domain. About 30% of the cyber security investments where done due to regulatory incentives. Other investment drivers were business process needs, major past breaches, customer and supplier demands.

B. Security metrics

Singhal and Ou [28] write that good analysis models should include rationale for measurements and by using the measurements security analysis can be automated. They name other benefits of basing security analysis on measurable data such as accuracy, repeatability, reliability and transparency.

Jaquith [17] defines good metrics in his security book as being constantly measured, cheap to gather, expressed as cardinal number, and using at least one unit of measure. As he puts it, a good metric should be relevant enough for decision makers to take action.

Rowe and Gallaher [25] list attack and vulnerability statistics and costs associated with past attacks as two robust sources for understanding past security costs and current threat level. However, they write that this information cannot be used for predicting future attacks.

Heyman et al. [13] looked into combining security metrics based on security patterns. They combine lower level measurements such as number of authentication attempts with security objectives like auditing using user expert defined algorithms. The values of associated patterns are manually calculated and propagated to parent nodes, which are first security objectives and then requirements. When aggregating individual protection patterns, AND-nodes propagate the minimum score of child nodes, while OR-nodes propagate the maximum. The authors suggest that weights should be assigned to each security objective according to the importance of the requirement it fulfils. Similar methods are used in attack trees and graph approaches.

C. Security modelling

Attack trees and attack graphs are popular ways to evaluate organizational and system security. Attack tree approach needs human expertise, while attack graph analysis can be conducted in a semi-automated way using available data like security metrics.

According to Mauw et al. [21] attack trees are a way to categorize attacks on systems. Each node in an attack tree is a representation of an attack, while the root node is the main goal of the attack. An attack tree lists possible ways to reach the goal and attributes are used to quantify aspect like cost or impact of an attack.

Edge et al. [10] extend the concept of attack trees to protection trees. For each attack tree, the authors recommend to create a corresponding protection tree, where nodes are, instead of attacks, protections. The root nodes of both trees need to match, but the sub-trees can be different. The authors propose metrics for both tree types, which are probability of success, cost, and impact to the system. The goal of the approach is to help decision makers to determine where to spend their limited resources in order to get the best protection. The approach, however, needs human expertise and is not automated.

A report from National Institute of Standards and Technology (NIST) of United States of America [28] proposes attack graphs analysis as a cost effective way to improve enterprise security. According to the report, attack graph based models allow users to compare different network and system configurations with each other and find out if critical systems are secure against complex attacks. The report says that attack graph based methods are able to capture interdependencies of systems and are superior to traditional approaches like intrusion detection systems.

Other authors have worked with attack graphs. For example Philips and Swiler [23] applied graph theory for network vulnerability analysis already in 1998. They created a library of known attacks, network configurations, and topology information. The nodes in their solution represented the stages of attacks, while edges represented changes in the state of one or more devices as the result of an action by an attacker. The traversing between nodes was based on the defined success rate of the attacker and shortest-path algorithms.

There are several tools available for attack graph based analysis. In [30] Swiler et al. introduce a tool for attack graph based analysis based on the previous work and add algorithms that match information about attack requirements to generate an attack graph. They state that the ability of their tool to represent dynamics of system states over time (configuration change for example) is an important strength. Jajodia, Noel and O'Berry [16] developed a tool for topological analysis of network attack vulnerability (TVA). Their tool is able to reason about high level attack goals and automates labor intensive analysis of potential attack paths. The tool considers attacker exploits by rationalizing over low level vulnerabilities. NIST report [28] lists numerous other tools available for attack graph generation.

D. Cyber situational awareness

One topic that has received increased attention the past few years is cyber situational awareness, which roughly can be described as the ability to observe what is going on in one's cyber domain of responsibility, understand it correctly, and be able to draw the appropriate conclusions. A recent literature review on cyber situational awareness [12] finds two gaps similar to the strategic/operational one described in the introduction above. First, whereas national cyber security strategies all over the world call for nation-wide, large scale cyber situational awareness, this topic has not received very much scholarly attention. Second, while there is a lot of research on technology that has the *potential* to improve cyber situational awareness, e.g. intrusion detection systems or attach graph formalisms, there is comparatively little empirical research on whether this technology *actually does* improve the cyber situational awareness of decision-makers.

III. STUDY DESIGN

The first part of the study was designed as a series of qualitative interviews. One goal for interviews was to investigate security management practices on different levels in organizations and identify gaps between the levels. Another goal of the interviews was to find solutions to address the possible gaps.

The interviews were conducted with the employees of well-known Swedish enterprises, both commercial companies and government agencies. In total the representatives of 10 companies were approached, where the determining factors were the existence of strategic security planning and heavy usage of IT systems. The positions of the interviewed people include security and risk managers, security consultants, security experts, and a security tester. They work in government agencies, power, automation, and telecommunication companies. Each of these organizations had more than 250 employees. In total, seven persons were interviewed. Table 1 lists the main duties of the interviewees. Due to the sensitivity of the information revealed, the companies' names are not disclosed.

TABLE 1. MAIN DUTIES / ROLES OF INTERVIEWEES.

Organization ID	Main duties of the interviewee
Organization 1	Responsible for development projects
Organization 2	Research and development, and consulting in information security
Organization 3	Senior consultant for internal stakeholders
Organization 4	Risks and security to support other departments
Organization 4	Operational testing and consulting services to internal customers
Organization 5	Information security management
Organization 5	Information systems security management

Before this series of interviews we first conducted a pilot interview with one person from Organization 3 and based on this pre-study 16 questions were formulated. The 16 questions prepared for the interviews were open-ended and the interviews were conducted as discussions around those questions. Each interview lasted for approximately one hour. The questions can be found in appendix 1.

The second part of the study uses the results from the interviews and links the results to other studies found in the existing literature. Then design science guidelines are used to propose an improved method for assessing cyber security that would address the needs on a strategic level as well as on the operational.

IV. RESULTS

This section presents the findings from the interviews and a list of requirements that were formulated based on the findings and studying existing literature.

A. Findings from the interviews

The following section describes the findings from the seven qualitative interviews that were conducted with the employees of big international and national organizations. All of the employees are working with ICT security on everyday basis. The findings are grouped for readability purposes.

Gap between levels

a) Statements.

People working on strategic level and with strategic issues (Organizations 1, 2, 4, 5) see requirements, ISO standards, and guidelines as a central part of their work. On the operational level (Organization 4, 5) on the other hand service level agreements are deemed important and the type of incidents that the agreement covers. One interviewee (Organization 4) mentioned technical defense measures such as firewalls or encryption, and testing those measures as means of ensuring operational security. Another practitioner (Organization 1) claimed that on the business level, ICT architecture is not important, only business functions and processes are studied. One interviewee worked with ISO 17799 (Organization 5) and two others with ISO 27005 (Organization 2, 4). Representatives of one organization (Organization 5) thought that there is a gap between high level security decisions and low level operations, and that risk management only scratches the surface.

b) Interpretation.

- There is a divide between how cyber security is seen on strategic and operational levels.
- Considering the aforementioned statements we can say that there is a risk that people talk past each other about cyber security.
- On the strategic level standards of security and risk management are important, but on the operational level mostly meeting the requirements of service level agreements.

Standardization

a) Statements.

Project and product owners tend to be responsible for the security of the end products (Organization 1, 4), but often lack the appropriate security knowledge and skills and therefore rely on outside experts. Sometimes there is blatant copying of security solutions that have got accepted previously (Organization 1). In one organization (Organization 4) the security of products was said to be non-mandatory. There is low automation in risk management as it is conducted as part of team work and judgments of employees are used for decision making (Organization 4, 5). Data driven methods and autonomous agents are used to monitor suspicious behavior of key assets on the operational level (Organization 4).

b) Interpretation.

- The studied organizations had standardized security tracking through checklists and guidelines, but strategic decisions don’t seem data driven.

Asset management

a) Statements.

Departments themselves have the best overview of their assets and are part of the organization wide identification process (Organization 1, 4). Several interviewees (Organization 1, 4, 5) said that the organization wide assets are commonly identified using infrequent risk management and the lists are updated rarely, as the core assets do not change often. Classification to different security levels is used as a means of prioritizing key assets (Organization 4, 5). The representative of the organization (Organization 5) where no major incidents had happened said that gut feeling is the deciding factor for system classification. The majority of organizations (Organization 2, 4, 5) look at data and systems separately when evaluating key asset security. Representative of one of the organization (Organization 4) said that key assets are monitored using autonomous agents to find suspicious behavior, but most serious incidents have been found by testing the underlying systems. In one organization (Organization 5) the IT department was said to be responsible for meeting internal customers’ operational requirements. In the same organization the potential attack attempts get logged, but this information is rarely reported to higher management.

b) Interpretation.

- Key assets are considered important on all organizational levels.
- While each department knows its key assets, the organization wide ones tend to be identified using static infrequent risk management methods.
- Assets are categorized into different security levels and in some cases this is done only based on gut feeling.
- On operational level key assets are monitored and data is gathered about them, but not always used for strategic security analysis.

Driving forces

a) Statements

In the organization (Organization 5) that has not yet had any serious cyber security incidents, investments are said not to be incident driven. However, in an organization with a lot of incidents (Organization 4), security investments are said to be incident driven. Several interviewees (Organization 1, 4, 5) talked about the importance of internal service level agreements (SLA) that are in place to regulate the needed uptime of systems and services and the time that problems needed to get solved (the time when somebody starts working on a discovered incident).

b) Interpretation.

- There is a clear difference in the approaches used for security investments between the different organizations interviewed. This could have to do with the prevalence of discovered incidents.
- Security management in IT departments might be SLA driven.

Security concepts

a) Statements.

One stakeholder (Organization 1) said that the key concepts confidentiality, integrity and availability were not directly measured other than through incident reports and SLA breaches. According the interviewee the question of what are going to be the consequences of a breach is more important. One interviewee (Organization 2) thought that it is important to distinguish different types of attacks, because then the appropriate countermeasures can be taken. Another interviewee said that for their most critical assets availability (Organization 5) is of the highest priority and other aspects come second.

b) Interpretation.

- There is a divide in what kind of security concepts practitioners see as important.
- The consequences of a successful attack against critical assets and interlinked assets seem to be the biggest concern.

Risk management and prioritization of security

a) Statements.

Several interviewees (Organization 3, 4, 5) said that there is no acceptable threshold for accepting loss consciously, but assets are divided into different categories. In one organization (Organization 5) the security levels are information driven. One interviewee (Organization 1) said that in some rare situations security is consciously sacrificed to functionality. Another said (Organization 4) that the last thing product developers want to spend their budget on is security, but they also don’t want to accept the risk. A representative of the same organization said they know that they don’t have resources to fight against advanced persistent threats, so they are focusing more on other perpetrators like organized crime. It is not possible to penetration test everything.

b) Interpretation.

- Business stakeholders often do not prioritize security.
- Distinguishing between different types of attackers is important as it takes different amount of resources to defend against them.
- Assets need to be categorized as resources for security measures are limited.

Threat intelligence

a) Statements

In one organization (Organization 4) identifying threats was assigned to a research department. In another organization (Organization 5) the interviewee said some threat intelligence is gathered, but the major sources of threats are standards and security assessment methods. A major source of threat intelligence for that organization was mailing lists. Two organizations (Organization 4, 5) were said to have used penetration testing support for compliance and operational security evaluation. However, one representative (Organization 4) said that it was difficult to evaluate and compare penetration testing reports, especially if nothing alarming was found.

b) Interpretation

- Main sources for threats are standards and security assessment methods, but in some cases mailing lists are used.
- Some organizations use penetration testers.

B. Requirements

To understand the needs of the security experts on different levels of the organization we derived a list of requirements from the interviews, based on the needs of the interviewed people and literature. These requirements where then used to devised a cyber security analysis approach. The following principles were considered when choosing the requirements, as described by Ralph R. Young [33], a good requirement should really be needed, it should be allocatable, unambiguous, attainable, and verifiable. Other important characteristics for good requirements include completeness, consistency, and conciseness.

The requirements have been divided into four categories and are listed below.

Architecture

- It must be clear how investments in security infrastructure influence the security level of key assets.
- It must be possible to evaluate the effectiveness of design and operation of information & communication technology architecture security.
- Automation in cyber threat and risk management is required to cut cost and speed up analysis.
- It must be clear how an attack on one part of the infrastructure influences the rest.
- It must be possible to classify data and functionality to different security levels.
- It must be possible to view data, systems, and functionality layers separately.

Assets

- Key assets must be identifiable.

- The analysis must show what assets need to be defended.
- The analysis must include the asset types of data, systems, and functionality

Threats

- Different type of attacks and attackers must be supported, like APT, to be able to prioritize defenses.
- Threat catalogues must be frequently updated according to threat intelligence.

Metrics

- It must be transparent how security metrics are calculated.
- It must be possible to evaluate security characteristics such as confidentiality, integrity, and availability separately and to compare them to business priorities.
- The value of the protected assets (data, systems, and functionality) must be clear.

We use the requirements presented here as a starting point for improving our existing cyber security analysis method, with the goal to provide decision support to stakeholders on operational and strategic levels.

V. AN EXAMPLE BASED ON CYSEMOL AND ARCHIMATE

This section proposes an attack graph based approach that bridges the gap between two organizational levels, it is able to express business functionality and includes quantitative metrics. The example builds on the Cyber Security Modeling Language (CySeMoL) [14] and a well-known enterprise modeling framework called ArchiMate [19][22]. Both are introduced in the following subsections.

A. CySeMoL

Researchers at KTH Royal Institute of Technology have developed a tool for probabilistic IT architecture modelling and analysis called the Enterprise Architecture Analysis Tool [5; 18] and an attack graph based security analysis framework CySeMoL [14]. CySeMoL predicts the probability with which a single attacker or multiple attackers can compromise different parts of an organization and its IT architecture. CySeMoL models are based on organization’s structure and IT architecture and their characteristics (e.g., the attributes of the systems the architecture consists of). The results of this quantitative analysis show the likelihood of different assets getting compromised. It is an attack graph based cyber security evaluation framework that assumes that the attacker is a professional penetration tester having access to any publicly available tools that support performing cyber-attacks.

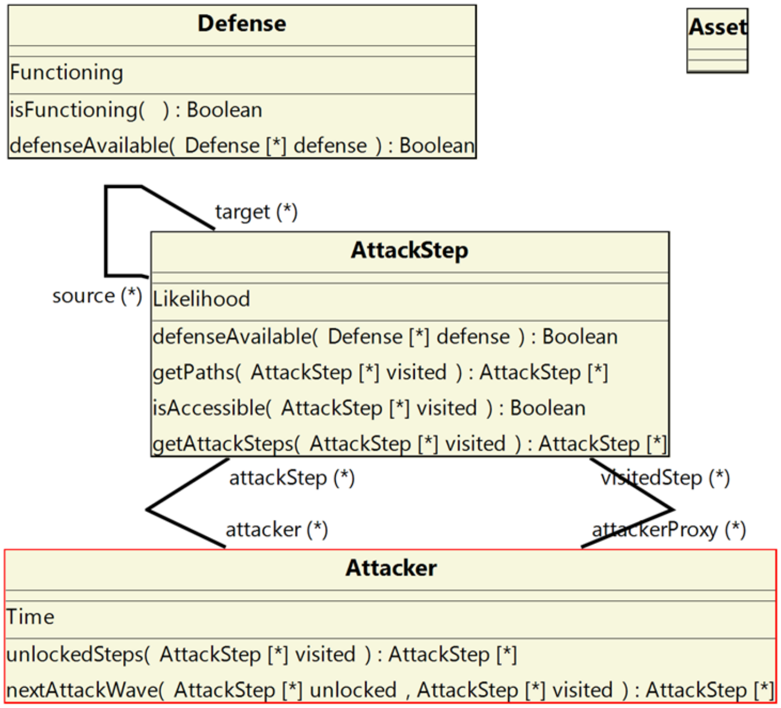
Defense
Functioning
isFunctioning( ) : Boolean
defenseAvailable(Defense [*] defense) : Boolean
Asset
target (*)
source (*)
AttackStep
Likelihood
defenseAvailable(Defense [*] defense) : Boolean
getPaths(AttackStep [*] visited) : AttackStep [*]
isAccessible(AttackStep [*] visited) : Boolean
getAttackSteps(AttackStep [*] visited) : AttackStep [*]
attackStep (*)
visitedStep (*)
attacker (*)
attackerProxy (*)
Attacker
Time
unlockedSteps(AttackStep [*] visited) : AttackStep [*]
nextAttackWave(AttackStep [*] unlocked , AttackStep [*] visited) : AttackStep [*]

Figure 1. The CySeMoL meta-metamodel.

The reasoning is based on a series of attack steps that have been specialized and grouped into enterprise assets. These assets are for example type of operating system, communication protocol, data flows. Some of the specialized attack steps are ARP spoof, access through user interface, and find critical vulnerability. The core meta-metamodel of CySeMoL is shown in Fig. 1.

B. ArchiMate

ArchiMate [19; 22] is a widely used enterprise architecture language. It is used to document and visualize enterprise elements across business and technical domains. The language divides an enterprise into three layers – business, application, and technology and defines relationships between these layers. The ArchiMate language has been compared to traditional architecture fields, but for organizations, as it helps to communicate decisions and evaluate consequences of changes. The language is supported by various tool vendors, such as Archi [3] and BizzDesign Architect [4]. ArchiMate is an established and well-documented language that is easy for business stakeholders to understand.

C. Implementation

The goal of the implementation is to bridge a gap between strategic and operational business analysis. More precisely, to make technical security analysis understandable for stakeholders who are not experts in the technical security field. Architectural, asset, metric and threat related requirements introduced in section 4 were considered during the design.

The starting point for our implementation is an attack graph analysis method CySeMoL with a predefined ontology. One reason for choosing CySeMoL is that it already meets several important requirements that we have identified. For example it allows for automated security analysis that shows how an attack on one part of the infrastructure influences the rest. Moreover, by using CySeMoL, it is possible to evaluate the effectiveness of design and operation of ICT security and as a result of calculations it shows what assets need to be defended. It also partially allows for separately evaluating confidentiality, integrity and availability.

There are a number of requirements that CySeMoL does not satisfy. For example it has deficiencies in the business layer analysis. The main problem is that with CySeMoL it is not possible to see how security problems affect business processes (on which organization's business mission might depend on) as CySeMoL's ontology consists mainly of technical assets. Another problem is that CySeMoL does not allow to include the value of assets in the security analysis. In addition CySeMoL does not show how investment in security infrastructure improves the security of the infrastructure. The absence of business layer in CySeMoL is a major deficiency that needs to be resolved for CySeMoL to be usable by practitioners working with strategic security analysis. Overcoming this gap is the main focus of our implementation.

TABLE 2. THE MAPPING BETWEEN CYSEMOL-ARCHIMATE ELEMENTS.

CySeMoL	**Archimate equal**
AccessControlPoint	System software
ApplicationClient	System software
ApplicationServer	System software
Dataflow	Communication Path
Datastore	System software
Firewall	Device
IDSSensor (IDS)	Device
IPS	Device
NetworkInterface	NA
NetworkVulnerabilityScanner	System software
NetworkZone	Network
OperatingSystem	System software
PasswordAccount	Infrastructure function
PasswordAuthenticationMechanism	System software
Person	Infrastructure function
PhysicalZone	NA
Protocol	NA
SecurityAwarenessProgram	NA
SocialZone	NA
SoftwareProduct	System software
WebApplication	System software
WebApplicationFirewall	System software
ZoneManagementProcess	Infrastructure function

We identified Archimate as a potential solution and a source of business elements for CySeMoL. Archimate got chosen because it is an established framework and open for anyone to use. ArchiMate defines a taxonomy of elements, of which the behavioral types such as functions and services can be easily integrated with an attack graph.

The logic of connecting Archimate elements to CySeMoL elements is explained as follows. Attack graph approaches, like CySeMoL, consist of nodes that represent attack steps. Each attack step usually describes the likelihood of it being successful. The successful attack steps form a path to the end goal of an attack. The attack steps can be divided into several categories depending on the type of the threat they depict like to confidentiality, integrity, or availability. For attack steps to have a meaning, each has been linked to a certain type of asset. That implies that in essence the enterprise IT assets in CySeMoL are represented by groups of attack steps and counter measures. For example an operating system links to attack steps like denial of service, access through user interface, and so on. CySeMoL's taxonomy contains around 23 of these assets and even more related attack steps. Once attack steps are linked to enterprise IT assets, we need to decide how to connect these assets to the business functions and services that run on top of them. For example, a server running an operating system and SCADA software can be connected to a function called control function.

We took the following steps to add a business layer to an attack graph approach like CySeMoL using e.g. ArchiMate concepts:

1. Group attack steps to assets. In CySeMoL this has already been done.

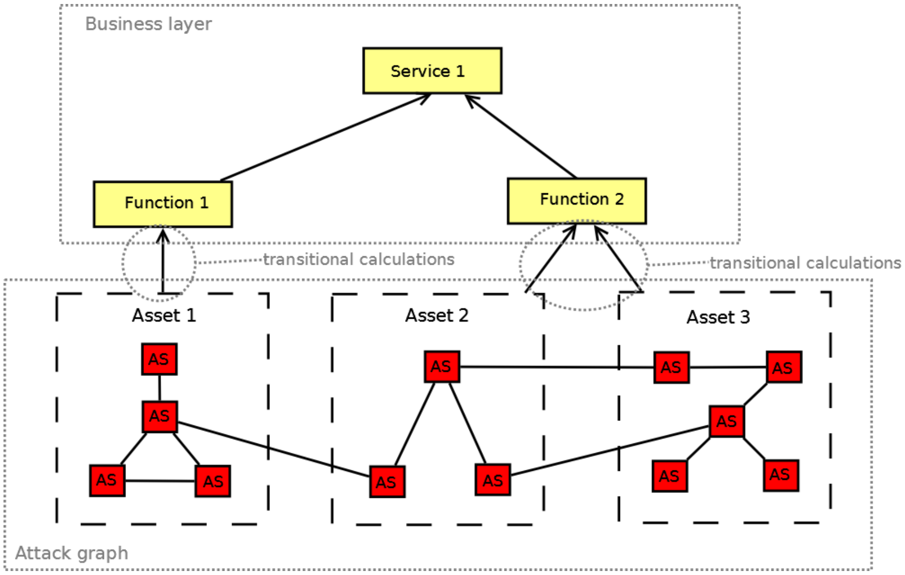

Figure 2. Mapping business layer to attack graph.

2. Map those assets to ArchiMate elements from different layers. The question to answer here is what ArchiMate element corresponds to what CySeMoL asset. Table 2 shows our attempt to do this mapping.
3. Connect ArchiMate functions and services with the CySeMoL assets as if CySeMoL assets were ArchiMate elements. For that purpose use the mappings from step 2 and ArchiMate logic of mapping functions and services to other elements. The logic of connecting CySeMoL elements to Archimate elements is shown in Fig. 2.
4. Decide metrics and create transitional calculation logic between the attack graph and the business layer.

Fig.2 consists of two parts. The first part shows the attack steps (denoted AS in the figure) that are connected with each other according to the attack graph logic and the second shows the business part, where different groups of attack steps (assets) are connected to the functions that depend on them. Functions can then be, as in ArchiMate, connected in turn to the services that rely on them. The use of Archimate business layer concepts allows us to connect security analysis to strategic business analysis and communicate problems to business stakeholders. Moreover, connecting operational assets to business functions allows not only to reason over cyber security, but also reliability of the architecture from the point of view of availability. For example if multiple systems have been set up in a redundant way to provide a certain service, then the failing of one of these systems does not influence the availability of the service provided.

An attack graph can consist of a large number of attack steps. For example CySeMoL includes more than 50 attack steps. In CySeMoL each attack graph node (attack step) can obtain a value from 0 to 100 that shows the success rate of an attacker reaching the attack step. For the abstraction to the business layer to make sense, we also need to find a way to summarize the security analysis results of groups of attack graph nodes to a business functions and services. Adding all the attributes of all attack steps to a function would be practically impossible and not very useful, there are often more than a hundred related to each function. Therefore, some kind of aggregation is needed. This aggregation is shown in Fig. 2 as the transitional calculation.

CySeMoL attack steps have different threat profiles. For example, one attack step describes denial of service, while another describes complete access to a system. One of the requirements we identified was that attacks against confidentiality, integrity and availability should be visible separately. It is a reasonable design choice as a full success of a denial-of-service type of attack is by no means as dangerous as a complete breach of a server. To achieve this distinction on the business layer, we need to group the attack steps and display the threat results in the three categories on the business layer. A simple choice would be to display the worst result in each three categories for each business function.

One of the requirements that was identified was that all of the assets should have their monetary value associated with them where applicable. That way the effectiveness of a security investment can be evaluated. Including the cost of equipment and software in the analysis allows a stakeholder to compare the security results of different architectural changes and their cost with each other. Another metric that is missing from CySeMoL is the importance of assets and the ability of being able to classify the assets to different security levels. Both of the metrics can be easily added to CySeMoL calculations and be made visible on the business layer.

As part of the design process we decided to add the following metrics to the implementation on the business level.

- Confidentiality compromised.
  The metric displays the likelihood of an attack against confidentiality succeeding in a given timeframe. The result is shown as a percentage. The highest value in the confidentiality type of attack step (graph node) group that is linked to a particular function is displayed.
- Integrity compromised.
  The metric displays the likelihood of an attack against integrity succeeding in a given timeframe. The result is shown as a percentage. The highest value in the integrity type of attack step (graph node) group that is linked to a particular function is displayed.
- Availability compromised.
  The metric displays the likelihood of an attack against availability succeeding in a given timeframe. The result is shown as a percentage. The highest value in the availability type of attack step (graph node) group that is linked to a particular function is displayed.
- Cost
  Calculated value. It is the aggregated cost of all the assets related to particular business function. It means that there must be possibility to define the cost for each asset in the model.
- Security level
  It is the security level of a function that can be set separately for each one. It shows the classification of functions according to the importance to the organization. The user can decide how many levels there are, but the amount of different levels could be for example 4. The operational assets get their security classification score from the functions they are connected to. The highest value is displayed for each asset. Later the level scores can be used to filter out some results.

Fig. 3 shows the extended version of CySeMoL, where technical assets are linked to business functions that are in term linked to a service which aggregates the underlying values. The actual metrics are hidden here for the sake of readability.

This paper aims at presenting two different contributions, one influencing the other. The first contribution is the identification and characterization of a gap between strategic level security management on the one hand, and operational level security practice on the other. Of course, one should be careful to generalize too far from our seven informants. Nevertheless, the diversity of organizations represented among our informants in combination with the literature addressing similar gaps (cf. e.g. [26], [27], [9], and [1]) hint that this problem is indeed often encountered in practice.

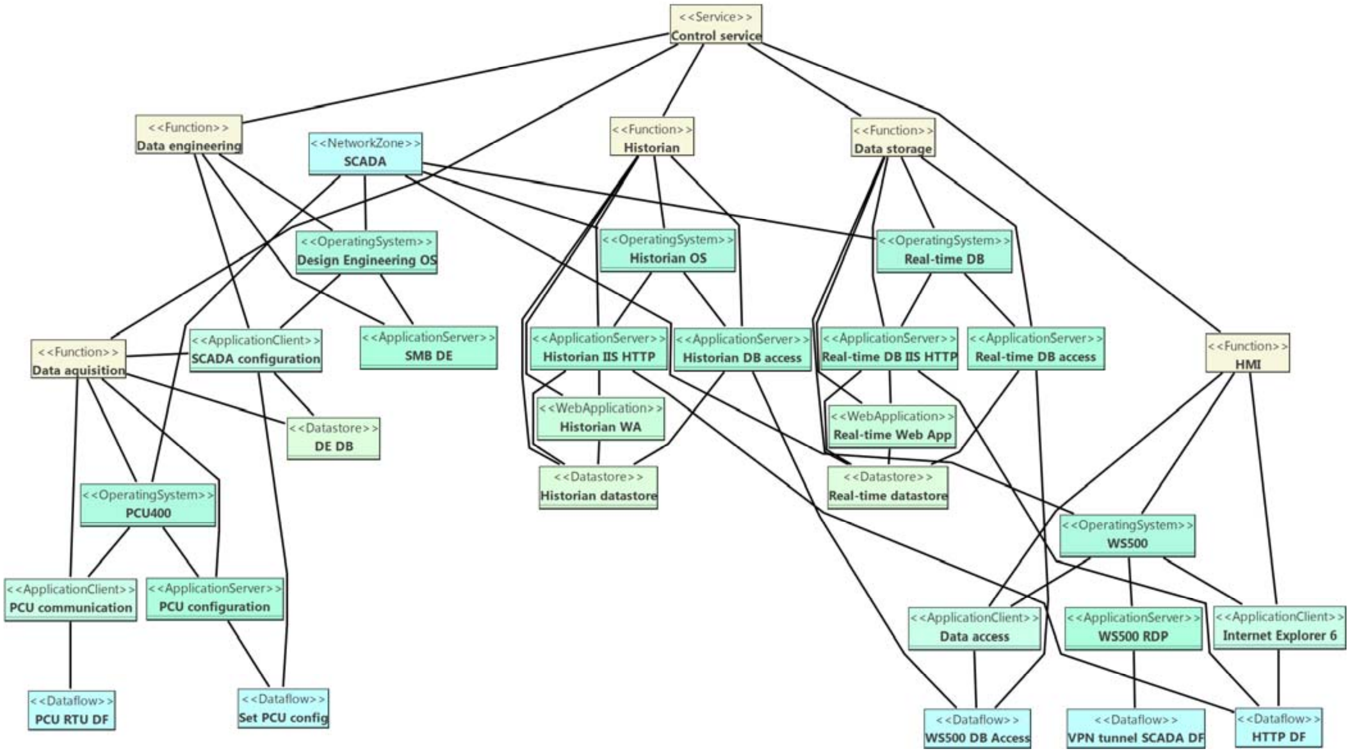

Figure 3. Extended version of CySeMoL with business functions.

VI. DISCUSSION

The second contribution is the proposed method designed to bridge this gap found, by providing a holistic common picture for stakeholders on the operational and strategic levels alike. However, this method needs to be adopted as part of the security strategy of the relevant organization in order for it to unleash its full potential. How to implement it in practice is left for future work. However, it should be noted that such future work needs to be both conceptual, i.e. spawning ideas, and empirical, i.e. investigating whether these methods work in practice or not. Above, some preliminary metrics are discussed, but again, these need to be revised and adapted by the organization itself, both in terms of validity (i.e. what should be measured) and reliability (i.e. how to measure this in a consistent way). The literature on security metrics is a good start.

The interviews were only conducted with representatives of big organizations as defined by European Commission [11]. Thus, the results do not pertain to small and medium size enterprises. Intuitively, one would assume that smaller organizations do not experience the same kind of gap, as the number of stakeholders and hierarchical levels are reduced. In the limit, a small company may have just a single person managing security, operational and strategic alike.

A limitation to the usability of the work and the example study is that the authors assume that Archimate type of business analysis methods are understandable for strategic level decision makers. In addition, the proposed method, or its usability have not been tested in a real environment with real problems, which remains future work.

VII. CONCLUSION

The authors of the paper investigate how cyber security is being managed in five organizations by interviewing 7 managers and operational experts. Based on the interviews, a gap was identified between the business oriented top down type of risk management approaches and the operational bottom-up type of cyber security analysis. The authors then come up with a list of requirements from the interviews and a literature review for a data driven cyber security analysis method that is usable by non-domain experts with business knowledge. The requirements were organized into the categories of architecture, assets, threats, and metrics.

The paper includes an example study that uses the identified requirements. The example demonstrates with CySeMoL and ArchiMate how to extend an operational data driven cyber security analysis to a business level and make it more understandable for non-technical users. Moreover, the approach makes it easy to add redundancy based availability analysis to the cyber security analysis, which was not supported in CySeMoL's earlier versions. As part of the example, CySeMoL elements are mapped to corresponding ArchiMate elements, and five new metrics are proposed. However, several identified requirements are not met by the first demonstration study. Meeting all the requirements remains future work.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Seventh Framework Program for research, technological development and demonstration under grant agreement no. 607109 (SEGRID). Also, part of it has been financed by Svenska Kraftnät (http://www.svk.se).

REFERENCES

[1] Albrechtsen, E.; and Hovden, J., "The information security digital divide between information security managers and users," Computers & Security, vol. 28, no. 6, pp. 476–490, 2009.

[2] Anderson, E.E.; and Choobineh, J., "Enterprise information security strategies," Computers & Security, vol. 27, no. 1–2, pp. 22–29, 2008.

[3] "Archi." [Online]. Available: http://www.archimatetool.com/. [Accessed: 05-Jan-2016].

[4] "BizzDesign Architect." [Online]. Available: http://www.bizzdesign.com/tools/bizzdesign-architect/. [Accessed: 15-Jan-2016].

[5] Buschle, M.; Holm, H.; Sommestad, T.; and Ekstedt, M., "A Tool for Automatic Enterprise Architecture Modeling," CAISE11 Forum, p. 8, 2011.

[6] Caralli, R.A.; Stevens, J.F.; Willke, B.J.; and Wilson, W.R., "The critical success factor method: establishing a foundation for enterprise security management," 2004.

[7] Chu, M.; Ingols, K.; and Lippmann, R., "Visualizing attack graphs, reachability, and trust relationships with NAVIGATOR," pp. 22–33, 2010.

[8] CMU, "OCTAVE." [Online]. Available: http://www.cert.org/resilience/products-services/octave/. [Accessed: 13-Jan-2016].

[9] Dai, L.; and Cooper, K., "Using FDAF to bridge the gap between enterprise and software architectures for security," Science of Computer Programming, vol. 66, no. 1, pp. 87–102, 2007.

[10] Edge, K.S.; Dalton, G.C.; Raines, R. a.; and Mills, R.F., "Using attack and protection trees to analyze threats and defenses to homeland security," Proceedings - IEEE Military Communications Conference MILCOM, pp. 1–7, 2007.

[11] European Commission, "SME definition." [Online]. Available: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/index_en.htm. [Accessed: 11-Jan-2016].

[12] Franke, U.; and Brynielsson, J., "Cyber situational awareness--a systematic review of the literature," Computers & Security, vol. 46, pp. 18–31, 2014.

[13] Heyman, T.; Scandariato, R.; Huygens, C.; and Joosen, W., "Using security patterns to combine security metrics," in ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings, 2008, pp. 1156–1163.

[14] Holm, H.; Shahzad, K.; Buschle, M.; and Ekstedt, M., "P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," Dependable and Secure Computing, IEEE Transactions on, vol. PP, no. 99, p. 1, 2014.

[15] ISACA, "COBIT." [Online]. Available: http://www.isaca.org/knowledge-center/cobit/pages/overview.aspx. [Accessed: 14-Jan-2016].

[16] Jajodia, S.; and Noel, S., "Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response," in Algorithms, Architectures and Information Systems Security, 2007, pp. 285–305.

[17] Jaquith, A. Security Metrics: Replacing Fear, Uncertainty, and Doubt. 2007.

[18] KTH ICS, "EAAT," 2014. [Online]. Available: www.ics.kth.se/EAAT. [Accessed: 01-May-2014].

[19] Lankhorst, M., Enterprise Architecture at Work: Modelling, Communication and Analysis. Springer Berlin Heidelberg, 2012.

[20] Lippmann, R.; and Ingols, K., "An annotated review of past papers on attack graphs," Lighthouse, no. March, 2005.

[21] Mauw, S. and Oostdijk, M., "LNCS 3935 - Foundations of Attack Trees," pp. 186–198, 2006.

[22] Open Group, "ArchiMate 2.1 Specification," 2013. [Online]. Available: http://pubs.opengroup.org/architecture/archimate2-doc/. [Accessed: 01-May-2014].

[23] Phillips, C.; and Swiler, L.P., "A Graph-based System for Network-vulnerability Analysis," Proceedings of the 1998 Workshop on New Security Paradigms, pp. 71–79, 1998.

[24] Posey, C.; Roberts, T.L.; Lowry, P.B.; and Hightower, R.T., "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," Information and Management, vol. 51, no. 5, pp. 551–567, 2014.

[25] Rowe, B.R.; and Gallaher, M.P., "Private Sector Cyber Security Investment Strategies: An Empirical Analysis *," no. March, pp. 1–23, 2006.

[26] Seeholzer, R., "Information Security Strategy: In Search of a Role," 2012.

[27] Sherwood, J., "SALSA: A method for developing the enterprise security architecture and Strategy," Computers & Security, vol. 15, no. 6, pp. 501–506, 1996.

[28] Singhal, A.; and Ou, X., "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs," 2011.

[29] SINTEF ICT, "CORAS." [Online]. Available: http://coras.sourceforge.net/. [Accessed: 15-Jan-2016].

[30] Swiler, L.P.; Phillips, C.; Ellis, D.; and Chakerian, S., "Computer-attack graph generation tool," Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01, vol. 2, 2001.

[31] Taubenberger, S.; Jürjens, J.; Yu, Y.; and Nuseibeh, B., "Problem Analysis Of It-Security Risk Assessment Methods – An Experience Report From The Insurance," pp. 259–270, 2011.

[32] The ISO 27000 Directory, "The ISO 27000 Directory." [Online]. Available: http://www.27000.org/. [Accessed: 15-Jan-2016].

[33] Young, R.R., Effective requirements practices. Addison-Wesley Longman Publishing Co., Inc., 2001.

APPENDIX 1

Interview questions

Common

1. What is your experience with strategic architectural and security decisions?
2. How is cyber security tracked in your department/organization?
3. How is compliance tracked?
4. What are the impacts of the results of good or bad decisions (good/bad). Examples?

Strategic vs. operational

5. How do operational and strategic cyber security decisions differ in your opinion?
6. What kind of architectural or security decisions do you need to take in regards to

- plans,
- personnel,
- procedures,
- guidelines,
- technology?

7. When evaluating cyber security what kind of analysis levels are more important in terms of technical level, functional level, data level? How are these levels used in cyber security analysis?

Metrics

8. Have key assets (the most valuable ones) inside organization found? How?
9. What kind metrics are relevant for strategic architectural decision making? How would you characterize these metrics (single, composite etc.)?
10. What kind of metrics do you use for cyber security decisions? How do they relate to key assets?
11. How usable are metrics based on confidentiality, integrity, availability for strategic decisions? What other metrics do you find useful?
12. How actionable must the cyber security metrics be?
13. Are there any thresholds in place in terms of acceptable security loss versus costs on cyber security?

Tools

14. What kind of tools have you used are using for strategic decision support in cyber security?
15. Which tools do you find the easiest to use for this?
16. How does cyber security management relate to other, general, risk management in your organization?