Mission-Centric Risk Assessment to Improve Cyber Situational Awareness

F. R. L. Silva
Athlone Institute of Technology
Athlone, Ireland
f.rogelio@research.ait.ie

P. Jacob
Athlone Institute of Technology
Athlone, Ireland
pjacob@ait.ie

ABSTRACT

Cyber situational awareness has become increasingly important for proactive risk management to help detect and mitigate cyber attacks. Being aware of the importance of individual information system assets to the goal or mission of the organisation is critical to help minimise enterprise risk. However current risk assessment methodologies do not give explicit support to assess mission related asset criticality. This paper describes ongoing efforts within the H2020 PROTECTIVE project to define a practical mission-centric risk assessment methodology for use across diverse organisation types.

KEYWORDS

Cyber Situational Awareness, Risk Assessment, Mission Dependency Model, Asset Criticality

ACM Reference Format:
F. R. L. Silva and P. Jacob. 2018. Mission-Centric Risk Assessment to Improve Cyber Situational Awareness. In *ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany.* ACM ICPS, Article 257, 8 pages. https://doi.org/10.1145/3230833.3233281

1 INTRODUCTION

Individuals and enterprises - commercial, military and even national security bodies - face constant, ongoing, dangers from cybercrime. Given the escalation in the number and diversity of attacks it can be difficult for organisations to know where to turn to defend themselves. Performing comprehensive information security risk management is therefore a fundamental requirement to enable organisations to effectively marshal their resources to battle cyber-security threats. *Risk assessment* is a vital piece of the overall risk management process. It is defined as *"the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system,"* [19].

Risk can be assessed from a number of different perspectives. Among the most common are *threat-centric* which focuses on how an adversary could exploit technical and non-technical aspects of a system to produce adverse effects and *vulnerability-centric* which aims to gauge how risk might arise to systems from an identified set of vulnerabilities within the system through exploitation by relevant threat events. Well known risk assessment methodologies based on these approaches include ISO/IEC 27005 [14], NIST SP 800-30 [20] and Octave Allegro [1]. In recent years, research to improve an organisations cyber-situational awareness has increased. This has generated renewed interest in a *mission-centric* approach to risk assessment, first popularised in the military domain [18]. Mission-centric assessment focuses on the mission or business objectives, that must be achieved despite the presence of threats. Mission-centric assessment enables an organization to quickly identify critical risk relationships between mission objectives and information system assets and so greatly assist to establish effective cyberattack defences.

Current risk methodologies [14][2][20] provide, at best, limited support for mission centric risk assessment. This arises both because they primarily adopt threat and/or vulnerability oriented assessment approach and also because they are assessment *frameworks* and as such are more concerned to define an end-to-end approach to risk assessment rather than detail specific procedures for particular steps. One seeming exception is Mission Oriented Risk and Design Analysis (MORDA) [17] a risk assessment developed by the US Navy. Under the hood, however, the methodology is threat-centric. Furthermore, it is not applicable to a general commercial environment and it is large and complex and, consequently, very "heavy" to use. This heaviness is a problem also for the already mentioned processes.

Although, there is growing research interest in mission-centric risk assessment, very little has been published to assist practitioners apply the technique in a practical way, particularly, to capture and express mission dependencies. The Asset Management domain review provided by the US-CERT [22], as part of the Cyber Situational Review, give guidelines to establish and express mission dependencies. A somewhat similar approach is described by the Risk-to-Mission Assessment Process (RiskMAP) [23]. This methodology defined a multi-layered dependency model to express and reason about dependencies between missions and elements of the information security system including assets. Other notable contributions to mission impact modelling include [15] and the body of work in [16]. None of these approaches, however, solves the problem of giving "real-world" security practitioners a comprehensive approach to applying mission centric risk assessment. In particular, two main problems exist:

- there is no comprehensive method with tool support to model and capture dependencies.

ARES 2018, August 27–30, 2018, Hamburg, Germany

ACM ISBN 978-1-4503-6448-5/18/08…$15.00
https://doi.org/10.1145/3230833.3233281

- the lower levels of the mission dependency tree are both large in scale and dynamic which makes the manual capture of dependencies difficult if not impossible.

Within the H2020 project PROTECTIVE [3], we are developing a mission-centric risk assessment methodology and toolset. In this status paper, we report on our ongoing work efforts to date to address the first of the above issues. We describe a structured mission-centric risk assessment methodology to enable simple capture of mission dependencies and detail a generic, technology independent and extensible mission dependency model. Section 2 describes current approaches to risk management and assessment and highlight shortcomings for mission-centric risk assessment. Our mission dependency model is described in Section 3 while Section 4 describes our proposed risk assessment methodology . Section 5 describes related work and the Section 6 summarises the paper and point to future research.

2 CURRENT RISK ASSESSMENT APPROACHES

Information security risk needs to be considered as a component of the overall risk, or enterprise risk, environment of an organization. In the commercial world enterprise, risk is defined as "*the extent to which the outcomes from the corporate strategy of a company may differ from those specified in its corporate objectives, or the extent to which they fail to meet these objectives*" [7]. A semi-formal way to express risk for a particular threat t is

$$R = f(tl, i) \tag{1}$$

where *R= risk, tl= likelihood of a threat occurring* and *i = impact of an attack.*

In this context, an information system forms part of the "*resources and organizational structure*" supporting the "*activities of the enterprise*". Consequently, information security risk is a component of enterprise operational risk due to the potential impact to information systems - and hence to supported enterprise activities - arising from internal and external information security threats.

In order to understand the degree to which current risk management methodologies support mission-centric risk assessment, we carried out an in-depth analysis of three of the leading approaches i.e.:

- The NIST Guide for Conducting Risk Assessments, NIST SP 800-30 [20].
- The ISO Information Security Risk Management Standard, ISO/IEC 27005 [14].
- The SEI Octave Allegro Risk Assessment Process, CMU/SEI -2007-TR-012 [2].

These three risk management (RM) methodologies are widely used and referenced as benchmarks in both the theory and practise of RM. NIST SP 800-30 and its sibling NIST SP 800-39 are used to conduct risk management activities in a broad spectrum of enterprise, critical infrastructure and other public service provision on a global basis. ISO/IEC 27005 is also used globally to frame RM in multiple domains. OCTAVE Allegro is part of a family of RM methodologies that includes its more comprehensive siblings OCTAVE and OCTAVE-S. OCTAVE Allegro is a lightweight RM methodology that focuses on information assets. It thus provides a useful complement and contrast to the more comprehensive ISO and NIST approaches.

From this analysis, we derived the generic RM taxonomy in Figure 1 that categorizes the main steps in risk management and maps the related steps in each methodology to the sub-parts of the taxonomy. Areas relevant to mission-centricity are shaded in the diagram. Risk assessment (RA) is our main area of interest and so is broken into more detail while risk response and risk monitoring are not considered any further in this paper. We have defined three steps in the RA process i.e.:

- *Preparing for RA* - this is setting the organisational context and scope of the RA i.e. it establishes the basic criteria for identifying and evaluating risk in the organisation and reflects the activities described in the previous section.
- *Conducting the RA* - this is the actual activity of identify the risks and evaluating their impact on an identified subset of the organisations operations.
- *Communicating the Risk* - the results of the RA are communicated to stakeholders. This step is not explored here.

The underpinning methodologies of our taxonomy do address, to varying degrees, the desirability to relate the organization mission to the information system assets. ISO/IEC 27005 is vocal is this regard but it is still not sufficient for hands-on application. OCTAVE Allegro does give guidance for mission-centric assessment for information assets - "*information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information*" [2]. It informally ties mission criteria to information assets and onwards to *information containers* - "*where information assets are stored, transported, or processed.*". As such then, OCTAVE Allegro is a good starting point for a methodology to derive mission-centric risk assessment. However, OCTAVE Allegro has a number of significant drawbacks including:

(1) it does not cover all the impact dependency layers that are likely needed for a general risk assessment approach. In particular, it omits the business process layer. This, in part, is a consequence of the design philosophy to keep the OCTAVE Allegro approach simple.
(2) the information asset container approach is high level and it is unlikely to be useful for very large and dynamic Information Technology (IT) infrastructures.

However, these issues have been examined by other researchers. The authors of RiskMAP decomposed the risk assessment into:

- *Define a business (or mission) model.* In this model, organizational objectives (e.g., military missions, business objectives) are identified and their relative importance assessed. These are then mapped to business processes and information assets. When completely developed, the business model identifies and assesses the value of the organization's process and information assets in a way that allows business decision-makers to understand how the relative values are assessed.
- *Define a system (or network) risk model.* Technical assets include systems, subsystems, and components (as configured hardware, software, and telecommunications). Identification of technical assets can be done manually (e.g., by examining

network diagrams and inventories of equipment and software licenses) and/or by using automated tools (e.g., network scanning, vulnerability scanning, configuration checking).
- Link the two models to complete the assessment process.

We have at this stage most of the main elements needed to define a high level mission-centric risk assessment process. However, one key element that needs further investigation before we are able to complete the process is to elaborate the mission-dependency metamodel.

3 MISSION DEPENDENCY METAMODEL

Creating a mission dependency metamodel is an essential requirement in order to be able to complete a mission-centric risk assessment. The model defines the dependency layers and entities that allow risk assessors to trickle down enterprise risk to information systems risk. A number of such models have been proposed in recent years, [23], [15] and [8], with dependency layers varying according to the particular goal of the individual contributions. Suggested layers include:

- Hardware (HW) (on a device e.g. hard-drive).
- Network (physical connectivity).
- IT services (i.e. layer 4 services e.g. SSH).
- Applications.
- Information Containers (e.g. databases).
- Information Assets (logical).
- Cyber Assets.
- Software (physical image, library etc.).
- System artifact (process, file, network socket).
- Business Process.
- Operational Tasks.
- Business Objectives.
- Mission.

It can be inferred from this list that there is a high degree of overlap amongst many of the proposed layers. Yet, none of the proposed models is entirely reusable for our purpose and so we have defined a mission dependency metamodel to meet our needs. The metamodel includes many of the elements of previous work but it is structured to be more generally applicable to handle the diversity of both organization types and of underlying information system infrastructure i.e. the metamodel is more flexible in its usage than existing approaches.

The metamodel is described in Figures 2 and 3. Figure 2 shows the main information security entities while Figure 3 shows the dependency layers and relationships. Only the principal dependency entities are shown in Figure 3. The shaded entities in Figure 2 indicate parent nodes in the inheritance hierarchy.

As with RiskMAP, the model is structured into an *Enterprise Model* and a *IT Model*, recognizing the two major steps of the risk assessment process. The model is further decomposed into four dependency layers with the first two as part of the enterprise model and the second pair part of the IT model. These are

- *Mission Layer* - this layer defines the enterprise and organizational entities for the the model. The essential entity at this level is *Mission* which captures the enterprise level business objectives of the organization.
- *Operational Layer* - this layer captures the principal business functions of the organization expressed as *Business Process* and *Information*. The business process artifact captures business functions and services essential for the organisation to function operationally while the information artifact models the various information assets that the business uses. Each of these entities can be decomposed into lower level sub-entities as required. A important distinction of our model is that this layer may be omitted altogether if so desired as may be the case for risk assessment in small organizations.
- *Application Layer* - this layer captures the main information system services that form the backbone of organizations business. The principal entity here is *IT Service* . The model is flexible to allow slightly different interpretation of this entity e.g. an IT service could be a so-called *microservice* that in turn offers one or more network services such as HTTP or SSH.
- *Infrastructure Layer*- this layer captures the software, hardware and networking entities that host and execute the IT services. The *Node* entity models both computing and networking elements - both physical and virtual while the *Software* entity captures all the various elements that constitute the software fabric for the application.

The relationships all imply dependencies though some of these may be indirect e.g. the 'ConnectedTo' relation may string together a number of elements along a path between two services indicating a dependency that may not be initially visibly obvious.

Using the above model, we identify the following dependency types:

- Inter layer Mission to Operational layer - this involves relationship between the Mission entity and the Business Process(BP), Information entities.
- Intra layer Operational layer between i) BP entities, ii) Information entities and iii) BP to Information entity.
- Inter layer Mission to Application layer i.e. Mission to IT Service.
- Intra layer Applications layer i.e. IT Service to IT Service.
- Inter layer Application to Infrastructure layer i.e. IT Service to Software (SW).
- Intra layer Infrastructure layer i.e. SW to SW, SW to Node and Node to Node.

Node to node includes execution dependencies e.g. a server may hosts Virtual Machine (VM) that in turn hosts a Docker container as well as physical connectivity dependencies via network nodes.

The model as presented is work-in-progress and several additional elements are needed before it can be considered complete. These include the addition of elements to capture the AND/OR nature of dependency relationships i.e. an entity may depend on a number of other entities and its ability to operate may depend on the correct functioning of ANY one of the group or it may require the correct functioning of ALL of the members of the group. Nor does the model in its current form address the question of weighting nodes and relationships and propagating dependencies down the model to determine asset criticality. Work is ongoing within the project to complete these tasks.

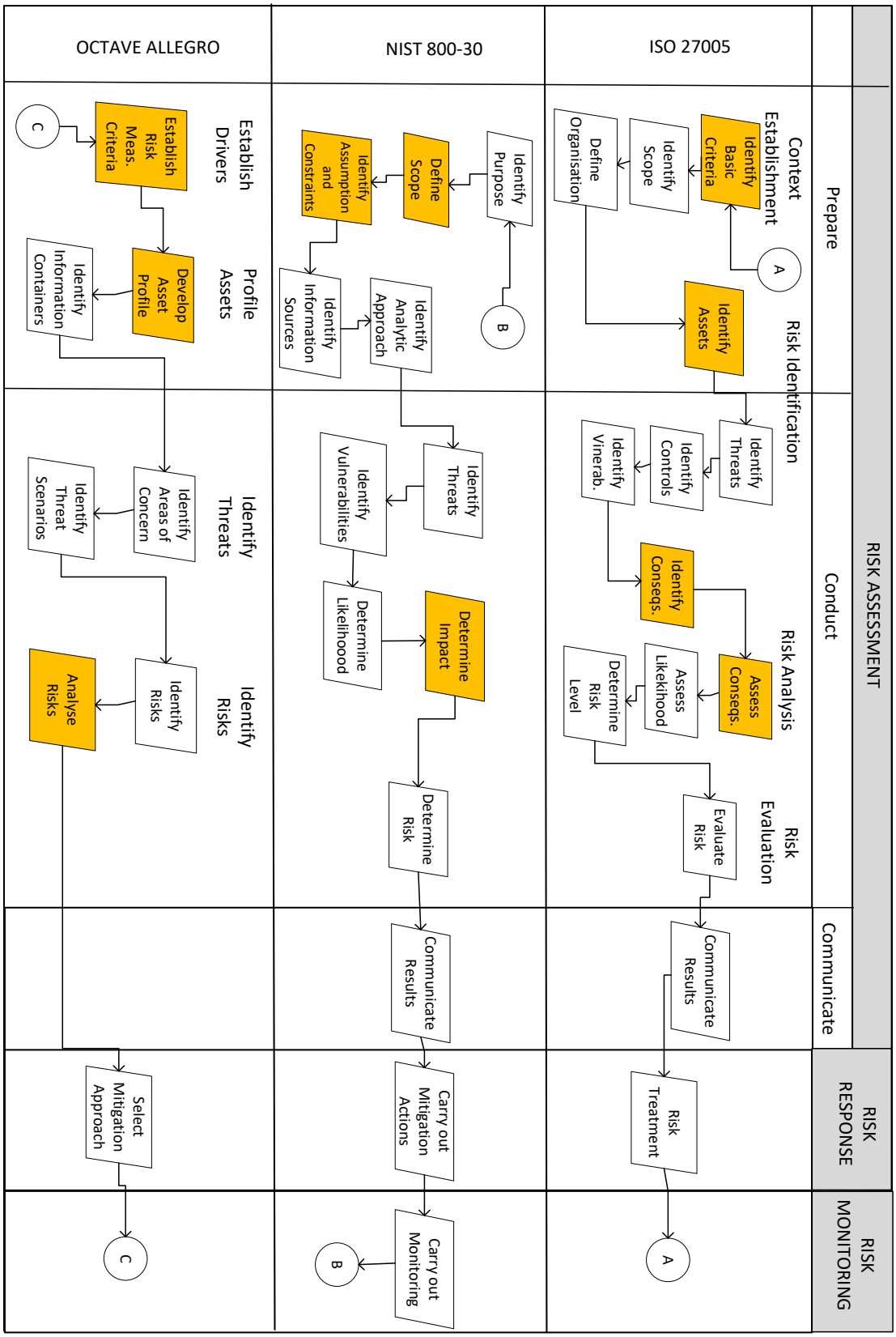

Figure 1: Risk Assessment Model Comparison.

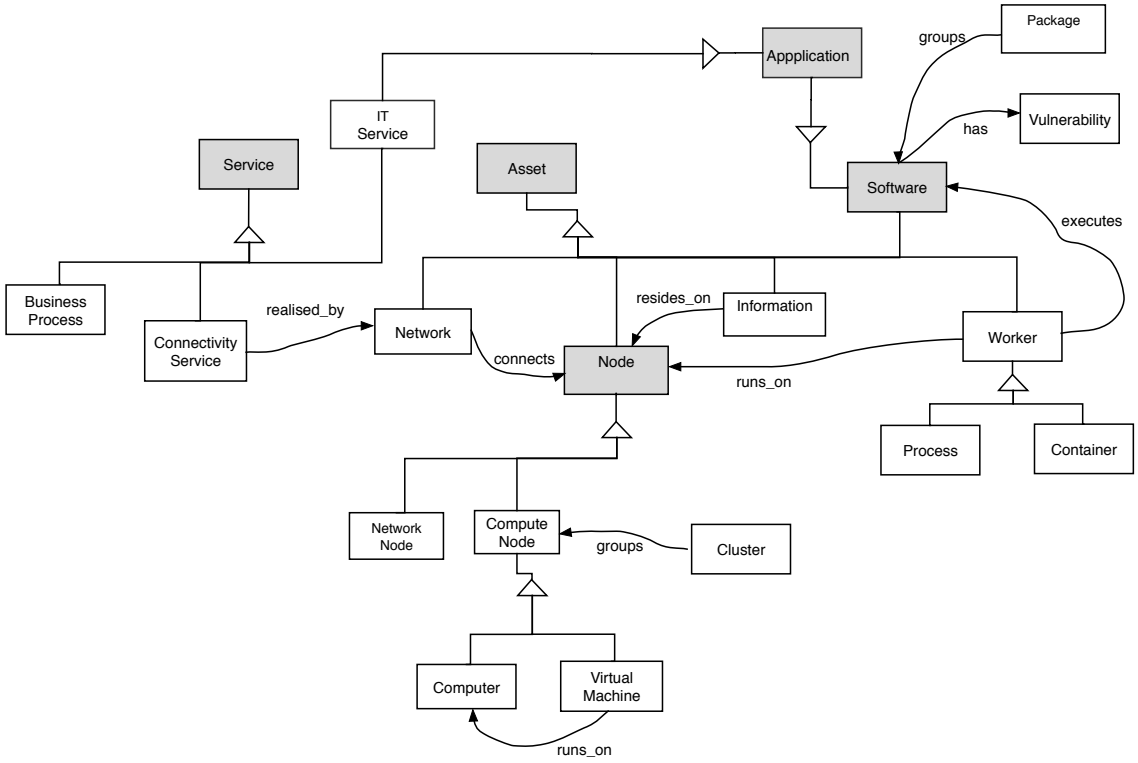

Figure 2: Metamodel IT Entities

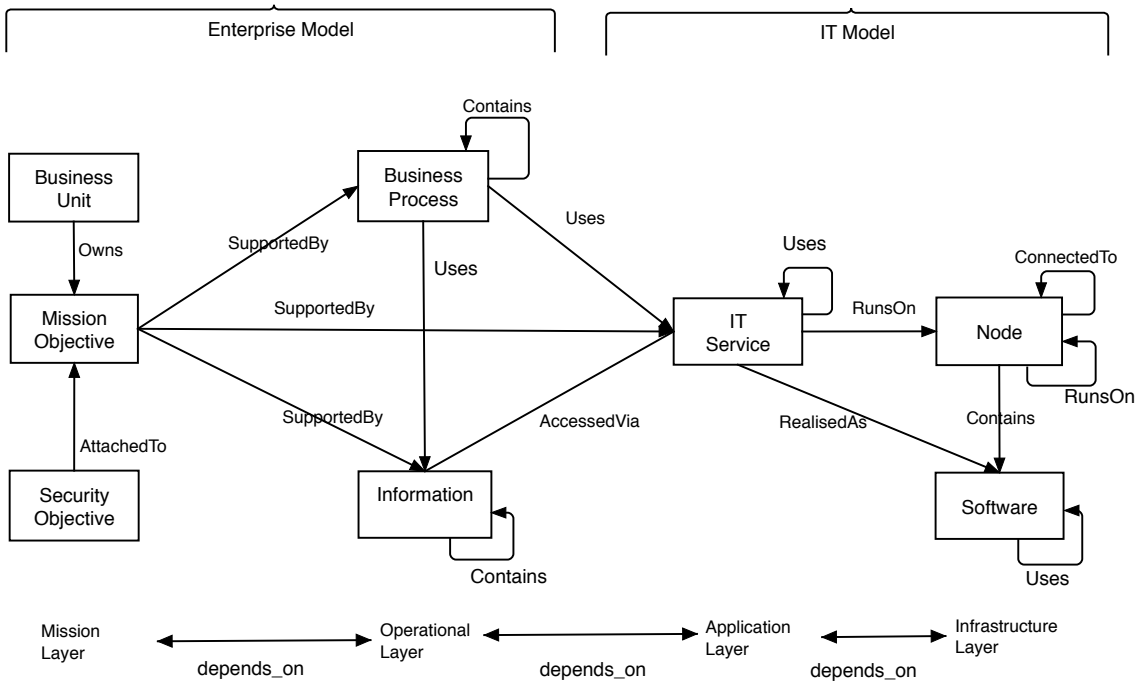

Figure 3: Mission Dependency Metamodel

Decoupling the Enterprise and IT models also recognizes that the models may be compiled by different means.

4 PROPOSED RISK ASSESSMENT APPROACH

Based on the above metamodel and the risk management taxonomy of Figure 1, we can now enumerate the principal activities to conduct a *mission centric risk assessment*. These are described in the risk assessment flow below. The flow is a composite of cherry-picking from existing models as well as addition of own elements.

4.1 Risk Assessment Preparation

Enterprise Model

(1) Identify and assess the relative importance of organisation mission/strategic objectives if this is not already done.
(2) Identify the risk measurement criteria that are most important to the mission and business objectives [9]. These criteria define a set of impact areas (e.g. damage to reputation) impact types (damage to reputation with customer; damage to reputation with suppliers) and the impact scale (low, medium, high, etc.). The risk management methodologies provide examples. Impact areas may/may not be related to mission processes e.g. reputation may apply to a number of mission functions whilst production line productivity may be specific to a single process. It may also be necessary to prioritise the impact areas.
(3) Identify the approach to express overall risk. Overall risk is often shown as a table/matrix that contains an estimate of the attack severity weighed against business impact/asset value - see Annex E in [14] or Appendix I in [20] for examples.
(4) Identify the scope of the risk assessment i.e. which parts of the enterprise will be assessed.
(5) Identify and prioritise critical processes that support the organisation mission.
(6) Identify and profile the information systems assets that support the mission processes. The information asset profile describes its features, characteristics and the criticality of each information asset to the operational processes it supports.
(7) Identify the network/system nodes and the relative criticality of each node to the information asset supports.
(8) The business model is the outcome from these steps. One of the main expressions of the business model is the generation of an impact dependency tree . This shows the risk/impact relationships across the multiple organisation level from Figure 2. It will enable mission values to be propagated down the resultant dependency tree in order to help determine asset criticality. While NIST SP 800-30 and ISO/IEC 27005 acknowledge the possible need to define dependencies, OCTAVE Allegro does so only implicitly by acknowledging that information assets have a value based on their support for mission objectives. Further while, ISO/IEC 27005 gives some guidelines on how to estimate asset valuation/criticality, NIST SP 800-30 only mentions that criticality may be determined from a business impact analysis. RiskMAP, on the other hand, has very explicit guidelines on how to identify and map the dependencies.

IT Model

(9) Define the threat context i.e. identify the threat sources and threat events that may be expected to occur in the system and which can be used as a exemplary taxonomy to carry out the assessment.
(10) Define the vulnerability context i.e. identify exemplary vulnerabilities and define a scale to assess their severity. This step might optionally be included as part of the threat identification step.

4.2 Conducting the Assessment

IT Model

(11) Identify likely threats to the specific information systems, technologies, or environments of operation that are of particular interest. This is conducted by defining threat scenarios using information from threat catalogues, system experts, end users, etc. The output from this activity is a list of threats ranked by relevance.
(12) Identify vulnerabilities - The primary purpose of vulnerability assessments is to understand the nature and degree to which organizations, mission/business processes, and information systems that are vulnerable to threat sources identified in the previous step. The output from this activity is a list of asset associated existing vulnerabilities together with an estimate of their severity.
(13) Determine the asset impact and asset risk on the network node or the information asset hosted on the node. The asset impact is derived from a consideration of identified vulnerabilities and its effect of the attack on the confidentiality (e.g. disclosure), integrity (e.g. modification) or availability (e.g. degradation) of the asset. A single vulnerability may have different impact values for each of these categories. The asset risk is calculated by estimating the likelihood of occurrence of the associated threat that exploits the vulnerability - note that the asset $risk = assetimpact * threatlikelihood$ (where $0 \leq likelihood \leq 1$) i.e. asset risk is a proxy for asset impact.

4.3 Link the Models

(14) Map the network level impacts to major operational activities and possible consequences using the business model i.e. the risk is propagated up the business model dependency tree - vs. down the business model tree to determine asset criticality. Assessment is thus related to asset criticality based on the business impact analysis.
(15) Prioritise the risks (severity of consequences) based the relative importance of the business or the priority of the associated business risks (expressed over impacts areas).

In effect in this step we have converted the equation (1) equation into

$$MissionRisk = f(AssetRisk, MissionImpact) \tag{2}$$

or equivalently

$$MissionRisk = f(AssetRisk, AssetCriticality) \tag{3}$$

This latter equation makes clear a critical fact on the nature of impact in information system risk management. There are two different types of impact:

- Mission impact - which is the impact/injury to part(s) of the organization mission arising from injury to the asset.
- Asset impact - which is injury to an asset that affects the confidentiality, integrity or availability of the asset.

Asset here can either be i) the hardware node and/or its systems software or ii) the information asset supported by or contained on the asset. Some activities may be performed as part of the preparation stage of each RA activity while some may be performed only once - it may also be organisation dependent. Note that we have included only those steps from our derived risk taxonomy here that are relevant for the hybrid mission/asset oriented assessment.

5 RELATED WORK

Significant early work on mission impact modelling was carried out in the military domain. Grimalia [10] identified the need for a well-documented information-asset based risk management methodology that quantifies mission dependence on information assets. He points out the binding between an information-asset and a mission may be dynamic and highlights the temporal value of information and captures the dependency between mission and asset via a "state" variable that contains confidentiality, integrity and availability attributes.

A number of researchers have explored used the concept of a *cyber-terrain* (CT) for mission based risk assessment and a number of tools have been developed to support this effort [11]. A CT is defined as "*systems, devices, protocols, data, software, processes, cyber personas, or other network entities, the control of which offers a marked advantage to an attacker or defender*". One such researcher is Jakobson [15] who introduced a number of model types to capture the various aspects of security attack impacts. He describes the CT as consisting of three subdomains, HW, SW and services encapsulating intra and inter-subdomain dependencies. The CT possesses a certain *operational capacity* (OC) which is a measure of its ability to provide a mission with the required resources and services. OC applies for each component and the whole CT, 0 implies no capability while 1 implies full capability. Jakobson also introduces a conceptual graph based attack model to capture the relationship between cyber-attacks and mission impact.

He also models missions as goal directed sequential or parallel flow of mission steps. Parallel branches can be forked by either OR or AND semantics. Each step can be another flow, or mission or (elementary) task. Missions are time dependent - they have a start, stop time and a duration. The mission depends on all steps being executed in the prescribed order. The state of the overall mission depends on the state of its individual tasks. He combines these various models into an Impact Dependency Graph, a multi-layered model that captures the dependency relationships between all the various concepts in the domain.

Musman and colleagues [18] also investigate an approach for Cyber Mission Impact Assessment (CMIA) for military missions. Although, the scope of their investigation is quite similar to Jakobson, their approach is at a higher level of detail and centres around the use Business Process Modelling Notation (BPMN) to describe and develop mission models. Their choice of process modelling reflects the dynamic, temporal and task-sequential nature of military missions

As described earlier, RiskMAP [23] is a hybrid mission/asset-centric modelling approach and, it was an early venture in this direction and many of the RiskMAP modelling concepts were incorporated into later works. Heinbockel [12] describes a mission dependency model that is very close to our own work and includes an implementation of the model in Neo4J. However, the work is proprietary and the implementation is not publicly available. Further, reflecting its military provenance, the model does not capture the complexities of software infrastructure.

Dai [4] proposes a *situation knowledge reference model* to assist with mission impact and asset damage assessment which contains four layers including Operating System artefacts (e.g. network sockets, files, processes etc.) as well as code level tracing. He suggests a number of approaches to construct, or discover, intra and inter layer dependencies. Workflows can be generated explicitly, as e.g. with a tool such as iGrafx [13] or implicitly via business process/workflow mining from system logs e.g. [5]. Similarly, the service layer human knowledge may be used for explicit dependency generation or automated service dependency tools may be used e.g [9]. Operating layer dependencies are discovered by capturing and mining system calls. Including socket call as system objects enables inter-host dependency tracking. Dependencies at the instruction layer are discovered by taint analysis and cross layer dependencies to the Operational System (OS) layer can be discovered at the same time [4]. Cross layer dependencies between the workflow and Service layers can be discovered from network traces and mining workflow logs.

Sun and some other members of this same team reuse a number of the ideas to take a slightly different approach to analysing impact, [21]. He describes a *Mission-Task-Asset (MTA) map* to associate mission with composing tasks and associated assets. The missions are the business processes used within the enterprise and the tasks are the application/services and the assets are the system objects such as files, processes etc. Each task (or service) is assumed to having a specific pattern/signature of system calls and tasks (and hence the dependency graph) can be retrieved by mining the system object dependency graph. Missions are assumed to be few and well known, and their dependency on each other and the underlying tasks to be "not a real issue". The major addition of Sun is the proposed use of Bayesian Networking (BN) for mission impact assessment. The input of the MTA based BN is intrusion evidence collected from various sensors and its output is the probabilities of interesting security events such as a system object or task being compromised or tainted by an attack.

Amico [6] conducted an interdisciplinary workshop on how to map relationships between cyber assets (hardware, software, data) and the users, missions, business processes and other entities that depend on those assets. The work provides a useful model and definition of the main entities involved in mission impact assessment but does not capture the layering aspects of the model.

6 CONCLUSION

In this work, we have described initial and ongoing activities within the PROTECTIVE project to derive a workable methodology for mission-centric risk assessment. We have analysed several current leading risk management methodologies and identified shortcoming in this regard. We have combined the best of these models with leading academic research and our own insights to define a comprehensive methodology for mission oriented risk assessment.

Much work remains to be done, however, to complete this task. The risk assessment model is very high level and in some cases serves as a framework to be specialised. We intend to develop this further into a more applied methodology and are focusing on the OCTAVE Allegro methodology as a staring point. We will augment OCTAVE Allegro with a business process and service modelling approach as well as a procedure to aggregate the assessment of individual assets to give an enterprise level risk assessment.

We will also enhance the mission dependency model, significantly, as indited in earlier section, to boost the AND/OR combinatorial semantics as well as enable inter layer and intra layer asset ranking using different algorithms such as e.g. PageRank.

Finally, we are developing an associated tool set to realise the mission dependency model to allow capture and reasoning over multiple asset types. This work is not described here but is well under way.

ACKNOWLEDGMENTS

This paper has received funding from the European Union Horizon 2020 research and innovation programme under grant agreement No. 700071 for the PROTECTIVE project.

REFERENCES

[1] Christopher J. Alberts, Audrey J. Dorofee, James F. Stevens, and Carol Woody. 2001. Introduction to the OCTAVE Approach. Retrieved may 20, 2018 from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546

[2] Richard A Caralli, James F Stevens, Lisa R Young, and William R Wilson. 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

[3] Protective Consortium. 2018. PROTECTIVE: Proactive Risk Management through Improved Cyber Situational Awareness. Retrieved May 20, 2018 from https://protective-h2020.eu

[4] J. Dai, X. Sun, P. Liu, and N. Giacobe. 2012. Gaining Big Picture Awareness through an Interconnected Cross-layer Situation Knowledge Reference Model. In *IEEE International Conference on Cyber Security ICCS 2012.*

[5] A. K. A. de Medeiros, W. M. P . van der Aalst, and A. J. M. M. Weijters. 2003. Workflow mining: Current status and future directions. On The Move to Meaningful Internet Systems. In *Proceedings of CoopIS, DOA, and ODBASE.* Rhodes,Greece.

[6] A. DeAmico, L. Buchanan, J.Goodall, and P. Walczak. 2010. Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships between Cyber Assets, Mission and Users. In *Fifth International Conference on Information Warfare and Security.* Ohio.

[7] Gerry Dickinson. 2001. Enterprise Risk Management: Its Origins and Conceptual Foundation. *Geneva Papers on Risk and Insurance - Issues and Practice* 26, 3 (jul 2001), 360–366. https://doi.org/10.1111/1468-0440.00121

[8] S. Noel et al. 2011. Analyzing Mission Impacts of Cyber Actions (AMICA). In *Proceedings of the Workshop: Assessing Mission Impact of Cyberattacks (NATO IST-128).* NATO, Istanbul, Turkey, 80–86.

[9] X. Chen et al. 2008. Automating network application dependency discovery: Experiences, limitations, and new solutions. In *Proceedings of the 8th USENIX conference on Operating systems design and implementation.* 117–130.

[10] M.R. Grimalia and L. W. Fortso. 2007. Towards an Information Asset-Based Defensive Cyber Damage Assessment Process. In *IEEE Symposium on Computational Intelligence in Security and Defence Applications.* Honolulu.

[11] J. Guion and M. Reith. 2017. Cyber Terrain Mission Mapping Tools and Methodologies. In *Proceedings of the 2017 International Conference on Cyber Conflict (CyCon U.S.).* Denver, 21–26.

[12] W. Heinbockel, S. Noel, , and J. Curbo. 2016. Mission Dependency Modeling for Cyber Situational Awareness. In *Proceedings of the Cyber Defence Situation Awareness (STO-MP-IST-148).* NATO, Sofia, Bulgaria.

[13] igrafx.com. [n. d.]. iGrafx process modelling tool. Retrieved June 7, 2018 from www.igrafx.com

[14] ISO. 2011. Information Technology- Security techniques-Information security risk management,.

[15] G. Jakobson. 2011. Mission Cyber Security Situation Assessment Using Impact Dependency Graphs. In *4th International Conference on Information Fusion.* Chicago.

[16] A. Kott, C. Wang, and R. F. Erbacher. 2014. *Cyber Defense and Situational Awareness* (1st. ed.). Springer, Switzerland.

[17] Donald L. Buckshaw, Gregory Parnell, Willard L. Unkenholz, Donald L. Parks, James M. Wallner, and O Saydjari. 2005. Mission Oriented Risk and Design Analysis of Critical Information Systems. 10 (March 2005).

[18] S. Musman, M. Tanner, A. Temin, M. Elsaesser, and L. Loren. 2011. Computing the Impact of Cyber Attacks on Complex Missions. In *Proc. Intl. Systems Conference (SysCon).* Montreal.

[19] NIST. 2011. Managing Information Security Risk. NIST SP 800-39 (March 2011).

[20] NIST. 2012. Guide for Conducting Risk Assessments - Information Security.

[21] X. Sun, A. Singhal, and P. Liu. 2015. Who Touched My Mission: Towards probabilistic Mission Impact Assessment. In *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense.* Denver, 21–26.

[22] US-CERT. [n. d.]. Asset Management. https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf

[23] J. Watters, S. Morrisey, D. Bodeau, and S.C. Powers. 2009. The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat Confidentiality Issues. *Mitre Corp. Technical Report* 09-2994 (2009).