Development of A Capability Maturity Model for Cyber Security in IIoT Enabled Supply Chains

Roy A Isbell[1], Carsten Maple[2], Bil Hallaq[*] Hugh Boyes

Roy Isbell, Cyber Security Centre, WMG, University of Warwick, Coventry, UK
Carsten Maple, Cyber Security Centre, WMG, University of Warwick, Coventry, UK
Bil Hallaq, Cyber Security Centre, WMG, University of Warwick, Coventry, UK
Hugh Boyes, Cyber Security Centre, WMG, University of Warwick, Coventry, UK
ri@warwick.ac.uk
cm@warwick.ac.uk
bh@warwick.ac.uk
hb@warwick.ac.uk

Keywords: CYBER, SUPPLY CHAIN, SECURITY, IIoT, MATURITY

Abstract

Many companies understand how their immediate suppliers and key customers access their information systems and handle their data, however they are often blind to how these immediate suppliers and key customers procure and transfer data, services and components with other companies down or up the supply chain. This means that the provenance and control of data, information and components cannot be guaranteed, introducing risk that is not understood and therefore not managed. The integrated cyber supply chain is an enlargement of the cyber-attack surface for the organisation adding to the risk and complexity of ensuring that the organisation is suitably protected. This paper identifies a process to develop situational awareness of the organisations cyber supply chain and the identification of metrics that identify key aspects of the connections with suppliers, to assist in the development of a model for organisations to assess their level of maturity with respect to cyber security of the supply chain.

1 Introduction

The use of engineering to drive down costs and improve productivity has been an ongoing business exercise since the first Industrial Revolution. The improvements in global transport and communications have a significant impact on the way organisations establish their supply chains in order to take advantage of cheap labour and access to raw materials. This resulted in the development of geographically diverse supply chains. The use of cyber technology to further improve communications and the ability to incorporate cyber technology into the engineering world has led to a rise in the development and use of automation across all sectors of industry, especially manufacturing.

One result of this drive towards autonomy is the development of complex supply chains that are increasingly utilising cyber technology with a consequent increase in the risk of cyber-attack as the interconnection of systems provides a larger attack surface for threat actors to exploit. The aims of this paper are to understand the use of cyber in the Supply Chain and to develop a methodology that allows organisations to investigate their cyber supply chain risk and complexity and to effect better targeted controls, resulting in a reduction of the possible adverse effects and an increase in the overall resilience of their cyber supply chain.

This problem is exacerbated as supply chains become more global and complex due to the desire to outsource and reduce costs, and as organisations identify new affordable locations to produce their products or deliver services. Supply chains are becoming more integrated and are leveraging technology to better collaborate and coordinate decisions along the supply chain, as organisations look to optimize the supply chain by integrating production, inventory, and logistical aspects along the chain.

2 Background

The development of a Capability Maturity Model for Cyber Security in the Supply Chain (CMM-CSSC) is a multi-phase project. The first phase was to look at the current status of Capability Maturity Models and their applicability to the cyber supply chain. The second phase is the development of a methodology to map the cyber supply chain. The third phase is the testing and refinement of the methodology through engagement with industry and the final phase is to use the methodology to establish a capability maturity model. This paper represents phase 2 of the project, the development of a practical methodology to map the cyber supply chain with a view to using the data gathered in the eventual creation of a capability maturity model.

2.1 The Increasing Threat Landscape

Utilisation of the supply chain has been identified as one of 10 methods of attaining initial access to compromised systems [1]. This coupled with an increased prevalence of lateral movement once access has been achieved [2], increases the risk of compromise for organisations that have multiple points of interconnection. By way of example there have been several targeted intrusion campaigns affecting the telecom sector with the aim of gaining access to a larger base of users for cyber espionage operations [1].

Organised groups, with various motivations from financial gain to industrial espionage, are conducting global attacks with increasing sophistication [1]. As such, many organisations

who have established, or are looking to establish, global supply chains, are becoming targets for these groups.

2.2 Risks to the Cyber Supply Chain

The growth of connectivity, volumes of data and information flows, along with greater digital integration of the supply chain (e.g. Industry 4.0, Additive Manufacturing and Servitization of Assets), increases the potential for cyber-attacks [1] and brings greater focus on the need for the contracting organisation to ensure that there is the appropriate level of cyber readiness and resilience across their supply chain. The changes being implemented as we move from rapid prototyping techniques to additive manufacturing see a greater interconnectivity and a blurring of the overall manufacturing process and supply chain boundaries.

By way of example, to contract with CNI level organisations, their Tier 1 suppliers, very often need to meet a Cyber Essentials or Cyber Essentials Plus [3] level of cyber awareness and hygiene. In the UK, the Ministry of Defence has introduced a tiered approach [4] to cyber security for defence suppliers, with 5 levels based on the assessed cyber risk of the suppliers' activities.

However, there is limited visibility for the Primary Contracting Organisation (PCO) on how the Tier 1 supplier is ensuring the same level of cyber maturity across the Tier 2, Tier 3, Tier n or ad hoc suppliers. In fact, there appears to be a general lack of appetite for the PCO to mandate similar readiness and resilience further down the supply chain [5]. Programs such as "Cyber Essentials" and "Cyber Essentials Plus" [6] provide a framework for assessing and reporting cyber security readiness but lack sufficient detail or guidance in relation to cyber security, and associated data and information management, across the entirety of the self-asserting organisations supply chain.

3 Developing Cyber Supply Chain Situational Awareness

In order to understand the risks and threats to the cyber supply chain we need to develop an overall situational awareness. Situational Awareness comes from "understanding all elements in an environment within a volume of time and space" [7]. To apply this to the cyber supply chain we need to understand all aspects of cyberspace within the context of where cyber is being used.

Utilising business process models provides much of the detail required to identify and understand the information required and a specification exists for Business Process Model & Notation (BPMN), available from the Object Management Group (OMG) [8]. Software tools have been developed from this specification and are available to purchase. Investigation into the various tools available is outside of the current methodology development and the subject of future work. It is expected that many organisations may have already deployed a tool to model their business processes and anticipated that the notation common between tools may be employed for use in this methodology for repeatability.

Understanding the relationship between the business and the use of cyber is key to developing an overall situational awareness. Technologists must understand the business if they are to maximise the benefits to the business from utilising technology, and businesses must recognise that cyber security is a cost of doing business when utilising technology to reduce costs or improve productivity.

3.1 Developing a Detailed Cyber Supply Chain Map

The development of a cyber supply chain map is about establishing a Situational Awareness of the cyber connectivity between the Primary Contracting Organisation (PCO) and their suppliers through the subsequent levels of the cyber supply chain. This cyber connectivity is directly related to the business processes that the cyber connectivity supports and their criticality to the overall business operations. The combination of the two provides for development of a prioritized list based on the business impact should the connectivity be compromised in any way.

3.2 Supplier Types and Data Groups

The clear majority of organisations continue to work with a traditional linear contracting model, utilising two-way contracts that flow down through their supply chains. In such contractual environments, the Primary Contracting Organisation (PCO) contracts with a Tier 1 supplier, who then contracts with a Tier 2 supplier and so on to Tier 'n'. The limitation of such a model is the reduced visibility of potential risks and threats across the entirety of the supply chain.

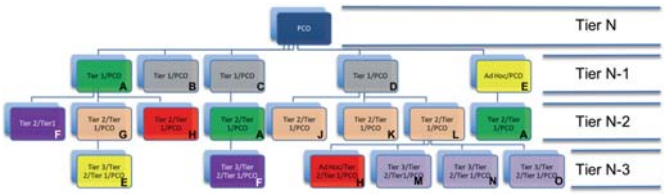

Figure 1 Complex Supply Chain Mapping

The larger the organisation the more complex the supply chain and the more 'Tiers' the chain may have. In addition, the organisations that make up the supply chain may not just have a one to one relationship with the PCO. Figure 2 shows a 3 Tier supply chain in a top down format; however, the relationships between the organisations may not be on a 1-2-1 basis. For example, supplier A(Tier N-1) [Green] is also a (Tier N-2) supplier to both C(Tier N-1) and E(Tier N-1), whilst H(Tier N-2) [Red] is also an Ad-Hoc(Tier N-3) supplier to L(Tier N-2). Also F(Tier N-2) [Purple] is a (Tier N-3) supplier to G(Tier N-2) supplier. These non-linear contractual connections may also be with different parts of the PCO and as such adds to the complexity of the cyber supply chain map.

This complexity requires greater granularity in order to identify the PCO cyber connected supply chain and the identification of business-critical links that require additional security and resilience measures to ensure continuity of supply. Only once the top level of the organisational cyber supply chain map has been created are we able to delve deeper into the lower tiers of the supply chain to develop a complete map for an organisation.

The end-to-end supply chain comprises vendors, producers, wholesalers, retailers and end clients with the intention to synchronize demand and supply [9]. For the purposes of this work we use these definitions to differentiate between them in our mapping of the cyber supply chain.

Supplier Type	Definition
Vendors	Organisations that supply products or services used for both Business to Consumer (B2C) and Business to Business (B2B) relationship.
Producers	Organisations involved in the production of goods and includes in this case manufacturers, though in some cases manufacturers are not always the end product producers.
Wholesalers	A middleman organisation that resells producer goods, may also be known as a distributor, especially used in locations where the producer may not have a presence.
Retailers	An organisation that normally sells in small quantities directly to the end user or consumer.
End Clients	Are organisations or Individuals who receive the goods or services provided by the organisation

Table 1 Supplier Types [9]

Using these definitions [9] helps to differentiate the relationships with suppliers and by extension establish whether the supplier is at the end of a chain from a cyber perspective, and if not, the detail required for discussion with the supplier to ascertain what further cyber related links may exist.

Identification of common supplier types within the above definitions allows a more granular classification schema to be utilised within the cyber supply chain map. The following relationship types have been established for the initial classification schema:

Figure 2 Supplier Types [Adapted from [9]]

Recognising that organisations may have supplier relationships that share data from industrial processes utilising operational technology and or data sharing from information technology we looked to categorize the data types being transferred between the PCO and the supplier. We therefore further subdivided the data exchange into data groups using the following table:

Data Group	
Operational Technology	**Information Technology**
Sensor Information	System Data
Device Programming	Network Data
Telemetry	OS Info
Communications Data	User Data
Actuation Status Information	Application / Application Data
Design Data	

Table 2 Data Groups

By defining and recording the data groups we are able to further analyse where multiple instances of the same data type is being shared giving rise to the possibility to utilise standardised protection and control measures for similar data types removing some of the bespoke elements that might otherwise be deployed.

3.3 Connectivity

Describing the connectivity relationship between the PCO and the suppliers at all levels is essential to understanding the overall complexity of the cyber supply chain.

3.3.1 Connectivity Attributes

The connectivity has a number of different attributes that allow a connection to be broken down into sub-class attributes [10] providing for each link to be categorised according to these attributes.

Category	Sub-Category	Class	Sub-Class
Connectivity	Mechanism	No Connectivity	Local Display
			No Local display
		Wired	Electrical
			Fibre Optic
		Wireless	RF
			Light
			Sound
		Physical	Pressure
			Mechanical
	Nature	Real time	
		Not Real Time	
	Initiations	By Device	
		By Receiving Device	
		Either Device	
	Protocols	Infrastructure	
		Discovery	
		Data Protocols	
	Link Security	Authentication	Manual
			One-way
			None
		Identification	Mutual
			One-way

			None
		Encrypted	Full
			Data only
			None

Table 3 Connectivity Categorisation [10]

3.3.2 Levels of Connectivity

Interconnectivity may be achieved at different levels and as such the level of interconnectivity between the PCO and each supplier is added to provide an additional degree of categorisation [11]. The model looks at 5 levels of integration for the business process:

1. Enterprise Integration – focused on functional processes
2. Corporate Excellence – at the intra enterprise level
3. Partner collaboration – begins the working with selected suppliers and customers
4. Value chain collaboration – through various cyber technologies
5. Full network connectivity – through integrating systems to the benefit of all parties

The higher the number, the greater the level of connectivity. Each link in the cyber supply chain link should be categorised.

3.3.3 Connection Status

Each supplier connection also has a status depending on whether or not it is New, Pending, Active, Disconnected or Old. We developed this status metric to ensure that the onboarding of new suppliers and their cyber supply chain connection is appropriately included within the maturity model. It ensures that a process exists for onboarding suppliers and that any supplier that is no longer supplying the PCO is removed, the data/information flow stopped, and any retained data/information is destroyed according to the PCO corporate policy.

3.3.4 Information Sharing & Threat Intelligence

Establishment of good communications between PCO and Supplier are essential for managing the security of the supply chain, especially where it is a 'Full Network Connected' [11] cyber supply chain. Sharing of intelligence, reporting of incidents and security alerts are key to maintaining an overall operational awareness picture of the cyber supply chain. Agreements have to be reached with the supplier on what is to be reported, by whom and when, this will also include any notifications that the supplier receives from their suppliers as communications channels are established further down, across or up the cyber supply chain.

3.4 Connectivity

How well a country is prepared is an indicator in assessing of how suppliers from that country are also prepared based on national posture. As part of the ITU overall support to its 193 Member States within the framework of the Global Cybersecurity Agenda, the 'cyberwellness' profiles are being presented as factual representations of each nation state's level of cybersecurity development. It aims to provide a clear perspective on the current cyber security landscape based on the five pillars of the Global Cybersecurity Agenda namely legal measures, technical measures, organization measures, capacity building and cooperation. [12].

Attack vectors are also known to differ by region and as such need to be considered when assessing cyber connected suppliers from different parts of the globe. By understanding the techniques used in the region allows the targeting of prevention and detection resources [1].

Utilising the cyberwellness score for the country where the supplier is resident [12] along with weighting scores with respect to controls against the known attack techniques used within the region will provide not only a score for maturity, but also an assessment against the relevant controls utilised to protect the data/information exchange.

3.5 Standards

The use of standards in assessing a suppliers' approach to cyber security may be considered a superficial assessment and not comprehensive or targeted enough to ensure the correct controls have been implemented relevant to the context of the cyber relationship. A survey by the UK Department for Culture Media and Sport (DCMS) [13] showed that only 13% of all businesses require suppliers to adhere to security standards and where standards are being used less than 50% of businesses require compliance with either PCI DSS [14] or ISO 27001-2017 [15].

The information security standards considered in the DCMS survey do not fully address wider cyber security aspects that arise when considering industrial control and automation systems used in manufacturing and other industries. We have therefore added additional standards to be considered when assessing a supplier's approach to cyber security, these are shown in Table 4:

Standard No.	Title
BS EN ISO/IEC 27001:2017	Information Technology–Security techniques–Information Security management systems–Requirements
PCI DSS v3.2.1 May 2018	Payment Card Industry, Data Security Standard, Requirements and Security Assessment Procedures
BS EN IEC 62443:2018	Security for industrial automation and control systems
BS ISO 28000:2007	Specification for security management systems for the supply chain
BS ISO/IEC 27031:2011	Information Technology–Security techniques–Guidelines for information and communication technology readiness for business continuity
PD ISO-TS 22318:2015	Societal security – Business continuity management systems – Guidelines for Supply Chain Security

Table 4 Standards Table

Requiring compliance with standards by suppliers provides an indication of the organisations culture and approach to cyber security. However, this does not provide the of level of

granularity required to assess the quality of the selected controls associated with the cyber connected supply chain.

Use of other guidelines/certifications such as Cyber Essentials [3][6] are focussed on information technology and do not consider the more industrial aspects of operational technology or industrial IoT. Assessment tools such as the Dstl-developed Cyber Defence Capability Assessment Tool (CDCAT) [16] utilise a framework of standards, including ISO/IEC 27001 and NIST mapped against a cyber lifecycle and the ITIL service lifecycle. These are focussed on assessing the cyber information security aspects of the PCO and not the cyber supply chain.

Identifying what standards have been implemented by the PCO and which standards are required from suppliers provides indicators of the level of cyber maturity for the organisation and the supplier, however in itself, this indicator is not sufficient to provide an overall measure of maturity or that the cyber connected key business processes have adequate security controls in place. It is accepted that the list provided in Table 4 is not comprehensive and additional standards, especially from the ISO 27000 series of standards, may be applicable dependent upon the industry vertical. These are identified at the point of engagement for consideration in the analysis process.

3.6 Governance Framework

The use of a cyber security framework to define a set of cyber security goals for the cyber supply chain provides a framework in which all the data gathered from the cyber supply chain map analysis output may be entered. Using this structured approach an overall assessment of the security and resilience of the PCO cyber supply chain may be ascertained. The framework selected has been adapted from previous work on cyber resilient supply chains [17] allowing for continuity of research output.

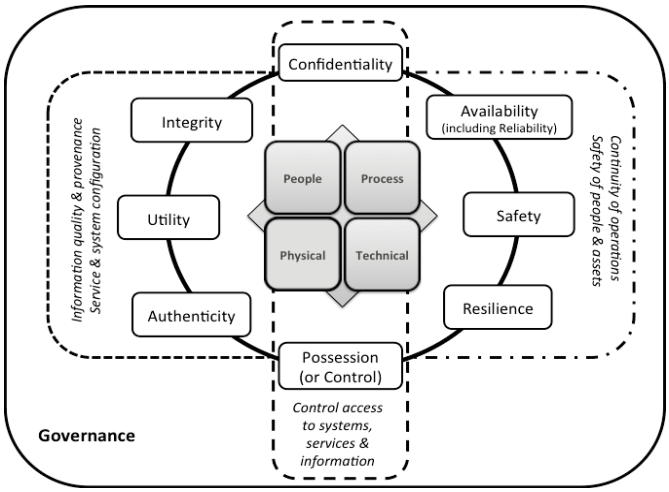

Figure 3 Overview of Security Framework [17]

The model at Figure 4 shows 8 security objectives captured in 3 groups with the standard controls mapped across all three groups. The following table consolidates the three groups and their controls:

Group	Objective	Objective	Target
Control of Access to Systems, Services & Information	To protect the confidentiality of sensitive information & to prevent unauthorised use of the system, data and information	Confidentiality	The prevention of unauthorised access to, and control of access to or observation of, data and/or information that might be sensitive or breach privacy, either in isolation or in aggregate.
		Possession	The holding, control and ability to use data and/or information, the ability to control and maintain the system's operation and to prevent unauthorised manipulation of or interference to it.
Continuity of Operations, Safety of People and Assets	This group seeks to preserve the safety and continuity of operations and ensure that if an adverse event occurs the CPS's operation degrades and is restored in a controlled fashion.	Availability	Maintaining the usability of and access to data and/or information and the system for a purpose, and where required to restore access and/or functionality in an appropriate and timely manner.
		Safety	The system and any supporting operating data and/or information are designed, implemented, operated and maintained, so as to prevent creation of harmful states that might lead to injury or loss of life, unintentional environmental damage, and damage to assets
		Resilience	The ability of the system, its functions, operational data and/or information to transform, renew and recover in a timely manner in response to adverse events.
Information Quality & Governance, Service & System Configuration	This group assures the quality of data and/or information used to operate the system and to deliver any products of service, it includes maintaining accurate configuration	Integrity	The prevention of unauthorised changes to the system, data and information, while maintaining the consistency, coherence and configuration of the system and the completeness, wholeness and readability of data and/or information, with the quality being

Group	Objective	Objective	Target
	information about the system, its interconnections, hardware and software		unchanged from a previous state.
		Utility	Maintaining the usefulness of the system, data and/or information for a purpose across the system lifecycle and for any subsequent period for which it may be required, in whole or in part.
		Authenticity	Establishing the validity, conformance and genuineness of the system, system components, data and/or information and preventing unauthorised changes, for example, tampering or modification.

Table 5 Consolidation of Security Framework

4 The Process

We have developed an overarching process to move from having little or no knowledge of the maturity of the cyber supply chain for any organisation to that where the organisation is able to monitor and maintain the maturity levels of their supply chain regardless of the complexity.

To start the process, we need to understand which parts of the Primary Contracting Organisation (PCO), have a data/information sharing connection to a supplier. This process needs to gather all available cyber related data/information about the PCO along with how this relates to the business of the PCO, allowing criticality of cyber assets and suppliers to be identified.

4.1 Stage 1 – Situational Awareness – Map Development

Having gathered the relevant data, we are able to generate a Cyber Supply Chain Map for the organisation. The map identifies all supplier relationships to the various internal business processes that have an element of cyber, with the map including an initial prioritisation assessment based on business criticality.

It is also essential that the map details the end of the supply chain for each data connection before the map assessment is carried out. This will entail discussions with each of the suppliers within the cyber supply chain tiers associated with the connection to ensure that full data trail is investigated and assessed.

Developing an individual end-to-end assessment for each cyber connection simplifies the overall assessment activity. However, it is complicated by the need to have discussions with organisations that the PCO does not have a direct relationship with and is reliant on suppliers being prepared to work with the PCO. We have not mentioned contracts in this paper, but consideration should be given for including such requirements as part of the PCO/Supplier supply agreement not only the direct relationship, but inclusion in any lower tier contracts that utilise any data/information from the PCO.

4.2 Stage 2 – Map Assessment

Once the cyber supply chain map has been created we assess each of the cyber supply chain connections using five steps. The assessment process has to be considered for each of the cyber connections with suppliers and as such the following individual steps are carried out multiple times.

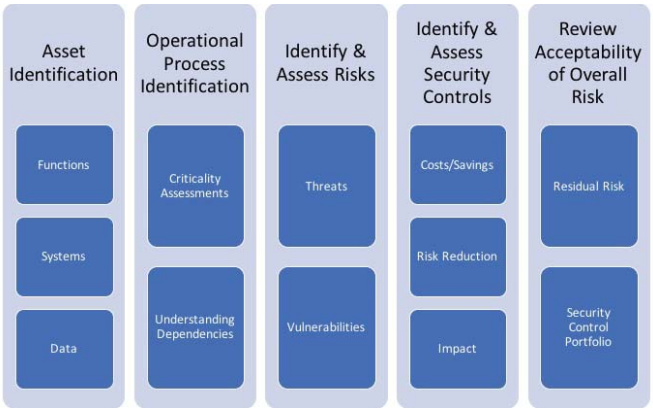

Figure 4 Assessment Process

4.2.2 Asset Identification

This is about the identification and evaluation of important assets and infrastructure within the PCO. From the map we understand; (a) how the different assets support the PCO's operational use, (b) the criticality of different areas within the PCO and the assets/systems they contain, and (c) the systems that operate in, support or protection of these critical assets. From a cyber security perspective, the business and operationally critical and/or sensitive elements of the PCO are likely to include:

(a) Those assets that have been identified that could be used to significantly compromise the integrity of any connection, with consideration given to; (i) cabling routes and containment, (ii) configuration, identification and use of control systems, (iii) critical permanent plant or machinery, (iv) security or other control rooms, including physical guarding, and (v) security, alarm and access control systems, CCTV and video processing.

(b) Data relating to the location, identification, technical specification and operation of business critical and sensitive assets.

(c) Systems, wherever they are hosted, used for planning, scheduling of PCO operations.

(d) Assets or systems upon which the business critical and/or sensitive elements are dependent for their normal operation and resilience.

4.3.3 Operational Process Identification

The operation of a PCO will depend on a set of business processes that rely upon data for the safe, secure and efficient

operation and enable supporting processes such as asset management, resource scheduling, financial and business planning, procurement, and the human resource processes. Having identified and assessed the important assets and infrastructure, the next step is to identify the PCO business processes that use the assets and infrastructure. This understanding of the business processes is used to assess the criticality of assets and to understand the interdependencies of the data and systems within the overall operational and business processes of the PCO. By so doing, the real impact of failure or compromise of individual components is better understood.

4.2.3 Identify & Assess Risks

The potential threats and vulnerabilities should have already been identified in the PCO Overall Security Assessment and Business Continuity Plan and mitigated via the PCO Security Policy. It will be necessary to understand the impact these threats and vulnerabilities may have on the connection to the supplier. The risk assessment should consider the nature of harm that may result and the impact that this may have to the overall supplier connection. The resultant cyber security risk calculation will depend on the likelihood that a threat actor may exploit one or more of the vulnerabilities and cause the nature of harm identified.

4.2.4 Identify & Assess Security Controls

For every cyber security vulnerability identified, possible mitigation or security controls should be identified and record. The assessment of each control should include; (a) the cost of the control and its implementation, (b) other impacts the control might have, for example, on asset or system usability and efficiency to the business processes operations.

The costs are to support the business justification for investment in the controls against the risk reduction achievable, any predicted cost saving or loss reduction. The other impacts reflect the potential for the controls to create further vulnerabilities or deliver any other business benefits.

The security controls that are chosen for implementation should be appropriate and proportionate to the risk they are intended to mitigate. The selected measures should be listed in the security assessment and form the basis of a connection security policy.

4.2.5 Review acceptability of Overall Risk

The assessment process continues for each connection until a point is reached where the level of residual risk is at an acceptable level given the criticality of the connection in respect of its overall criticality of the business process to the enterprise. The remaining residual risks for all supply chain connections has to be collated to ensure that the overall level of residual risk is acceptable for the organisation as a whole.

4.3 Stage 3 – Security Categories & Goals

The final stage in the process is to map the risks and security controls to the security categories and goals to allow and overall assessment of the PCO cyber supply chain security. Once this stage is completed it allows for gaps to be identified and for remedial action to be taken. This stage also provides for a capability to review and monitor the overall performance of maintaining the cyber supply chain security at an acceptable level especially as new suppliers are added, and existing suppliers are removed.

The process by definition cannot be a one-time event, it is an iterative process that needs to be repeated as the supply chain changes. This is made simpler once the initial work has been carried out.

5. Conclusions

The increasing threats and risks to the cyber supply chain are expected to increase as business becomes ever more interconnected. The consequent increase in attack surface and the inclination of attackers to move laterally once access has been obtain means that the weakest link in the chain has to be identified and managed. To understand the complexity of the cyber supply chain in any business a cyber supply chain situational awareness picture has to be developed and a cyber supply chain map generated. The use of categorisation of elements within the map relative to each of the cyber supply chain connections helps to understand the relationships, types of interconnections and applicability of standards related to the cyber supply chain connection.

Having a governance framework allows the development of goals relative to the PCO and the cyber supply chain connection to be developed, allowing assessments and monitoring of individual connections to be carried out, as well as providing an overall indication of the cyber supply chain security for the PCO. The process outlined to develop and assess the cyber supply chain map is based on a number of key activities leading to evaluation of threats and vulnerabilities, selection of controls to reduce the risk to the connection, as well as the evaluation of the overall risk to the cyber supply chain, and providing the data needed for the governance framework.

This paper draws out the complexity of understanding and dealing with a multi-tiered cyber supply chain and presents a process for drawing out the detail required to assess and quantify the state of cyber supply chain security, followed by a process to improve, monitor and maintain the acceptable level of security.

6. Future Work

This paper presents a process model that requires validation through testing with a number of organisations delineated by size and complexity. Engagement with a number of different organisations will be used to test different aspects of the process and model. Once the process model has been refined and proved the last stage of mapping to a Capability Maturity Model can be considered based on work already carried out on assessing maturity models associated with cyber and cyber security in the supply chain.

7. References

[1] Crowdstrike Global Threat Report, Adversary Tradecraft and the Importance of speed. Available: https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
[2] Carbon Black Global Threat Report, The Year of the Next-Gen Cyber Attack, January 2019. Available: https://www.carbonblack.com/wp-content/uploads/2019/01/carbon-black-global-threat-report-year-of-the-next-gen-cyberattack-0119.pdf
[3] "Cyber Essentials Scheme: overview", GOV.UK. [Online]. Available: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.
[4] "Cyber security for defence suppliers (Def Stan 05-138)", GOV.UK, 2015. [Online]. Available: https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138.
[5] "Using Supply Chain Modelling to Mitigate Risk in the Automotive Industry | LLamasoft", LLamasoft, 2018. [Online]. Available: https://www.llamasoft.com/using-supply-chain-modeling-to-mitigate-risk-in-the-automotive-industry-white-paper/.
[6] "Cyber Essentials Plus Test Specification v 1.2", Ncsc.gov.uk. [Online]. Available: https://www.ncsc.gov.uk/content/files/scheme_downloads/cyber-essentials-test-specs.pdf.
[7] Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors Journal 37(1),32-64
[8] Business Process Model and Notation (BPMN), Version 2.0, OMG Document Number: formal/2011-01-03. Available: http://www.omg.org/spec/BPMN/2.0
[9] A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. Journal: Computers & Industrial Engineering. Available: https://doi.org/10.1016/j.cie.2018.11.030
[10] Boyes, H., Hallaq, B., Cunningham, J. and Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 101, pp.1-12.
[11] Lahti, M & Shamsuzzoha, AHM & Helo, Petri. (2009). Developing a maturity model for Supply Chain Management. International Journal of Logistics Systems and Management. 5. 654-678. 10.1504/IJLSM.2009.024796.
[12] ITU, Global Cybersecurity Index & Cyberwellness Profiles, April 2015 Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
[13] DCMS Cyber Security Breaches Survey, April 2017 [online] Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf
[14] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures V3.2.1, May 2018 [Online] Available from: https://www.pcisecuritystandards.org/
[15] BS EN ISO/IEC 27001:2017 Information technology–Security techniques–Information Security Management Systems–Requirements (ISO/IEC 27001:2013)
[16] CDCAT® - Cyber Defence Capability Assessment Tool, available from APMG International https://apmg-international.com/product/cdcat
[17] Boyes, H. (2015) "Cybersecurity and Cyber-Resilient Supply Chains". Technology Innovation Management Review, 5(4): 28-34
[18} The principles of supply chain security, 28 Jan 2018, National Cyber Security Centre Guidance. Available: https://www.ncsc.gov.uk/guidance/principles-supply-chain-security