CYBERSECURITY INFORMATION SHARING: A FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT IN UK SME SUPPLY CHAINS

Complete Research

Lewis, Riyana, Brunel University, Uxbridge, UK, riyana.rlewis@gmail.com.

Louvieris, Panos, Brunel University, Uxbridge, UK, panos.louvieris@brunel.ac.uk.

Abbott, Pamela, Brunel University, Uxbridge, UK, pamela.abbott@brunel.ac.uk.

Clewley, Natalie, Brunel University, Uxbridge, UK, natalie.clewley@brunel.ac.uk.

Jones, Kevin, EADS Innovation Works, Coedkernew, Newport, UK, kevin.jones@eads.com.

Abstract

UK small to medium sized enterprises (SMEs) are suffering increasing levels of cybersecurity breaches and are a major point of vulnerability in the supply chain networks in which they participate. A key factor for achieving optimal security levels within supply chains is the management and sharing of cybersecurity information associated with specific metrics. Such information sharing schemes amongst SMEs in a supply chain network, however, would give rise to a certain level of risk exposure. In response, the purpose of this paper is to assess the implications of adopting select cybersecurity metrics for information sharing in SME supply chain consortia. Thus, a set of commonly used metrics in a prototypical cybersecurity scenario were chosen and tested from a survey of 17 UK SMEs. The results were analysed in respect of two variables; namely, usefulness of implementation and willingness to share across supply chains. Consequently, we propose a Cybersecurity Information Sharing Taxonomy for identifying risk exposure categories for SMEs sharing cybersecurity information, which can be applied to developing Information Sharing Agreements (ISAs) within SME supply chain consortia.

Keywords: SME Supply Chains, Information Sharing, Cybersecurity Metrics, Information Sharing Agreement, Information Security Management, Risk Management

1 Introduction

The UK Cabinet Office (2011) estimates the cost of cybersecurity breaches to the UK at £27 billion a year. In the last year 93% of large corporations (>250 staff) and 87% of small businesses (<50 staff) in the UK reported cybersecurity breaches amounting to approximately 50% more attacks than were reported in 2012 across the same organisations (PricewaterHouse Cooper, 2013). This report also claims that the average individual cost *for the worst of* these breaches ranged from £450,000 to £850,000 for large businesses, and from £35,000 to £65,000 for smaller ones, with the latter experiencing levels of attacks previously only seen in larger organisations (PricewaterHouse Cooper, 2013). Other recent cybersecurity surveys (Verizon, 2013; Cisco, 2013; Ponemon Institute, 2013) also indicate a range of cyber threats faced by small to medium sized enterprises (SMEs) including malware, hacking, mobile device loss/misuse, DDOS attacks, advanced persistent threats (APT), threats related to human factors and penetration threats.

Continuous investments in different information security measures and sophisticated data protection systems are generally needed to prevent financial loss due to cyber attacks. Such investments are usually associated with security decisions made at every level of an organisation (Bojanc and Jerman-Blazic, 2008). For example, at the tactical and operational levels of an organisation, cybersecurity decisions would focus on the optimisation of security resources, that is, an integrated combination of plans, personnel, procedures, guidelines and technologies that minimize damage and losses. While these actions and tactics reduce the frequency and/or consequences of security breaches, they are constrained by the organisation's global security budget (Anderson and Choobineh, 2008). An extensive security budget may be difficult, for example, for SMEs with low profit margins and income streams (Tawileh et al., 2007).

Supply chain consortia depend increasingly upon integrated and interoperable IT systems for efficient management (Hughes et al., 2008; Levary, 2000) and comprise multi-level networked relationships among a heterogeneous group of organisations, many of which are SMEs. The increasing threat of cyber attacks on SMEs, however, is potentially a major point of vulnerability in supply chain networks. This is because SMEs represent the weakest links in information security management in these types of networked business environments due to the fact that they are unable to afford to scale up security activities to the levels necessary to ensure stable operating environments (Finch, 2004) and that they represent a "soft" target for cybersecurity breaches (PricewaterHouse Cooper, 2013). In light of increasing cyber attacks on ICT systems in supply chain networks (InformationWeek, 2009), it is becoming crucial to minimize the potential risks that can endanger their operation (Inserra and Bucci, 2014).

It has been recognised that a key factor for achieving optimal security levels within a group of cooperating firms is the management and sharing of information related to any kind of attempt at breaching computer security (Gal-Or and Chose, 2005). The UK Government, for example, has recently launched the Cybersecurity Information Sharing Partnership (CISP) to share information and intelligence on cybersecurity threats, the objective of which is to make UK cyberspace more secure (Gov.uk, 2013). Although such information sharing should mitigate the risks associated with cyber threats within an ecosystem, negative exposure and loss of reputation as a result of information infrastructure violations being made public can however tarnish a firm's image. Thus, information sharing amongst SMEs in a supply chain network would give rise to a certain level of risk exposure. In response to this issue, the purpose of this paper is to assess the implications of adopting cybersecurity metrics that can contribute to cybersecurity information sharing in the collaborative environment of SME supply chain consortia.

The paper thus aims to: (i) evaluate the extent to which SMEs find it useful to implement cybersecurity metrics that would mitigate against a typical cyber attack; (ii) evaluate the extent to

which SMEs are willing to share cybersecurity information in the form of these metrics and (iii) develop a taxonomy of risk exposure to cybersecurity information sharing as perceived by SMEs in a supply chain network. To satisfy these aims the following objectives were set:

- Determine metrics which can be employed to directly monitor the status of cybersecurity for SMEs in the event of a typical cyber attack
- Assess the implications to the SMEs of implementing these cybersecurity metrics as well as sharing this information in the supply chain
- Evaluate the acceptance of these metrics within a collaborative environment
- Propose a Cybersecurity Information Sharing Taxonomy for qualitatively identifying risk exposure categories for SMEs sharing cybersecurity information in a supply chain.

2 Information Security in Supply Chain Networks

The development of methods, standards and processes to address cybersecurity assurance in supply chains is a relatively recent area of research in both industry and academia (Bartol, 2014). The field is only now beginning to address risk parameters and best practices related to cybersecurity in the supply chain (Boyson, 2014). Given this context, this section approaches the topic by first addressing the business processes involved in managing information security in organisations, then assesses the feasibility of sharing these metrics as part of formal information sharing agreements among supply chain partners and finally makes a link between information sharing and cybersecurity risk mitigation strategies.

2.1 Cybersecurity Metrics for Information Security Management

Information security management can be viewed as an evolved set of processes for identifying, mitigating and documenting an organisation's major security breaches. A review of the relevant literature (Dorofee, 2007; Booz Allen Hamilton, 2011; Bodeau and Graubart, 2011; TMForum, 2013) implies four main stages in an information security management model, namely, Prevent, Detect, Respond and Recover. Security experts believe that metrics are a key aspect in monitoring, controlling and managing the security aspects of information systems which, in turn, underpin organisational processes (Chew et al., 2008; Jansen, 2009). Information or cyber security metrics should thus form the foundation of any security management framework and should be tied to the organisation's business processes (Hayden, 2010). Cybersecurity metrics can assist in measuring an organisation's capability to address the four main stages of an information security management framework, i.e. prevent, detect, respond and recover, from any cyber attack and indicate improvements needed in the process to thwart future attacks or reduce the impact of such attacks (Chew et al., 2008).

For the purpose of tracking and evaluating cyber threats, a manageable number of metrics should be selected based on the size of the organisation and the economic viability of their maintenance since a large number of metrics can be challenging to interpret as well as to evaluate and maintain (Boyer and McQueen, 2008). When monitoring the security status of IT systems, for example, reviewing logs or control measurements, quantifiable metrics are particularly useful. Thus measures that can be expressed in terms of numbers, levels or rankings, can provide numerical indicators of the security status of a system for use in further statistical analysis or performance measurement (Heyman et al., 2008). Thus, for example, the Key Performance Indicators (KPIs) of service levels for federated or standalone systems can be expressed and measured as quantifiable metrics. Additionally, the usefulness of cyber security metrics tends to be context-dependent, i.e., the interpretation of the measurements is highly dependent on the organisation's information security goals, business critical assets, relationship to collaborating partners, specific threat vulnerabilities, etc. (Vaughn et al., 2003).

For the purpose of this study a set of metrics has been selected from the literature (see Appendix) based on the following criteria:

- They are quantifiable so that the values generated can be easily compared as well as reported across SMEs in a supply chain
- They were assumed to be relevant to the organisation in the context of the chosen business scenario

The importance of these metrics might vary between SMEs. Some SMEs may have much higher profiles than others, and would thus be a more attractive target for attackers, whose attack vectors and capabilities may also vary. Additionally, some of these metrics may be normally considered unsuitable for sharing since their disclosure could cause damage to the reputation of the SME or reveal sensitive information.

2.2 Cybersecurity Information Sharing

One of the major components for organisations achieving cyber intelligence capability is information sharing amongst collaborative partners and trusted associates (Barnum, 2013; Fernandez et al., 2012; ENISA, 2010). Cybersecurity information sharing amongst supply chain participants may help to propagate valuable insights into the latest techniques used by cyber attackers along with information about their objectives (Fleming and Goldstein, 2012). Cybersecurity information sharing has also been recognised at national levels as well, resulting in the launch of the Cybersecurity Information Sharing Partnership (CISP) in the UK (Gov.uk, 2013) and the Cyber Intelligence Sharing and Protection Act (CISPA) in the US (Congress.gov, 2013). The Centre for Protection of National Infrastructure (CPNI) in the UK[1] facilitates 'information exchanges' which allow one company to learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities. However, the sharing of information amongst members of a supply chain is not necessarily straightforward. Pujara et al. (2011) and Zahedirad and Shivaraj (2011), for example, have indicated some potential barriers as below:

- Exposure of sensitive data that is highly important to the organisation and could be misused
- Other organisations gaining a competitive advantage due to the information that is shared
- Lack of trust in the channels through which the information is being shared
- Not enough knowledge about the implications or the benefits of information sharing.

A way of reducing these barriers would be to share information through a trusted intermediary, which promotes information sharing by providing the ability to analyze and redistribute information in a timely, actionable and relevant manner (ENISA, 2010), for example, ISACs[2] in the US or CISP in the UK. In the absence of such an intermediary other risk mitigation strategies may be considered such as, for example, the sorts of legally binding agreements recommend by Boyens et al. (2013) to reduce supply chain security risk from external IT service providers engaging with federal agencies:

> *"For services external to organisations, a chain of trust requires that organisations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organisations*

[1] Cybersecurity information provided by CPNI is available at: http://www.cpni.gov.uk/

[2] Information about ISACs can be found at: http://itlaw.wikia.com/wiki/Information_Sharing_and_Analysis_Center

> *and the external providers. Organisations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance" (Boyens et al., 2013, p. 204).*

Thus Information Sharing Agreements (ISAs) or Cyber Information Sharing Agreements (CISAs) amongst SMEs in supply chain consortia would help in building a pool of information to which businesses will have access. This information pool would include the best strategies that could help SMEs in reducing the cost related to preventing attacks (Aviram and Tor, 2010). An added advantage would be that the more valuable the information contributed by each participant SME, the more the collective knowledge of the entire supply chain would increase (Fernandez et al., 2012). Information sharing efforts should also ideally be governed by legal frameworks to avoid any misuse of information (Fernandez et al., 2012; Aviram and Tor, 2010). As such, being part of an ISA would alleviate the risks of poor quality of information being shared. Also, risks related to trust issues with regards to misuse of data could be mitigated by introducing clauses pertaining to the same in the information sharing agreement (ENISA, 2010). Knowledge about the types of devices and technology used by the other organisations can also help in filtering out information (Boyens et al., 2013). For example, if malware has been found which affects only the Linux OS, then the metric related information for this attack can be shared only with the SME which actually uses the Linux OS.

The success of an ISA depends on building trust between the collaborating partners (Fleming and Goldstein, 2012) such that they are willing to share sensitive information and there is confidence in the quality of the information being shared. Fleming and Goldstein (2012) also recommend that information sharing be directed by collective goals. In the case of cybersecurity in the supply chain the goal would be to mitigate shared risk in the entire supply chain (Boyson, 2014). It should be noted, however, that not all kinds of exploits and attacks can be addressed with the help of information sharing, such as zero-day exploits (Fleming and Goldstein, 2012; Bayuk, 2013) i.e., vulnerabilities that no one knew existed before they were exploited. Additionally, the legal and economic barriers to cybersecurity information sharing may not be easily addressed by a set of conditions in one agreement and may need considerable negotiation and compromise between partners (Gordon et al., 2003; Gal-Or and Chase, 2005; Aviram and Tor, 2010).

There is thus merit in determining the types of incentives and circumstances that might be deemed appropriate for an Information Sharing Agreement (ISA) under which SMEs could adopt cybersecurity information sharing. The remainder of the paper addresses this issue and also develops a taxonomy of risk profiles related to the metrics deemed important to establishing cybersecurity information sharing arrangements in a supply chain.

3 Study Design and Analysis

3.1 Design and Sample

For the purpose of this paper a scenario-based study has been used in which a business scenario related to a cyber attack was given to respondents and a self completion questionnaire issued against the background of this business scenario. The questionnaire was hosted on an online platform and the respondents were sent an online link via email to invite them to complete it. The questionnaire was divided into four parts:

- **Part 1** contained basic information about the size and sector of the organisation and their perception of the overall importance of cybersecurity.

- **Part 2** outlined the cyber attack business scenario.
- **Part 3** provided a list of cybersecurity metrics that would help prepare organisations to deal with these attacks. The questionnaire employed a 5-point Likert scale to assess the extent to which the respondents thought each metric: (i) was *useful to implement* in their own organisation and (ii) they would be *willing to share* the same metric amongst other SMEs in their supply chain network. The existence of a cybersecurity Information Sharing Agreement (ISA) between SMEs in the supply chain is assumed and detailed in the scenario.
- **Part 4** of the questionnaire covered general questions such as: (i) the percentage of the organisation's IT budget allocated for cybersecurity, (ii) a request to rank both the *incentives for*, and *barriers against*, the adoption of cybersecurity information sharing, (iii) a list of general conditions under which the organisation would agree to share cybersecurity information.

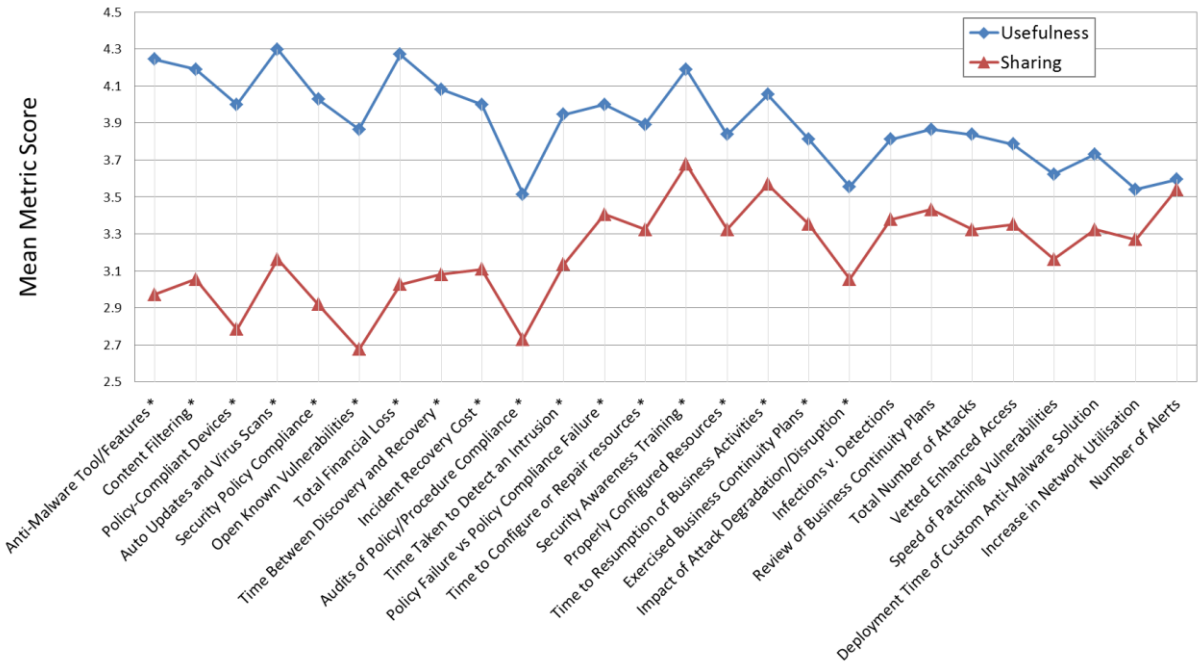
The sample frame for this paper was managers/business owners of UK SMEs and cybersecurity professionals in SMEs since it was assumed that people with these types of profiles would be knowledgeable about decisions regarding implementing and sharing cybersecurity metrics. The sample consisted of 37 participants from 17 UK SME organisations. 51.3% of the respondents were managers, managing directors and small business owners and 48.7% of the respondents were IT and cybersecurity professionals. The majority of the respondents were from SMEs with staffing sizes greater than 100 employees (64%), followed by SMEs of more than 50 employees (21.6%), those of more than 10 (8.1%) and those of 10 or less employees (5.4%). The industry sectors represented were Information Technology (48.6%), Banking and Investment (18.9%), Telecoms Services (18.9%), Electronics (8.1%) and others (5.4%).

3.2 Analysis

The analysis comprised of four parts. Firstly, a comparison of the two variables willingness to implement based on usefulness of metrics (*usefulness*) and willingness to share the metrics (*sharing*) amongst other SMEs in the supply chain was conducted using Paired T-Tests. Secondly, analysis of the importance of cybersecurity, budget allocation to cybersecurity and the benefits of and incentives for sharing the metrics with other SMEs within a supply chain was conducted using ANOVAs. Additionally, analysis of incentives for sharing of cybersecurity metrics amongst SMEs in a supply chain was also conducted using ANOVAs. Finally, the barriers for adopting cybersecurity information sharing are discussed. The following sub-sections present the results in detail.

3.2.1 Paired T-Tests: Comparison between Usefulness and Sharing

Based on the Kolmogorov Smirnov test which confirmed normality, a Paired T-Test was carried out to determine whether there were significant differences between the responses for *usefulness* and *sharing* in Part 3 of the questionnaire. Figure 1 shows a plot of the means for each metric. Of the 26 metrics, the majority (n=18) were found to be significantly different ($p<0.05$) with 12 of these metrics having a *p* value of less than 0.01. Although both variables provide more or less similar results, *usefulness* consistently scored higher than *sharing*, meaning that generally participants would prefer to implement the metrics more than they would share them. The metrics with the most significant differences include total financial loss, number of open known vulnerabilities and percentage of assets that have specific anti-malware tools or features installed. Since these metrics relate to factors that would affect an SME's reputation, i.e., income and future business, SMEs would be more reluctant to share this type of information with competitors. On the other hand, the metric scores that were not significantly different (e.g. vetted enhanced access, speed of patching, number of alerts, number of infections vs. detections) are not perceived as damaging to reputation, income or future business and show that participants were not so averse to sharing these with other SMEs in a supply chain.



**denotes statistically significant scores ($p<0.05$)*

Figure 1. Difference between mean metric scores for "Willingness to Implement (Usefulness)" and "Willingness to Share (Sharing)".

3.2.2 ANOVAs: The Importance of Cybersecurity, IT Budget Allocation and the Benefits of Information Sharing in an SME Supply Chain

In order to assess the differences between the metric scores for the three factors Importance of Cyber Security, IT Budget Allocation to Cybersecurity and Benefits of Sharing, a one-way between groups analysis of variance (ANOVA) was conducted (Table 1). These factors were assessed using the total number of employees, which was designed to measure how much the size of an SME affected their perception of cybersecurity investment. In terms of the Importance of Cybersecurity, it can be inferred from the non-significant result that irrespective of SME size, all SMEs considered cybersecurity to be important.

ANOVA Groups	Importance of Cybersecurity	Allocation of IT Budget	Belief that Information Sharing is Beneficial
	P-Value	P-Value	P-Value
Total number of employees	0.529	0.091	0.076

Table 1. ANOVA Results for Importance of Cybersecurity, IT Budget Allocation to Cybersecurity and Benefits of Sharing Cybersecurity Information.

In terms of the percentage of IT budget allocated to Cybersecurity, there was also no significant difference between the groups meaning that perception of budget allocation is consistent across the groups. More specifically, SMEs which have fewer than 50 employees tend to spend less than 10% of

their IT budget on cybersecurity, whereas larger SMEs with employees of more than 50 spend between 5% and 30% of their IT Budget on cybersecurity. This is consistent with the findings of Cresswell and Hassan (2007) that though security management is of the utmost importance to fulfil the current needs of cybersecurity, affordability could be an issue amongst the smaller organisations in a supply chain.

Again, there was no significant difference between the groups for the belief that the introduction of information sharing in their security management process would benefit the cybersecurity of the entire organisation. These findings lend support to the UK Government CISP initiative (Gov.uk, 2013) and Fernandez et al. (2012) who suggest that information sharing is an important component in achieving enhanced cybersecurity across the supply chain. It indicates that SMEs in supply chain consortia would be willing to be a part of such initiatives.

3.2.3 ANOVAs: Incentives for Information Sharing in an SME Supply Chain

ANOVA Groups	Incentive 1: Distribution of Profits	Incentive 2: Sharing of Techniques	Incentive 3: Cost Reduction	Incentive 4: Cyber Insurance
	P-Value	P-Value	P-Value	P-Value
Total number of employees	0.008*	0.590	0.250	0.877

Table 2. ANOVA Results for Incentives for Cybersecurity Information Sharing.

The second set of ANOVA results (shown in Table 2) looked at the level of support for cybersecurity information sharing incentives within an SME supply chain (part 4 of the questionnaire). Four incentives were given, including: (i) distribution of profits caused by saving cost to be spent on remediation if the attack was to spread; (ii) sharing of the techniques used to thwart such attacks; (iii) cost reduction by minimising security breaches; and (iv) providing greater liability protection/cyber insurance for companies participating in the sharing that are attacked.

The distribution of profits (*Incentive 1*) was found to significantly differ between SME sizes. Only small organisations with employee numbers fewer than 10 seemed to support the idea of distribution of profits as an incentive. Smaller organisations can become easy targets for cyber attacks since they would not have sufficient infrastructure in place to thwart the attack as well as the attacker could easily gain information about the larger organisation with which the smaller organisation is associated. Thus, smaller organisations might have more information to share related to a particular attack as it might be the first target of the attack, but might not have enough funds to thwart the attack. Hence, in return for sharing the information related to the attack, the small organisation might desire a distribution of the profits gained by the larger organisation through addressing the attack. The smaller organisations can then strengthen their cybersecurity management processes using these funds and continue to share the information.

Neither the sharing of techniques (*Incentive 2*) and cost reduction (*Incentive 3*) significantly differed between groups. Sharing of techniques was preferred on a high scale across all the groups, which when implemented in conjunction with an information sharing agreement (ISA) would lead to cost reductions through knowledge sharing across beneficiaries in the SME supply chain.

Although cyber insurance (*Incentive 4*) did not significantly differ between groups, larger SMEs (those with >100 employees) scored this incentive higher than the smaller SMEs. Cyber insurance is a relatively new idea and as such the reason for this outcome could be that the smaller organisations taking part in the cyber information sharing do not have enough information about it. Another reason for this could be that larger SMEs have comparatively more IT infrastructure as well as sensitive information and damage to this could cause substantial financial losses.

3.2.4 Barriers to the Adoption of Cybersecurity Information Sharing

Five barriers to the adoption of cybersecurity information sharing were also given to respondents to rank in order of the most influential in Part 4 of the questionnaire. *Organisations competing in the same market* and *trust issues with regards to misuse of data* were cited as the barriers that most deterred SMEs from participating in cybersecurity information sharing, whilst *poor quality of information* and *lack of support from the network leader* were consistently ranked the lowest.

This study also analysed the circumstances under which SMEs would agree to share cybersecurity information. The circumstances which are most preferred by SMEs for undertaking sharing of cybersecurity information are "keeping data anonymised" and "being part of an Information Sharing Agreement (ISA)". These circumstances can be seen as drivers for undertaking the sharing of the cybersecurity metric related information. If the above mentioned drivers are put into place the barriers to sharing the metric related information can be greatly reduced in the following manner:

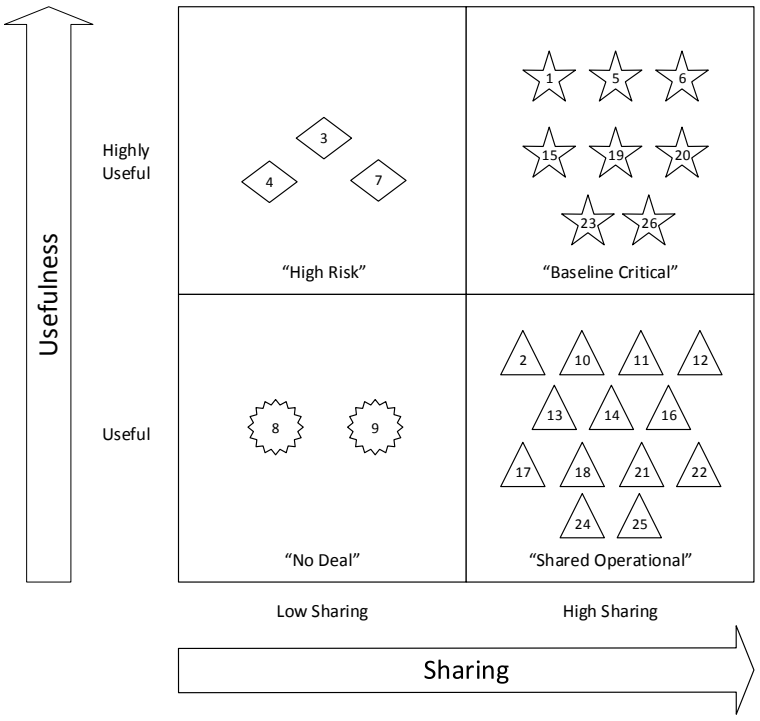
- If the **data is kept anonymised**, the organisations receiving the information would not know the origin of the information, and thus the risk of rival organisations using the data for their advantage could be reduced. Also, the risk related to misuse of the information to harm the reputation of a particular organisation would be highly reduced.
- **Information Sharing Agreements (ISAs)** would provide formal, legally binding arrangements for sharing risk and compensation in the event of cyber attacks. Responsibility, liability and accountability would be catered for in such agreements thus providing shared indemnity.

3.2.5 A Framework for Information Security Sharing in SME Supply Chains

All the data provided by the respondents was confined within the ranges of low to high usefulness and low to high sharing. Therefore, the means from the Paired T-Tests (shown graphically in Figure 1) were plotted on a 2x2 grid of quadrants, with the axes representing the degree of *usefulness* and willingness to *share*, in order to create the Cybersecurity Information Sharing Taxonomy (Figure 2). The resulting quadrants demonstrate qualitatively the degree of risk to which an SME deems itself exposed when sharing certain cybersecurity metrics. Each quadrant is further interpreted and discussed in this context.

High Sharing/Highly Useful – "Baseline Critical": The metrics categorised into this quadrant include those that SMEs consider to be vital to understanding the impact on business processes and sustainability, and should definitely be shared across the supply chain. For example, the level of content filtering, automatic updates and virus scanning, incident recovery costs, time between attack discovery and recovery, time to resumption of business activities and the total financial loss of attacks are all related to the business processes and would directly affect sustainability of the business. The strategic nature of these metrics and the willingness of SMEs to share cybersecurity information associated with them mandates their inclusion in the ISA.

High Sharing/Useful – "Shared Operational": The metrics categorised into this quadrant are those that the SMEs would find useful to share to ensure a common standard of cybersecurity. For example, the speed of patching vulnerabilities, increase in network utilisation, time taken to detect an intrusion, number of alerts, number of infections vs. detections and time taken to configure or repair resources, all relate to the characteristics of a cyber attack. Sharing this information provides SMEs in the supply chain with a common reference that protects the cyber infrastructure that underpins the business processes and overall delivers a higher standard of cybersecurity. These metrics can also be used to contractually specify a minimum level of cybersecurity which membership of a supply chain demands. Therefore, to operationalise any ISA, all of the Shared Operational metrics should be included.



Metric	Description
1	Security Awareness Training
2	Vetted Enhanced Access
3	Security Policy Compliance
4	Policy-Compliant Devices
5	Content Filtering
6	Auto Updates and Virus Scans
7	Anti-Malware Tool/Features
8	Audits of Policy/Procedure Compliance
9	Open Known Vulnerabilities
10	Speed of Patching Vulnerabilities
11	Increase in Network Utilisation
12	Time taken to Detect an Intrusion
13	Number of Alerts
14	Infections v. Detections
15	Policy Failure vs Policy Compliance Failure
16	Impact of Degradation/Disruption
17	Deployment Time of Custom Anti-Malware
18	Total Number of Attacks
19	Time between Discovery and Recovery
20	Time to Resumption of Business Activities
21	Exercised Business Continuity Plans
22	Review of Business Continuity Plans
23	Incident Recovery Cost
24	Properly Configured Resources
25	Time to Configure/Repair Resources
26	Total Financial Loss

Figure 2. Cybersecurity Information Sharing Taxonomy.

Highly Useful/Low Sharing – "High Risk": These metrics are categorised as high risk and SMEs would be reluctant to share this sensitive information because it would expose weaknesses in their cybersecurity capability. For example, security policy compliance, number of policy compliant devices and number of assets with anti-malware tools or features configured would directly affect the organisation's reputation if lower than expected. In addition, this information can be used directly in the targeting of a cyber attack against an SME as it gives clues as to their vulnerabilities. However, these metrics are of potential benefit to the entire supply chain to help ensure that the entire supply chain is operating at a common level in terms of their cybersecurity capability. The migration of these metrics to the next quadrant, i.e. from "High Risk" to "Baseline Critical", is essential for the maintenance of security across the entire supply chain. As found in the results from the incentives, keeping data anonymised and governing the sharing of this information through legal frameworks like an ISA can help reduce the risks related to the sharing of these metrics. As such incentives like cyber insurance, sharing of techniques to thwart future attacks and distribution of profits might encourage the organisation to share these within an ISA.

Low Sharing/Useful – "No Deals": The metrics in this quadrant are those that are perceived to be both unimportant to other SMEs and highly risky to share. For example, known vulnerabilities can easily be found through sites such as the Common Vulnerabilities and Exposures (CVE) list (Mitre, 2014), but the number of specific vulnerabilities an organisation is yet to address would be extremely risky for an SME to share as this would expose weaknesses in their cyber defence capability. The same applies for the results of policy and procedure compliance audits as it might not be useful to another organisation but could again expose vulnerabilities in defence capability. An ISA that includes these metrics would meet with some resistance from SMEs, so their inclusion in a supply chain ISA should be carefully considered.

4 Conclusion

Contemporary work on cyber supply chains emphasises the need to address cybersecurity information sharing among supply chain partners so as to enhance collective threat intelligence and thwart potential cyber attacks (Barnum, 2013; Fernandez et al., 2012; Gordon et al., 2003; Fleming and Goldstein, 2012). UK SMEs are facing increasing cybersecurity breaches, the prevention of which is often too expensive for a small firm to fully manage (Tawileh et al., 2007). This situation thus exposes SMEs as the vulnerable points of the overall security of a supply chain network. Despite the criticality of this problem, current research is slow to address it, with almost no work specifically focusing on the SME component of cyber supply chains or on specific metrics that would be applicable to cyber supply chain security. This paper thus makes an important contribution by addressing: (i) the types of information that could be shared among SMEs in a supply chain network when faced with a specific cyber attack scenario; (ii) the willingness of SMEs in the supply chain to share this information; and (iii) the perceived risk exposure of SMEs sharing such information. The paper also makes a further important contribution by exploring the incentives and barriers which either encourage or hinder cybersecurity information sharing from an SME perspective. While current studies present generic information about incentives and barriers to information sharing (ENISA, 2010; Gal-Or and Chose, 2005; Gordon et al. 2003; Fernandez et al., 2012), we are not aware of any current study that attempts to test, using a specific, practical scenario-based study, the actual concerns about sharing cybersecurity information from SMEs participating in a supply chain network. Thus, the research process by which this study has been undertaken is also a potential contribution to methodologies that can be used to investigate phenomena in context-dependent situations such as the kind this research presented. This study thus augments previous work in the field and illustrates the practical applicability of the theory to a critical target group.

Moreover, the results of the paper can be practically applied to some of the critical issues hampering the implementation of cybersecurity information sharing schemes (Aviram and Tor, 2010; Bojanc and Jerman-Blazic, 2008; Boyens et al., 2013). One of these issues is the complexity of the legal frameworks which may need to be implemented in order for such schemes to work (Aviram and Tor, 2010). The Cybersecurity Information Sharing Taxonomy developed by this study categorises SMEs' perceived risk exposure for the selected business scenario and demonstrates the conditions under which SMEs might be prepared to enter into a formal Information Sharing Agreement (ISA). It is conceivable that for any of a number of given business scenarios similar taxonomies can be established along with corresponding lists of conditions to be covered by an attendant ISA. Another issue lies in managing the risks associated with sharing information about sensitive security breaches (Boyens et al., 2013). Since the taxonomy is comprised of context-dependent security metrics, it can also potentially be the basis for sensitivity dashboards, shared by supply chain partners indicating their collective risk exposure to specific incidents represented by the business scenarios. Thus the study has the potential to operationalise current theoretical and conceptual work done on the practical applicability of metrics frameworks and cybersecurity risk management across the supply chain.

The study is limited in its ability to generalise to larger SME cohorts due to the relatively small size of the sample (17 SME organisations) and the fact that the companies were UK-based. Nonetheless, the results are compelling in that there is apparent face validity in the categories developed in the Cybersecurity Information Sharing Taxonomy. Further work would address the sampling issues by distributing the survey to a much larger cohort of SMEs in a supply chain network. Various industry sectors could be tested and comparative analyses between country contexts, which operate according to different legal frameworks, could be investigated as well. The scenario-based nature of the study would allow for the testing of the select metrics under different business scenarios, thus creating different taxonomy categories. These would represent cross-sectional comparative studies, however, longitudinal studies could also be undertaken to study the change in perception of risk exposure by SME supply chain participants over time.

Appendix

Metric	Description of Metric	Literature Source
1	Percentage of employees who have completed the security awareness training	(CISWG, 2005; TMForum, 2013)
2	Percentage of employees with an enhanced level of access to systems who have been vetted	(CISWG, 2005; TMForum, 2013)
3	Level of security policy compliance on the targeted systems	(Patriciu et al., 2006)
4	Total count of Policy-Compliant Devices	(Patriciu et al., 2006)
5	Percentage of emails, websites and web domains undergoing content filtering within the organisation	(Patriciu et al., 2006)
6	Percentage of high-value assets (systems) with automatic virus definition updates and automatic virus scanning	(Dorofee et al., 2007)
7	Percentage of high-value assets (systems) that have specific anti-malware tool or feature installed and up to date	(Dorofee et al., 2007)
8	Results of internal and third party audits of policy and procedure compliance	(TMForum, 2013)
9	Number of known vulnerabilities open	(Bodeau et al., 2012)
10	Average speed of patching vulnerabilities	(Bodeau et al., 2012)
11	Percentage of increase in network utilisation	(Patriciu et al., 2006)
12	Time taken to detect an intrusion	(Voas et al., 1996)
13	Number of alerts per system that is targeted	(Miani et al., 2013)
14	Percentage of variance of reported/discovered infections versus detections	(Patriciu et al., 2006)
15	Cause of incident : policy failure vs policy compliance failure	(Patriciu et al., 2006)
16	Number of employees affected by the degradation or disruption of the network, systems or application services	(Patriciu et al., 2006)
17	Time taken to deploy a custom anti-malware signature for this attack across the enterprise.	(Langweg, 2006)
18	Total number of attacks caused by this malware throughout organisation	(Sandoval and Hassel, 2010)
19	Time between discovery of attack and completion of system remediation	(Bodeau et al., 2012)
20	Time taken to resume business activities after being attacked	(Bodeau et al., 2012)
21	Level up to which business continuity plans are exercised across all the organisational units.	(CISWG, 2005)
22	Level up to which business continuity plans are reviewed across all the organisational units	(CISWG, 2005)
23	Incident recovery cost	(CIS, 2010)
24	Percentage of cyber resources that are properly configured after an attack	(Bodeau et al., 2012)
25	Length of time to combine tools, services, and data sources needed to repair or reconstitute the infrastructure	(Bodeau et al., 2012)
26	Total amount of financial loss caused	(Bodeau et al., 2012)

Table 3. Ranked list of Metrics by P-Value from Paired T-Test with Literature Sources.

References

Anderson, E.E. and Choobineh, J. (2008). Enterprise information security strategies. Computers & Security, 27(1–2), 22-29.

Aviram, A. and Tor, A. (2010). Overcoming Impediments to Information Sharing. Harvard Law and Economics Discussion Paper No. 427. http://ssrn.com/abstract=435600.

Barnum, S. (2013). Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). The MITRE Corporation. Accessed 26/03/2014. https://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf.

Bartol, N. (2014). Cyber supply chain security practices DNA – filling in the puzzle using a diverse set of disciplines. Technovation, in Press. http://dx.doi.org/10.1016/j.technovation.2014.01.005i

Bayuk, J.L. (2013). Security as a theoretical attribute construct. Computers & Security, 37, 155-175.

Bodeau, D.J. and Graubart, R. (2011). Cyber Resiliency Engineering Framework. The MITRE Corporation. Accessed 6/12/2013. http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf.

Bodeau, D.J., Graubart, R., LaPadula, L., Kertzner, P., Rosenthal, A. and Brennan, J. (2012). Cyber Resiliency Metrics Version 1.0 Rev.1. Accessed 6/12/2013. The MITRE Corporation. http://www.mitre.org/work/cybersecurity/pdf/cyber_resiliency_metrics.pdf.

Bojanc, R. and Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management, 28(5), 413-422.

Booz Allen Hamilton (2011) Cyber Operations Maturity Framework: A Model for Collaborative, Dynamic Cybersecurity. Booz Allen Hamilton. Accessed 6/12/2013. http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf.

Boyens, J., Paulsen, C., Moorthy, R., Bartol, N. and Shankles, S.A. (2013). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161(Initial Public Draft). Accessed 27/03/2014. http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf.

Boyer, W. and McQueen, M., (2008). Ideal based cyber security technical metrics for control systems. In Proceedings of the Second international conference on Critical Information Infrastructures Security. pp. 246–260, Springer-Verlag, Malaga, Spain.

Boyson, S., (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, in Press. http://dx.doi.org/10.1016/j.technovation.2014.02.001i.

Cabinet Office (2011). The Cost of Cyber Crime. Accessed 20/3/2014. https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. and Robinson, W. (2008). Performance measurement guide for information security. National Institute of Standards and Technology (NIST) Special Publication 800-55 Revision 1. Accessed 27/03/2014. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

CIS (2010). The CIS Security Metrics: CIS Security Metrics (Version 1.1.0). The Center for Information Security. Accessed 6/12/2013. https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf.

Cisco (2013). Cisco Annual Security Report. CISCO Systems Inc. Accessed 6/12/2013. http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

CISWG (2005). Report of the Best Practices and Metrics Teams (Revised). Corporate Information Security Working Group. Accessed 6/12/2013. http://net.educause.edu/ir/library/pdf/CSD3661.pdf.

Congress.gov (2013). H.R.624 - Cyber Intelligence Sharing and Protection Act. Library of Congress. Accessed 26/03/2014. http://beta.congress.gov/bill/113th-congress/house-bill/624.

Cresswell, A. and Hassan, S. (2007). Organizational impacts of cyber security provisions: A sociotechnical framework. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences, January 2007.

Dorofee, A., Killcrece, G., Ruefle, R. and Zajicek, M. (2007). Incident Management Capability Metrics Version 0.1. Software Engineering Institute, Carnegie Mellon University. Accessed 6/12/2013. http//:www.cert.org/archive/pdf/07tr008.pdf.

ENISA (2010). Incentives and Challenges for Information Sharing in the Context of Network and Information Security. European Network and Information Security Agency. Accessed 27/03/2014. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing.

Fernandez, V, D., Acosta, O., Brown, S., Reid, E. and Spirito, C. (2012). Conceptual framework for cyber defense information sharing within trust relationships. In Proceedings of the 4th International Conference on Cyber Conflict (Czosseck, C., Ottis, R. and Ziolkowski, K. Eds.), pp. 429-445, NATO CCD COE Publications, Tallinn.

Finch, P. (2004). Supply chain risk management. Supply Chain Management: An International Journal, 9(2), 183 – 196.

Fleming, M.H. and Goldstein, E. (2012). Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts. http://ssrn.com/abstract=2201033

Gal-Or, E. and Chose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16 (2), 186-208.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22(6), 461–485.

Gov.uk (2013). The Cyber Information Sharing Partnership. Accessed 6/12/2013. https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security.

Hayden, L. (2010). IT Security Metrics: A Practical Framework for Managing Security and Protecting Data. McGraw-hill, New York.

Heyman, T., Scandariato, R., Huygens, C. and Joosen, W. (2008). Using security patterns to combine security metrics. In Proceedings of the third International Conference on Availability, Reliability and Security, 4-7 March 2008, pp. 1156-1163.

Hughes, A., Balasescu, M. and Balasescu, S. (2008). The role and importance of information technology in the supply chain management. Bulletin of the Transilvania University of Brasov, 5(1), 33-38.

InformationWeek. (2009). Securing the Cyber Supply Chain. Accessed 25/03/2014. http://www.informationweek.com/security/risk-management/securing-the-cyber-supply-chain/d/d-id/1084619?.

Inserra, D. and Bucci, S.P. (2014). Cyber Supply Chain Security: A Crucial Step toward U.S.

Security, Prosperity, and Freedom in Cyberspace. Accessed 25/03/2014. http://report.heritage.org/bg2880.

Jansen, W. (2009). Directions in Security Metrics Research. National Institute of Standards and Technology. Accessed 6/12/2013. http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf?q=applicationspecific-attacks-leveraging-the-actionscript.

Langweg, H. (2006). Framework for malware resistance metrics. In Proceedings of the second ACM Workshop on the Quality of Protection, October 30, 2006, pp. 39-44, Alexandria, Virginia, USA.

Levary, R. (2000). Better supply chains through information technology. Industrial Management, 42(3), 24.

Miani, R., Cukier, M., Zarpelão, B. and de Souza Mendes, L. (2013). Relationships between information security metrics: an empirical study. In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, article 22.

Mitre (2014). Common Vulnerabilities and Exposures List. Accessed 21/03/2014. http://cve.mitre.org/cve.

Patriciu, V.V., Priescu, I. and Nicolaescu, S. (2006). Security metrics for enterprise information systems. Journal of Applied Quantitative Methods, 1(2), 151–159.

Ponemon Institute (2013). Endpoint Security Report 2013. Ponemon Institute. Accessed 6/12/2013. http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf.

PricewaterHouse Cooper (2013). Security Report 2013. PricewaterHouse Cooper. Accessed 6/12/2013. http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf.

Pujara, A.A., Kant, R. and M.D. Singh. (2011). Information sharing in supply chain: Modeling the barriers. In Proceedings of the 2011 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 6-9 Dec. 2011, pp.918-922.

Sandoval, J.E. and Hassell, S.P. (2010). Measurement, identification and calculation of cyber defense metrics. In Proceedings of the 2010 Military Communications Conference, pp. 2174-2179.

Tawileh, A., Hilton, J. and McIntosh, S. (2007). Managing information security in small and medium sized enterprises: A holistic approach. In ISSE/SECURE 2007 Securing Electronic Business Processes, pp. 331–339, Springer-Vieweg.

TMForum (2013) TMForum Quick Guide Pack. TM Forum. Accessed 6/12/2013. http://www.tmforum.org/Guidebooks/GB965CyberOpsMetrics/49903/article.html.

Vaughn Jr., Rayford B., Henning, R. and Siraj, A. (2003). Information assurance measures and metrics - state of practice and proposed taxonomy. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 6-9 Jan. 2003.

Verizon (2013). Verizon Data breach Report [online]. Verizon. Accessed 6/12/2013. http://www.verizonenterprise.com/DBIR/2013/.

Voas, J., Ghosh, A., McGraw, G., Charron, F.A.C.F. and Miller, K.A.M.K. (1996). Defining an adaptive software security metric from a dynamic software failure tolerance measure. In Proceedings of the Eleventh Annual Conference on Computer Assurance, pp. 250-263.

Zahedirad, R. and Shivaraj, B. (2011). Supply chain: barriers and benefits Indian SMEs. SCMS Journal of Indian Management, 8(4), 11-30.