Implementing Cybersecurity in DoD Supply Chains

White Paper

Manufacturing Division Survey Results

July 2018

(This Page Intentionally Blank)

I. FOREWORD

Cybersecurity is not simply a corporate concern; it is a supply chain issue. This report explores how the United States Department of Defense supply chain has responded to the recent DFARS requirement. The results show that supply chain cybersecurity is critical but that the weakest link is the small to medium sized firm found in the upstream supply chain. Important recommendations are provided

II. PAPER DISPOSITION

The paper will be made available on the National Defense Industrial Association website as a reference resource at the following: (http://www.ndia.org/divisions/manufacturing/resources). Permission is granted to widely distribute and quote from the paper with proper attribution.

III. PRINCIPAL AUTHORS

The following were the principal authors of this report which was based on a survey of small and medium-sized businesses conducted at Michigan State University by Dr. Steven Melnyk. The principal authors of this report are:

- Steven A. Melnyk, Ph.D., Michigan State University; University of Newcastle (AU)
- Chris Peters, The Lucrum Group
- Joseph Spruill, Captain USN (Ret.), Lockheed Martin Corporation and Industry Chair at the National Defense University's Eisenhower School for National Security and Resource Strategy
- Kenneth W. Sullivan, Ph.D., Micro Craft, Inc.

This report was reviewed by members of the Manufacturing Division prior to being published. It was also reviewed by members of the Cybersecurity Division, which has an active Supply Chain Committee concerned with the same issues highlighted in this report.

For more information on the Manufacturing Division including a schedule of meetings may be found at Http ://www.ndia.org/divisions/manufacturing.

(This Page Intentionally Blank)

IV. TABLE OF CONTENTS

V. LIST OF TABLES AND FIGURES

1 EXECUTIVE SUMMARY

1.1 Overview

In today's environment, where innovation and responsiveness are critical performance requirements and where digital is becoming increasing important, cybersecurity must become an imperative. Often, management views cybersecurity as primarily an Information Technology (IT) and corporate issue. Yet, this perspective is too narrow and too limited. Cybersecurity is also a supply chain issue that also must be addressed across all facets of a company's business. Recognizing this "fact of life", the United States Department of Defense (DOD) recently introduced a new DFARS requirement aimed at ensuring appropriate levels of cybersecurity in any supplier involved in the DOD supply chain. This requirement has met with resistance. In this study, we explore how members of the DOD supply chain are responding not only to this requirement but also to cybersecurity in general. The resulting analysis and recommendations are critical and should be acted upon within not only the DOD supply chain but also with any supply chain that deals with IT and intellectual property (IP) and where its digital system offers an attractive target of opportunity.

1.2 Major Findings

- Overall, respondents had an uneven awareness of cybersecurity: they appreciated the need for protection of IT/IP; there was far less support for operational aspects.
- Most small- to medium-sized (SME) suppliers have a poor understanding of cybersecurity.
- Understanding of both the mandatory DFARS requirements and the underlying NIST framework are limited.
- Most firms in the early stages of implementation severely underestimate the costs of becoming compliant by as much as a factor of 10.
- Respondents see the DFARS requirements not as something that is economically justified but rather as a cost of doing business (along with all that this view brings).

1.3 Major Recommendations

1.3.1 For the Federal government:

Develop awareness that cybersecurity is both a national and economic security issue within the supply chain.

Help simplify the process of meeting the new DFARS requirement.

Focus immediate implementation emphasis on critical flight or programmatic items in the supply chain.

Develop a certification program focusing on supply chain cybersecurity.

1.3.2 For Prime Contractors:

Help develop a compelling business case for cybersecurity.

Help the SMEs by developing and using appropriate measures of cybersecurity.

Treat SME suppliers appropriately, as to whether they are early or late adopters, by rewarding proactive implementation.

1.3.3 For Small/Medium Sized Suppliers

Focus on improving knowledge and awareness regarding cybersecurity.

Understand that cybersecurity is now a cost of doing business in today's cyber/digital market.

Understand that cybersecurity is a corporate responsibility – one that cannot be subcontracted.

2 Understanding the Need for Supply Chain Cybersecurity

In October 2016, the Department of Defense (DOD), in response to increasing cyber risks in its supply chain, included a new mandatory clause in the Defense Federal Acquisition Regulations Supplement (DFARS) -- "Safeguarding covered defense information and cyber incident reporting" (DFARS 252.204-7012). This DFARS requirement was based on the National Institute of Standards and Technology (NIST) publication "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (Special Publication 800-171). The announcement in October 2016 informed suppliers they had until December 31, 2017 to be fully compliant. Failure to be compliant would result in termination of their status as DOD suppliers.

Anecdotal evidence involving these defense suppliers has indicated that the imposition of this requirement has created numerous concerns. Some included confusion over what was needed to be considered compliant, concerns regarding the costs and benefits (if any) of becoming compliant), and the short-term problems possibly created by being compliant. On this latter point, some firms expressed fears of being at a cost disadvantage relative to other suppliers who have decided NOT to pursue compliance (these suppliers did not have to incur the same costs faced by the suppliers who were pursuing DFARS compliance).

Finally, there is concern over whether the DOD is serious enough to be willing to reduce its supplier base during a time where there is trepidation regarding whether there are enough capable suppliers to serve DoD readiness and sustainment needs.

To assess the response of the DOD supplier base to this mandate, the National Defense Industry Association (NDIA) in conjunction with the Department of Supply Chain Management, Michigan State University, developed and deployed a survey designed to capture the reactions and perceptions of this group to these new mandates.

This study reports the results of this survey. Specifically, this study is intended to address the following questions:

- To what extent are the DOD suppliers complying with this new mandate?
- What differentiates the early adopters of the mandate from the late adopters?
- What type of firm is likely to be an early adopter when it comes to this mandate?
- How is cybersecurity viewed by the DOD supplier?
- What factors affect or influence the decision to pursue cybersecurity improvement?

Before proceeding to the theoretical foundations of this study, it should be noted that this is one of the first empirically based studies into cybersecurity, improving corporate resilience to cyber threats, and the factors affecting corporate receptiveness to mandates such as DFARS 252.204-7012. As such, this study can be regarded as exploratory since one of its goals is to frame the issues and challenges surrounding cybersecurity within the supply chain.

3 DFARS 252.204-7012 – Understanding the Mandate

The DOD released a revised mandate of DFARS 252.204-7012 "Safeguarding covered defense information and cyber incident reporting" in October of 2016. The revision provides compliance requirements for cloud computing, preferred security protocols, and subcontractor compliance regarding covered defense information, controlled technical information, or controlled unclassified information.

The previous set of terms seems to be used in similar context; therefore, a reasonable definition would be the one listed by the National Archives. In summary, covered defense information would be all information "subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination" (CUI Registry, 2017). The introduction of the NIST framework provides a more simplified specification of controlled unclassified information: "only information that requires safeguarding or dissemination controls pursuant of federal law, regulation, or government wide policy" (Ross, et. al, 2015). From these guidelines, the key takeaways are found:

- Provide adequate security on all covered information systems including cloud computing software
- Implement NIST SP 800-171 recommended cybersecurity standards on all systems relative to the contract (with exception to cloud computing)
- Rapid Incident reporting or within 72 hours of the knowledge of the incident.
- Information and retrievable evidence relative to the incident should be included in the report
- Subcontractors are subject to similar requirements with added reporting responsibilities. Subcontractors are required to report a breach to both their customer and continuously through the supply chain with the DOD as the final node for communication.

4 NIST SP 800-171 Framework.

Central to the DFARS mandate is the NIST framework. This framework originated from attempts by the executive branch to standardize inconsistencies in the management, control and protection of unclassified information held within suppliers IT platforms as they have evolved and become more and more networked. Initially, this framework was targeted towards governmental agencies. To avoid unnecessary redundancies, the framework was subsequently modified – resulting in the NIST Special Publication 800-171.

The major contribution of this publication was that it eliminated criteria not required for non-governmental stakeholders. The framework provides a baseline for a moderate security approach incorporating fourteen security families based on this requirement. The NIST framework also connect the proposed recommendations to ISO 27001 Information Security Management requirements with the intention of simplifying alignment initiative of the proposed framework to current widely implemented technological security standards.

5 DFARS as Certified Management Standard – Understanding the Adoption Process

Having set the stage, the next challenge is that of providing the theoretical framework to be used to drive the empirical data collection and analysis. Given that DFARS is a mandate, it can be regarded as a form of certified management standard (CMS). For the purposes of this study, we define a CMS using the framework offered by ISO, the International Organization for Standardization (ISO. 2015): *a model for firms to follow when setting up and operating a management system to achieve a specific outcome, whereby the implementation and execution of the practices associated with the specific outcome have been externally validated.*

That is, a CMS specifies a desired outcome (in the case of this study, this is improved cybersecurity); it also identifies specific practices that are strongly correlated with the presence of the desired outcome. Finally, a CMS also specifies the minimum level of performance that must be attained for the organization to be considered compliant with the CMS.

Next, using the theoretical perspective used by Ritchie and Melnyk (2012), Melnyk, Ritchie, and Calantone (2013), and Ni, Melnyk, Ritchie, and Flynn (2016), in their studies of the C-TPAT (Customs – Trade Partnership Against Terrorism) CMS, we treat DFARS 252.204-7012 as a form of administrative innovation. When viewed from this perspective, research into CMS often focuses on two critical decisions:

- whether to pursue the new standard; and
- when to implement the new standard.

For the purposes of this study, we make the critical assumption that since this mandate has been specified for any supplier wishing to be part of the DOD supply chain, the decision of whether to pursue has, for most firms, already been made. Consequently, this study will focus on the timing decision. There is, however, anecdotal evidence that some suppliers may choose to abandon the DoD market rather than suffer the expense of complying with the DFARS mandate.

Central to the question of the timing decision this study explores how the following factors influence the adoption process:

- size of the firm;
- resource levels of the firm;
- views of cybersecurity; and
- level of commitment to and importance of the DOD to the respondent.

6 Research Methodology

To address the research questions posed earlier in this paper and to help us better understand the factors influencing the adoption process, a survey was developed and implemented jointly by personnel from the NDIA and the research team from the Department of Supply Chain Management at Michigan State University. Critical to the survey was its structure that enabled the collection of both quantitative and qualitative data.

The survey was developed and deployed using Qualtrics – an on-line platform that can be used to develop and distributes on-line surveys and to collect and do initial analysis of the resulting data. The initial survey was pre-tested by a panel of practitioners and academics knowledgeable in supply chain management, cybersecurity and DOD business. The survey was administered and completed in 2017. All the data collected was statistically evaluated using STATA 14.0. The audiences targeted for the survey were practitioners who were members of the NDIA.

7 Summary of Findings

Initially, the survey was circulated to a wide range of NDIA members and attracted 395 respondents. The survey included a qualification question to identify those respondents who manufactured or supplied components and services to the DOD. The question was used to remove NDIA members who were consultants, academics, or governmental members. This question combined with a question querying whether the participant wanted to continue to participate resulted in a reduced sample of 227. Finally, it should be noted that participants were not required to answer questions.

The presentation of results will be done using the following structure:

- Demographic information about the respondents and their companies;
- Initial Attitudes to DFARS 252.204-7012 and the associated NIST document;
- Investment Patterns regarding DFARS 252.204-7012;
- Factors influencing the decision to be an early adopter relative to be a late adopter; and,
- Qualitative Insights.

This white paper will only address a few of the key responses.

The details of the survey will be available in a white paper published by Dr. Steven A. Melnyk, Michigan State University.

7.1 Key Demographic Information about the Respondents

The remaining respondents were asked to provide some demographic information about themselves and their companies. Listed below is a summary of the key demographics responses:

- Approximately one-half of the respondents were small businesses (less than 500 employees)
- Fifty-seven percent of the respondent's organization, the DoD business was very important since it accounted for at least fifty percent of their revenue.
- Eighty percent of the respondents had been DoD suppliers for at least ten years.
- Forty-one percent of the respondents' company's revenues for 2016 exceed $50 million.
- Seventy-five percent of the respondents functioned as prime and/or first tier suppliers.

7.2 Initial Attitudes to Cybersecurity Mandates

This section focuses on how the respondents viewed the various dimensions of cybersecurity, DFARS 252.204-7012, and the supporting NIST risk management framework. First, the respondents were asked to assess the perceived risks of the three dimensions of cyber security (business system threats, factory/shop floor threats, IT/IP threats). The results are summarized in Table 1 and shown in Figure 1.

As can be seen from this table and figure the respondents viewed all three dimensions of cybersecurity as important, with the highest emphasis being on IT/IP Threats and Business System Threats. Factory/shop floor threats were not viewed as being as high relative to the prior two.

Not surprisingly, the level of company efforts (see Table 2 and Figure 2) of the respondents is strongly consistent and correlated with the expressed level of perceived risks, with most of the attention being paid to Business System IT/IP threats.

Table 1 – Perceived Cybersecurity Risks

Level of Perceived Risk	Business System Threats		Factory/Shop Floor Threats		IT/IP Threats	
	Frequency	***Percent***	***Frequency***	***Percent***	***Frequency***	***Percent***
No Concern	1	0.51	17	8.76	3	1.53
Low	14	7.14	38	19.56	7	3.57
Medium	32	16.33	48	24.74	16	8.16
High	68	34.69	57	26.29	64	32.65
Extremely High	81	41.33	40	20.62	106	54.08
Summary	196	100.0	194	100.0	198	100.0
Average	4.09		3.30		4.53	
Std Deviation	0.957		1.245		0.889	

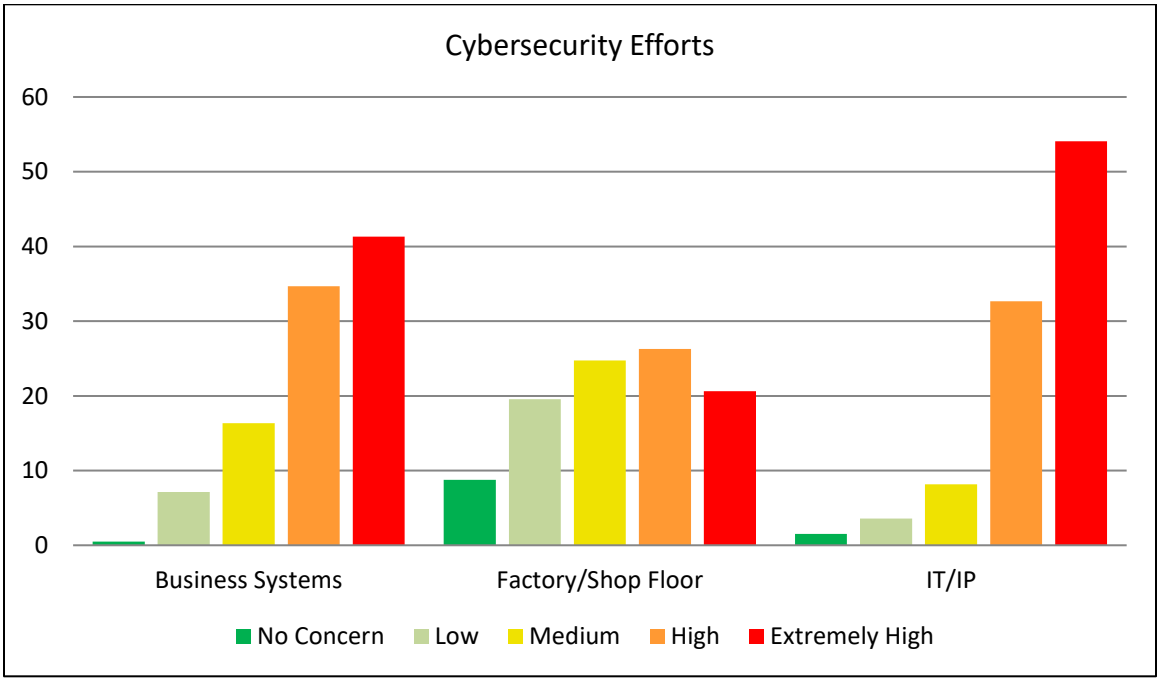

Figure 1 –Risk Perception across Enterprise Dimensions

Table 2 –Cybersecurity Investment Efforts

Level of Perceived Risk	Business System Threats		Factory/Shop Floor Threats		IT/IP Threats	
	Frequency	***Percent***	***Frequency***	***Percent***	***Frequency***	***Percent***
No Concern	1	0.5	13	6.70	1	0.57
Low	14	7.22	35	18.04	12	6.09
Medium	37	19.07	46	23.71	30	15.23
High	74	38.14	53	27.32	59	29.95
Extremely High	68	35.05	47	24.23	95	48.22
Summary	194	100.00	194	100.00	197	100.00
Average	4.00		3.44		4.19	
Std Deviation	0.939		1.226		0.944	

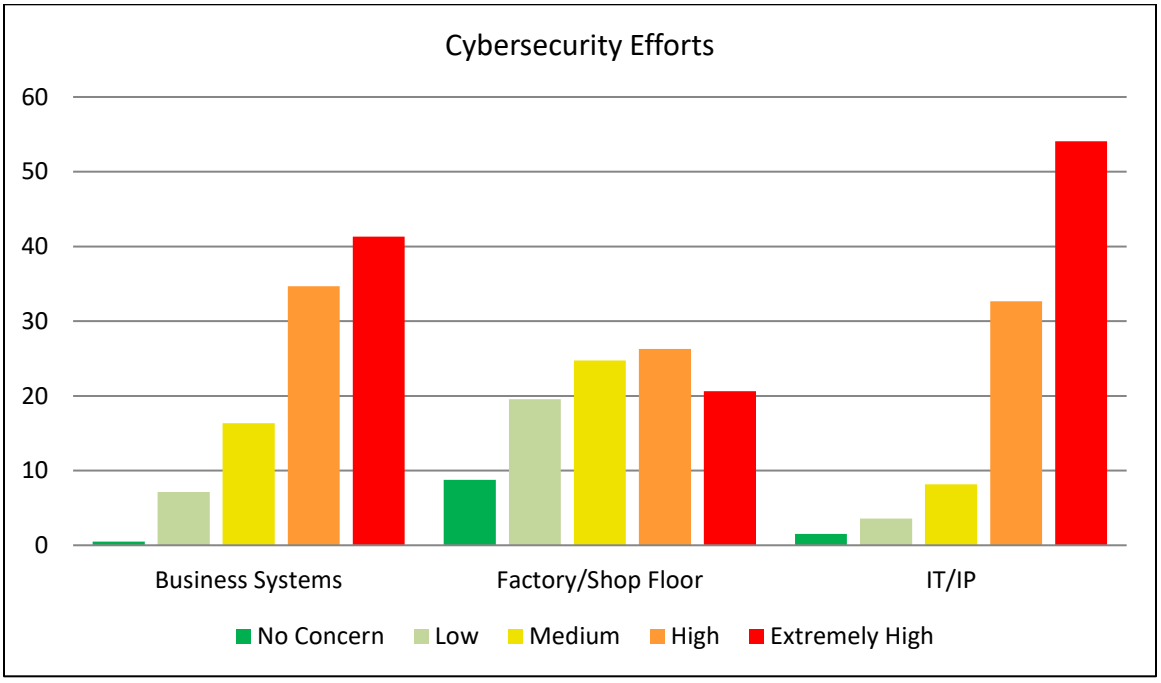

Figure 2 – Cybersecurity Investment Efforts Across Enterprise Dimensions

The NDIA Manufacturing Division has addressed the concerns regarding factory and shop floor systems in a series of reports: Cybersecurity for Advanced Manufacturing. The joint working group identified ways for the Department of Defense (DoD) and its prime contractors to assist manufacturers, particularly small and medium enterprises (S&MEs) to improve cybersecurity.

(See http://www.ndia.org/divisions/working-groups/cfam for final CFAM report).

7.2.1 Assessing Initial Attitudes to DFARS 252.204-7012

The next step was to assess the initial attitudes to the new DFARS requirement and the other associated supported material. To this extent, the respondents were asked a series of questions regarding these issues. An analysis of the results indicated the following:

- Awareness of the mandatory DFARS requirement was limited, with only 63.82% (127 out of 199) indicating that they were aware of the new requirement.
- Many of the respondents have not even read the new DFARS requirement documentation (less than 60% (99 out 166) indicating that they had even read this document).
- Many of the respondents (46.46%) indicated that they found the DFARS requirements to be difficult to understand.
- A large minority of the respondents (i.e., just over 45% or 79 out of 173 respondents) had not read the NIST publication, "Protecting Controlled Unclassified Information" – a document that forms the theoretical foundation for the new DFARS mandate.
- Many of the respondents felt that the NIST document was difficult to understand, with only 39.59% (39 out of 91) indicating that they felt that this document was clear and easy to understand.

In short, there was significant confusion regarding both the DFARS mandate and the associated NIST document. This confusion is a potential factor influencing the analysis presented in the next section.

7.2.2 Additional Analysis

In further analysis of the data carried out by Professor Melnyk and his research team, additional key findings were uncovered, namely:

- Firms in the early stages of implementation tend to underestimate the cost of implementation by as much as a factor of 10.
- Firms that understand the value of cybersecurity to their business were more likely to be early adapters.

- Respondents viewed the DFARS mandate more as a requirement for doing business with DoD than something that could be economically justified.

8 Discussion of Results

The results of the survey paint an interesting picture of early adopters. In general, these are relatively large firms that strongly believe in the value and need for cybersecurity. They are highly dedicated to the DOD as a customer. While these insights are important, they are not complete. What we have not done is to understand the factors motivating the late adopters.

On one hand, it can be argued that the late adopters should be working on meeting the DFARS mandate. After all, it is a requirement for being a supplier to the DOD. In addition, meeting this requirement had a firm deadline – December 31, 2017. Consequently, it is important to understand why these firms are hesitant. It should be noted that after this survey was complete, the DoD decided to permit suppliers to have a Systems Security Plan (SSP) and a POAM (Plan of Action and Milestones) in place by December 31, 2017 rather than be fully compliant.

First, it can be seen, from the results previously reported, that these firms significantly under-estimated the costs of meeting the new mandate. Second, there is additional information that can be used to understand the concerns raised by these late adopters. The survey collected not only quantitative data but also qualitative data. That is, the respondents were encouraged to share their insights and concerns at several points in the survey. In reviewing these qualitative comments, a tentative picture of the late adopter begins to emerge.

In many ways, the late adopter appears to exhibit many of the same traits of the early/late majority adopters, as described by Moore (1991), in his book, "Crossing the Chasm." Moore identified five categories of adopters: innovators, early adopters, early majority, late majority, and laggards. He also argued that separating the early adopters from the early majority was a chasm – a chasm that caused the failure of many feasible innovations. Furthermore, he described the critical traits associated with early majority users – traits that were evident when reading over the comments.

Early majority users are pragmatists; they are also risk averse. They are not likely to buy into new innovations unless there is widespread acceptance of this innovation in the marketplace. They are driven by economic considerations. For them to embrace any new innovation there must be a compelling business case. They want to see the innovation working elsewhere so that they can see it in act and they can talk with the people associated with its use and operation.

Like the early majority of Moore (1991), the late adopters could be described as risk adverse. They wanted to know more about the new DFARS mandate and what had to be done to satisfy it. They were concerned because they could not make a compelling business case for the adoption of the new DFARS mandate. They were interested in knowing firms had already met this mandate so that they could visit those firms and see first-hand the requirements and impact. Because they had difficulty in identifying the economic benefits, their focus drifted to lowering the costs of meeting

the new mandate. That meant that they were interested in templates, identification of efficient practices, support from the DOD in terms of implementation and education. They were faced by uncertainty – an uncertainty that was shared by the DOD – and they were interested in reducing this level of uncertainty. They were waiting in the hopes that the level of overall uncertainty could fall along with the level of support and guidance increase. The only question left unresolved was that of whether they would have enough time in which to attain the DOD DFARS mandate by the deadline currently in place.

The other issue that needs to be discussed is that of the increasing importance of enhanced cybersecurity. There are five aspects of this importance that must be recognized. The first is that it should not be regarded as an IT issue. Improving cybersecurity is not simply a matter of hiring more IT people or buying a new piece of software that promises improved protection. Rather, it must be integrated into the business process and it must become everyone's responsibility. This is a position that we are starting to see emphasized by numerous consulting companies such as Bains and Company (2014) and Gartner (Panetta, 2017).

Second, cybersecurity is no longer a corporate/internal affair – it is a supply chain issue and it also impacts all areas of a company's business systems. Companies and governmental agencies are now recognizing that the real vulnerabilities in their cyber environments does not lie in the primes – it lies in the second and third tiers. As previously noted in this paper, most of the major security breaks have occurred through the supplier side of the supply chain.

Third, we can expect the level of cyber-attacks to increase in the future. In a recent report, Morgan (2017) identified five major trends in cybersecurity: (1) cybercrime damage costs to expected to hit $6 trillion annually by 2021; (2) cybersecurity spending is expected to exceed $1 trillion USD from 2017 to 2021; (3) cybercrime will more than triple the number of unfilled cybersecurity jobs; (4) human attack surface to reach 6 billion people by 2022; and, (5) global ransomware damage costs are expected to exceed $5 billion in 2017. These trends underlie the increasing importance of cybersecurity and its associated activities. Is it any wonder that Ginni Rometty, IBM's Chairman, president, and CEO said on November 3 2015 that "Cyber Crime Is The Greatest Threat To Every Company In The World" (Morgan, 2015). In fact, Warren Buffet went further, when he called cybersecurity the number one threat to all mankind – even more so than nuclear weapons (Morgan, 2017). These threats were largely supported by McAfee in its 2017 Threats Predictions (2016).

Fourth, the level of awareness of cybersecurity and the level of resources available for this activity is lowest in the small to medium sized enterprises. Consequently, when taken with the preceding developments, we find ourselves facing a "perfect storm" when it comes to cybersecurity – increased importance of cybersecurity combined with awareness of the threats coming from the supply chain and few resources or low awareness of the small to medium sized enterprises – the firms most likely to be found at the lower levels of the supply chain.

Finally, in conversations with several managers from small to medium sized firms who were NDIA members, a critical clash began to emerge. Today's supply chain, irrespective of whether it is

focused on private business or the DOD, is faced by the increased importance of speed (Melnyk & Stanton, 2017). Yet, in discussions with these managers, it was found that a common strategy used to deal with cybersecurity threats is to "wall off" the affected areas. What this strategy does is not only to reduce the exposure to cybersecurity threats but also to reduce the overall responsiveness of the system. This trade-off must be resolved.

9 Recommendations

Due to the depth and breadth of these issues, recommendations have been developed for the government, the prime contractors and the suppliers.

9.1 Federal Government

9.1.1 Cybersecurity is both a national and economic security issue within the supply chain.

The Federal Government needs to educate the entire United States Industrial Base on issues involving cybersecurity. The DoD may wish to work with the Department of Commerce or associated organizations to raise awareness along with economic cost to the US gross national product through loss of intellectual property.

9.1.2 Help simplify the process of meeting the new DFARS requirement.

This can be done in numerous different ways: (1) developing templates that the small to medium-sized enterprise (SME) suppliers can follow; (2) identifying effective practices; (3) publishing case studies describing other organizations' experience in implementing effective cybersecurity systems; and, (4) developing and deploying measures associated with cybersecurity (such measures are important because they help to communicate to the rest of the organization the fact that cybersecurity is important and how it is operationally defined). The DOD and other organizations must take a more active role in pushing the SMEs to become better protected. They must convince their supplier base that cybersecurity is important; it can be done; it works; and, it may have benefits that exceed beyond simply meeting the DFARS mandate. The industrial base must understand their responsibility and the risk of violating and/or losing contracts should they not comply. **It should be noted, as of the publication of this paper, NIST has provided further guidance (on their website) including System Security Plan (SSP) and Plan of Action and Milestones (POAM) templates.**

9.1.3 Initially focus on critical hardware in the DoD Supply Chain.

Instead of attempting to implement the DFAR Cybersecurity requirements across the entire depth and breadth of the DoD Industrial Base, the DoD should consider focusing immediate implementation on critical flight or programmatic items in the supply chain. Such items might include avionics, propulsion systems and/or critical aerodynamic features.

9.1.4 Develop certification.

The DoD need to encourage some type of certification like ISO 9001 and 27001 or expand that certification to include cybersecurity.

9.2 Prime Contractors

9.2.1 Help develop a business case for cybersecurity.

Currently, the results indicate that most of the respondents view the DFARS requirement as something that the firm must do to qualify for DOD business. Such an attitude does really encourage aggressive investment; rather, it encourages just enough spending to be seen as being compliant. For firms in the supply chain to embrace cybersecurity, a quantitative business case for cybersecurity must be developed. This case must help the firm see how the costs of investing improved cybersecurity are far outweighed by the resulting benefits. Such an argument is compelling for early to late majority types of firms. It is currently lacking.

9.2.2 Help the SMEs by developing and supporting the use of appropriate cybersecurity-based measures.

Measures play a critical role in the firm. They facilitate the identification and correction of problems; more importantly, they communicate importance. That is, when something is measured, the act of measurement tells everyone in the firm that the activity being measured is important. When something is not measured, then effectively, the message to the rest of the firm is that the activity is not important. Measures also make issues like cybersecurity operationally clear. Currently, the DOD supply chain has a lack of appropriate, widely used cybersecurity related measures. These measures are needed because of the functions that they fulfill.

9.2.3 When dealing with SME suppliers, treat them as either early or late majority.

Geoffrey Moore, in his famous book, *Crossing the Chasm*, noted all firms, when faced by innovation (the new DFARS can be regarded as an example of such an innovation), fall into one of five categories: (1) innovators, (2) early adopters, (3) early majority, (4) late majority, or (5) laggard. Furthermore, Moore noted that most firms fell into the early majority category. These were firms that were very risk-adverse; they needed to see the innovations in practice before they would commit their firm; they needed a compelling, quantitatively (read, money) based argument for adopting the new development. These traits fit the majority of the SMEs to a "T". Once you recognize these traits, then the way forward is relatively straight forward. You help them develop a compelling business case that can be justified in terms of dollars and cents. You help these firms by identifying other firms that have gone through the process and that have become certified – these become the companies that others visit to learn first-hand about the process of pursuing compliance and of the impact of compliance on performance. Finally, you develop an infrastructure consisting of conferences where management from the firms pursuing enhanced cybersecurity can meet others

and where they can learn about what is involved and what steps their firms should go through. In other words, you support and encourage their activity rather than mandating compliance.

9.3 Small/Medium Enterprises

9.3.1 Focus on improving the level of knowledge regarding cybersecurity.

The findings strongly indicate that the level of knowledge and support for cybersecurity is lowest in the small to medium sized enterprises. For example, when a pairwise correlation was carried out between cybersecurity and SME firms, a significant negative correlation was noted. This indicated that the SME was less likely to see cybersecurity in a positive light. This finding should not be interpreted as indicating that these firms were against cybersecurity. Rather, it reflects several factors: (1) cybersecurity is a relatively new development; (2) SME lack resources both financial and managerial for addressing cybersecurity issues; and, (3) there is a great deal of confusion surrounding the concept of cybersecurity.

9.3.2 SME firms must recognize that Cybersecurity is part of doing business now.

As stated earlier, Cybersecurity is a national security issue. It is anticipated that other industries (i.e. automotive) will follow suit. SMEs must adapt to this new way of doing business or face extinction.

9.3.3 SME firms cannot subcontract out Cybersecurity accountability and responsibility.

Even though SME's usually subcontract out many activities that large firms have entire staffs, responsibility for Cybersecurity cannot be handled in this manner. SME's may be able to use subcontractors or consultants to greatly assist them in the implementation; however, the SME's culture must change to recognize this threat is a 24 hour a day/7 day a week activity.

10 Concluding Comments

Cybersecurity is now becoming new battlefield for supply chain management. In this study, we have attempted to lay out the reasons that we believe so strongly in this position. We have also examined the challenges facing the first supply chain focused attempt at improving cybersecurity.

In studying the challenges facing the DOD, in implementing DFARS 252.204-7012, we see issues that are not unique to the DOD; they are supply chain issues. We have sought to understand the differences between the early and late adopters. We have found that the early adopters tend to be large companies who fundamentally believe in the value of cybersecurity and its need.

We also found that the late adopters not only tend to underestimate the costs of improving cybersecurity (by a factor of 10x); they also tend to be very traditional in terms of their response to innovations such as cybersecurity. They are looking for guidance in understanding and improving

cybersecurity; they are also looking for assistance in developing a compelling business case for improving cybersecurity.

These factors, when combined, present the supply chain management researcher with a rare opportunity to do research that is not only needed but that is also being demanded by practitioners. It is a chance for supply chain management to "shine". We hope that this study encourages future similar studies into this emerging and increasingly critical issue.

11 References

Bains and Company. 2014. "Why Cybersecurity is a Strategic Issue." *Insight*. February 12 2014. http://www.bain.com/publications/articles/why-cybersecurity-is-a-strategic-issue.aspx. Accessed November 3 2017.

International Organization for Standardization (2015). *Management System Standards*. http://www.iso.org/iso/home/standards/management-standards.htm. (accessed 4 April 2015).

McAfee. 2012. *Threat Predictions*. https://www.mcafee.com/au/resources/reports/rp-threat-predictions-2012.pdf. Access 11/3/2016.

McAfee. 2016. *McAfee Labs: 2017 Threat Predictions*. November 2016. https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf. Accessed November 3, 2017.

Melnyk, S.A., Stanton, D.J. 2017. The Customer-Centric Supply Chain. *Supply Chain Management Review*. July/August. Pp. 8-17.

Melnyk, S.A., Ritchie, W.J., Calantone, R.J. 2013. "The Case of the C-TPAT Border Security Initiative: Assessing the Adoption/Persistence Decisions when Dealing with a Novel, Institutionally Driven Administrative Innovation." *Journal of Business Logistics*. Vol. 34, No. 4 (December), 289-300.

Moore, G. A. 1991. *Crossing the chasm: Marketing and selling technology products to mainstream customers*. New York, N.Y.: Harper Business.

Morgan, S. 2015. "IBM's CEO on Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'". *Forbes.* November 23, 2015. https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#2e85548973f0. Accessed November 3 2017.

Morgan, S. 2017. "Top 5 cybersecurity facts, figures and statistics for 2017." *Cybersecurity Business Report*. October 19, 2017. https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html. Accessed November 3, 2017.

National Defense Industry Association's Manufacturing Division and Cyber Division. 2014. *Cybersecurity for Advanced Manufacturing: A White Paper*. May 5, 2014.

Ni, J., Melnyk, S.A, Ritchie, W.J., and Flynn, B.B. 2016. "Why be first, if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification." *International Journal of Operations and Production Management*. Vol. 36, No. 10, 1161-1181.

Panetta, K. 2017. "Link cybersecurity to business outcomes." *Smarter with Gartner.* February 13, 2017. https://www.gartner.com/smarterwithgartner/link-cybersecurity-to-business-outcomes/. Accessed November 3 2017.

Ritchie, W. and Melnyk, S.A. 2012. "The Impact of Emerging Institutional Norms on Adoption Timing Decisions: Evidence from C-TPAT - a Government Antiterrorism Initiative." *Strategic Management Journal*. 33(7), pp. 860-870.

StataCorp. 2015. *Stata Statistical Software: Release 14*. College Station, TX: StataCorp LP.

-- END --