SENATE ARMED SERVICES COMMITTEE
Subcommittee on Cybersecurity

Christopher Peters
CEO, The Lucrum Group

Testimony on the cybersecurity responsibilities of the defense industrial base.

March 26, 2019

INTRODUCTION

Chairman Rounds, Ranking Member Manchin and distinguished members of the subcommittee. Over the past two years, I visited more than 200 small- to medium-sized manufacturers (SMMs) in the Defense Industrial Base (DIB) through work on various DoD-funded projects. I helped develop and analyze surveys that reached out to hundreds more. One of the primary topics in my research was manufacturing cybersecurity in the defense industrial base. Through my involvement with the National Defense Industrial Association (NDIA), I was a senior advisor to the Cybersecurity for Advanced Manufacturing Joint Working Group, consisting of participants from industry, the Pentagon and other government agencies. I am also a co-author on the NDIA paper, "Implementing Cybersecurity in DoD Supply Chains."[1]

BACKGROUND

Before I discuss some of the key findings from that research, I'd like to make an important distinction between information technology (IT) and operations technology (OT). IT consists of business applications and equipment, such as financial systems or enterprise resource planning software. OT includes industrial control systems and software that run machinery on the shop or plant floor.

The priorities for protection of IT are confidentiality, integrity and availability. The priorities for OT are reversed, with availability being the most important. As an example, it's not uncommon to find plant floor computers with the password taped to the machine so that if there is a production problem, someone can log in and quickly correct the issue.

IT typically uses modern operating systems and applications that are regularly patched and maintained. OT systems often consist of custom applications running on old operating systems, such as Windows NT or DOS. These systems cannot be easily patched or upgraded, as it may negatively impact production. Anti-virus software and firewalls cannot easily be added to OT environments, as they also may impact production.

In short, cybersecurity vulnerabilities are considerably greater in OT than in IT. These are easily exploited portals to steal or alter information or even shut down production. One example of an

[1] NDIA, "Implementing Cybersecurity in DoD Supply Chains," July 2018. http://www.ndia.org/-/media/sites/ndia/divisions/manufacturing/documents/cybersecurity-in-dod-supply-chains.ashx?la=en

OT breech is Lubrizol, where hackers stole intellectual property through the industrial control systems, causing significant financial damage. Another example is a German steel mill, where hackers took over the production control systems and caused significant physical damage.

This distinction between IT and OT is important, because it means the cybersecurity threats to the DIB are even greater than most realize.

KEY FINDINGS

Through my work, there are three key findings that I would like to present to this committee.

#1 The defense industrial base is at considerable risk

Most of the SMMs surveyed rate the importance of cybersecurity on the plant floor a lower priority than IT and intellectual property, even though OT represents the greatest risk. Sixty percent of the respondents to the NDIA survey have not read the DFARS documentation, and 46 percent of those who did said that they found it difficult to understand. Forty-five percent of the respondents had not read the NIST 800-171 publication, and only 40 percent of those who did felt that the document was clear and easy to understand.

What the research found was that SMMs have a poor understanding of cybersecurity in general. They often don't understand the threats, much less what action should be taken. The educational information that does exist, such as the 170-page document titled "NIST MEP Cybersecurity Self-assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements," is confusing and not written for SMMs, which often have little technical support.

For companies that do understand the threats and want to act, the lack of viable solutions that do not negatively impact operations is a barrier to adoption. We found those companies that did begin adopting cybersecurity solutions tend to underestimate the cost of implementation by as much as a factor of 10.

The overall lack of awareness and preparedness by the SMMs in the DIB should be alarming for a variety of reasons. The large manufacturers in the DIB typically have very robust security measures for both their business and operations systems. That makes the less knowledgeable and poorly defended SMMs a greater target for cyberattacks, particularly since they often handle much of the technical data sent from the larger contractors. Whether the attack is to steal intellectual property, introduce defects into military products or shut down entire operations, the SMMs are prime targets.

#2 Manufacturers are quitting defense work

SMMs have quit defense work because of the new DFARS cybersecurity requirements. Rather than recognizing that these cybersecurity precautions are something they should take regardless, they perceive the new DFARS requirements as just one more burden the DoD is imposing.

There are several factors that contribute to this situation. One is that the SMMs were not educated on the cyberattack threats and potential impact on their businesses, whether commercial or defense. Our findings have shown that there is an uneven awareness of cybersecurity risks and prevention, particularly for operations technologies.

Compounding the challenges facing manufacturers is that the DFARS requirements were written largely for IT systems, and many of the controls cannot be easily implemented in manufacturing environments without causing harm.

Finally, SMMs leaving the DIB cited a lack of clarity by the DoD on requirements, timing and enforcement. That lack of clarity is exacerbated by the confusing messages from many consultants, some even offering to help SMMs become "DFARS Certified." There is no such thing as "DFARS Certified." Many of these consultants have gouged the SMMs.

#3 Manufacturers are increasingly frustrated by uneven enforcement

Manufacturers are increasingly frustrated by uneven enforcement of the DFARS cybersecurity regulations. Some companies have incurred significant overhead expense to become DFARS compliant, while competitors that have not acted or have simply lied about compliance are still winning DoD business.

The lack of established metrics against which to measure the level of compliance is viewed by many manufacturers as a weakness that other suppliers will exploit. That perception of inequality or a lack of fairness is often a barrier to adoption of costly cybersecurity practices and solutions.

RECOMMENDATIONS

#1 Better educate the SMMs

Awareness is the first step in driving adoption, yet most SMMs in the DIB have not been made aware of the cybersecurity threats to their businesses. A coordinated government campaign should be targeted to the SMMs to raise awareness of the threats and the steps necessary to protect their businesses. Much like the “Loose Lips Sink Ships” campaigns of World War II, awareness campaigns are a cost-effective means to quickly spur the desired action throughout the entire U.S industrial base.

#2 Address the unique needs of operations technology

A key recommendation in the NDIA “Cybersecurity for Advanced Manufacturing” white paper is “Work with DoD stakeholders in cybersecurity policy, acquisition policy, sustainment policy, and procurement policy to ensure manufacturing requirements are adequately addressed in policy documents and implementation reviews; and develop separate guidance to protect OT networks where needed.”[2]

[2] NDIA, “Cybersecurity for Manufacturing Networks,” October 2017. P12 https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023.ashx?la=en

#3 Increase emphasis on resilience to withstand attacks

One of the most important yet overlooked aspects of this situation is that threat vectors are always changing and attacks will happen, yet there has been very little discussion about resiliency. SMMs need help in understanding how to design resilient OT systems, detect when an attack does occur and then respond and recover.

#4 Aggregate disparate manufacturing cybersecurity activities

There are currently at least four organizations just within the Office of the Secretary of Defense addressing cybersecurity for industrial control systems. The NDIA "Cybersecurity for Advanced Manufacturing" paper recommends that the DoD "Establish, and adequately fund, a new program for Manufacturing Cybersecurity Capabilities in the Industrial Base, with a DASD-level Champion and participation from the DHS." A concerted government message and effort are needed to achieve the desired results.

#5 Fuel the rapid development of OT cybersecurity solutions

The DoD should explore innovative means, such as grand challenges, to quickly raise awareness and spur development of OT cybersecurity solutions. Such solutions should be designed to not only prevent attacks, but detect them as well.

#6 Develop a means to measure and certify cybersecurity compliance

Manufacturers in the DIB must have confidence that their investments in cybersecurity meet DoD requirements. Large manufacturers also need a means to quickly and cost-effectively assess the cybersecurity readiness of each manufacturer in the supply chain. This requires the establishment of meaningful metrics that can be readily certified, whether by a customer, government agency or an independent third party.

SUMMARY

In summary, the DIB risks are greater than many realize, and much work is needed to mitigate those risks, particularly for industrial control systems. The SMMs do not have the resources to tackle these issues on their own – they need help if we are to rely on their capabilities. Consider the following scenario.

> An adversary wants to disable production of weapon system parts or components. DoD procurement data are publicly available and provide a blueprint of the SMMs to target. By gaining access through the industrial control systems at manufacturers producing those parts, an adversary could plant undetected malware that can disable the manufacturing equipment at a predetermined time or when signaled. The adversary can then disable tens, hundreds or even thousands of manufacturers on command. Or, perhaps they just target two critical suppliers of missile components. Such an event could have a profound impact on the ability to produce and support any or all weapon systems. This is not just a scenario for the future – it may have already happened.