TechSolve®

STATEMENT FOR THE RECORD OF
DAVID LINGER, PRESIDENT/CEO - TECHSOLVE, INC.

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
HOUSE SMALL BUSINESS COMMITTEE

REGARDING A HEARING ENTITLED
"ZTE: A THREAT TO AMERICA'S SMALL BUSINESSES"

WEDNESDAY, JUNE 27, 2018

INTRODUCTION

Chairman Chabot, Ranking Member Velázquez, and Members of the Committee, thank you for inviting me to testify on behalf of U.S. small manufacturers regarding the impact of cyber-attacks on this critical national asset. Only the government tops the manufacturing sector (followed by finance and healthcare) as the most targeted sector by cyber espionage. These aggressors are seeking to disrupt manufacturing not only through the espionage of intellectual property; but also the destruction of the U.S. supply chain by crippling them both financially and through attacks on their intelligent machines.

These foreign criminals are exploiting the information that manufacturers believe they've safely locked away. These hackers have proven how private data, on any computer or manufacturing device that is connected to the Internet, is vulnerable and susceptible to malicious attacks, tampering, theft, and misuse. Unfortunately, it is not an exaggeration that there are only two types of companies – those who have been hacked and those who don't know that they have been hacked. "Most manufacturing systems today were made to be productive – they were not made to be secure. Every manufacturer is at risk – it isn't a matter of if they will be targeted, it's a matter of when." said Rebecca Taylor, senior vice president for the National Center for Manufacturing Sciences (NCMS).

TechSolve has found that a majority of manufacturers can be described as "not very well prepared" or "not prepared at all" to handle cyber-attacks. A 2017 Ohio Manufacturing Extension Partnership (OH MEP) survey of Ohio manufacturers revealed that only 12.51% manufacturers responded that they understand what cybersecurity is and have worked to protect their machines, intellectual property, and IT systems and only 4.48% have undergone a cybersecurity assessment.

THE IMPORTANCE OF SMALL MANUFACTURERS

According to 2015 Census data, the vast majority of manufacturers are very small. Of the 251,744 firms in the U.S. manufacturing sector, only 1.5% of those manufacturers have greater than 500 employees. And out of the remaining 98.5% of manufacturers with less than 500 employees, 75% of those manufacturers have less than 20 employees. The importance of these 188,000+ very small manufacturers to the United States' economy is staggering. These small firms are the backbone of manufacturing – the ninth largest economy in the world with over $2.1 trillion in value-added.

In addition to their contributions to the economy, creating jobs, and building products critical to our daily life and defense of this nation, small manufacturers are especially important because they drive innovation. Brian Raymond, Director of Innovation Policy for the National Association of Manufacturers (NAM) impeccably summarized manufacturers' recent digital transformations, and subsequent rising exposure to cyber-attacks in the Fourth Industrial Revolution: "Manufacturers are the creators, users, servicers, and installers of the Internet of Things (IOT). Billions of connected devices are pervasive throughout manufactured products and on the shop floors where they are made. This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies. The IOT will increase the attack surface for manufacturers. The more that shop floors become imbued with intelligent machines, the more those machines will contain data worth stealing."

THE CYBERSECURITY CHALLENGES THAT SMALL MANUFACTURERS FACE

Attacks against larger businesses and nations hit the headlines with such regularity that many have become numb to the sheer volume and hastening of cyber threats. These threats are not hypothetical evils. For those of us that work with small manufacturers who have teetered on the brink of closing their doors due to cyber-attacks; their cyber-crimes are personal, real, and distressing. As president of TechSolve, I have a very unique perspective of the devastation these cyber-attacks have caused our customers. I am here today to share the story of one such manufacturing company that has experienced these attacks and exemplifies the risks a majority of these manufacturers face on a 24/7 basis.

To Tony Strobl, President of Cincinnati Crane & Hoist, these cyber-attacks are war on his company and his employees. Cincinnati Crane is a very small, 20-person company, based in Southwest Ohio, that supplies turn-key crane systems, parts, and services, through hard work, innovation, and quality craftsmanship, at competitive prices to a global market. Cincinnati Crane is a veteran-owned business that has seen domestic growth of more than 400% in the last three years and was awarded the U.S. Department of Commerce Export Achievement Award in 2017. Earlier this year, Tony's company was the victim of social engineering, or more specifically a spear phishing campaign that contained malicious macros that breached their email system; went undetected for an uncertain amount of time; embedded hidden folders within Office365®; "spoofed" legitimate invoices that were being emailed to Cincinnati Cranes' customers; replaced those invoices with bogus invoices providing illegitimate banking information that ultimately syphoned over $200,000 from his customers. When the Cincinnati Crane invoices had aged 30 days and collection calls were made, customer after customer told Cincinnati Crane that they had already paid their invoices.

The $200,000 that was stolen from Cincinnati Crane is unrecoverable according to the FBI. Due to Cincinnati Crane's current financial standing, Tony had to make the devastating decision to lay off four of his employees - 20% of his company. Not only has this cyber war devastated the lives of those four families; but it has also severely hampered Tony’s capability to complete customer orders, grow, and innovate. This cyber-attack has also resulted in a devastating fluctuation in customer trust. Cincinnati Crane’s customers are afraid to conduct business with Tony. Not only are they concerned about sensitive drawings and corporate data that they have shared with Tony’s project managers; but they are also afraid to open email correspondence from Cincinnati Crane or make payments to him electronically. Even though TechSolve, and its IT sub-contractors, have scrubbed their systems and are working on long-term cybersecurity policies and procedures through remediation and adaptation of the NIST SP 800-171 cybersecurity controls, the effects of these cyber-attacks continue to devastate his company and threaten its long-term viability.

Customers, like Cincinnati Crane’s, share their sensitive information with manufacturers, assuming these companies have the proper security measures in place to protect their data. As soon as a data breach occurs, customers will question the amount of trust they've put into that business. Furthermore, these customers want to believe that the manufacturer can not only prevent; but also properly manage a potential data breach. While the cyber-hack itself might affect customer loyalty, manufacturers that don't handle the attack with competence will likely see a more negative impact on customer confidence. Obviously, the majority of customers won’t do business with a manufacturer they can't depend on and when it comes to a large prime or the Department of Defense (DoD), these manufacturers probably should expect to lose their government contract. Government primes already have a difficult time finding and maintaining quality suppliers.

Besides typical IT cyber-attacks, both foreign and domestic espionage will continue to target manufacturers and devastate these companies, and their customers and supply chain primes, because there is fierce competition for intellectual property; industrial control systems (ICS) that are largely left unguarded; and their systems are increasingly connected through the use of IOT devices, robotics, and human-machine interfaces to improve automation and decrease costs.

In 2018, reports released by highly-respected American corporations Symantec Corporation, NTT Security, and Cisco Systems validated data that TechSolve has encountered when working with small manufacturers. The four biggest obstacles to adopting advanced security processes and technologies in small U.S. manufacturers are: 1) Budget constraints; 2) Competing priorities – focus on productivity and efficiency; 3) Lack of knowledge regarding the invasiveness and impact of cyber-attacks; and 4) Defense contractors choosing the calculated risk of not implementing and/or slow cybersecurity remediation since (to date) there is a lack of enforcement of the current DFARS SUBPART 204.73--SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (Revised December 28, 2017).

The Cisco 2018 Security Capabilities Benchmark Study further corroborates data TechSolve has observed when it comes to manufacturers in general; but especially small manufacturers. There will be more operational technology (OT) and IOT attacks in the future. Attacks targeting OT are still classified as “uncommon” enough that many cybersecurity professionals haven’t experienced them firsthand. But in Cisco’s study, security professionals absolutely agree that manufacturers should expect such attacks to occur in the future. Since TechSolve has 35+ years’ experience in serving the needs of manufacturers in the areas of machining, data extraction, and manufacturing process improvement, we are used to working with small manufacturers every day to translate emerging technologies into everyday manufacturing and business solutions. TechSolve is currently working on solutions for manufacturers that will help them “connect and protect” their systems that, a majority of the time, have unpatched and out-of-date software making them even more vulnerable to cyber-attacks. Many manufacturers have older OT devices and equipment that use controllers based on Microsoft Windows XP®, and even MS DOS, that are connected to the Internet; therefore their risk of cyber-attacks is exacerbated. Some other manufacturers have fabrication presses, machine tools, and material handling equipment that are 25, 30, or even 40+ years old. Manufacturers don’t get rid of these items just because they aren’t the “latest and greatest”; but are working to connect the analog control of this equipment to the digital thread via the Internet. The Industrial Internet of Things (IIOT) will be pervasive and therefore, the need to protect is vital.

Similar cyber-attack opportunities also exist for “disruption of operation” attacks and hardware attacks. Cyber-attackers can hack into machine tool accessories or machine tools and adjust/alter the program; therefore either stopping the manufacturer from providing the right parts for their suppliers, or even worse; altering the quality of the part that is a portion of a larger assembly, thus compromising the entire system. For large defense primes and original equipment manufacturers (OEMs), it is critical for their supply chains to protect what happens to their parts before they enter back into their network.

HOW CYBERSECURITY REGULATIONS & PROGRAMS AFFECT SMALL MANUFACTURERS

Today, companies like Cincinnati Crane & Hoist have DFARS regulations to which they must comply in order to keep their government contracts. However, the spirit of these regulations may have the safety of our nation at heart; but the government’s lack of enforcement make Cincinnati Crane’s systems and critical information no safer by merely becoming “compliant” with DFARS.

Safeguarding data is too important to the United States to allow “loose compliance” to be the platinum standard. There are a number of ways to entice companies to begin implementing cybersecurity best practices and the DoD has done a great job by leading the way and establishing one method – regulation through the current DFARS and NIST SP 800-171 controls. The current shortcoming of this exercise is the lack of enforcement. TechSolve is working with several manufacturing companies that are conducting business with the DoD. They are technically "in compliance" with the DFARS by completing all four of these items: 1) conducting a cybersecurity assessment; 2) creating a security plan based on the assessment; 3) creating a plan of action with milestones (POAMs) based on the work that needs to be done in the security plan; and 4) creating an incident response plan (IRP) that will report designated security breaches within 72 hours of the incident; however they are not automatically cybersecure. These documents, without remediation of the weaknesses in their systems, are merely "pinky swears" to make their networks safer at some future date. A plan of action is great; however, there are no existing checks and balance system that is currently being implemented by the DoD to manage these POAMs.

Another approach is being discussed in the state of Ohio. Attorney General Mike DeWine is working with the Senate and House on former Senate Bill 220. This "safe harbor" legislation, if passed, will create a law that will protect companies that can prove that they have proactively implemented and are maintaining cybersecurity measures within their systems. If these Ohio companies can document that they have taken steps to safeguard the information on their networks, they will have a limited amount of protection from civil litigation.

Although both of these examples have different goals; the methods in both cases are implementation of cybersecurity best practices. While cybersecurity is not a solution to being hacked, it does make it much more difficult for these cyber-criminals to devastate our nation's small manufacturers. Research conducted by the National Cyber Security Alliance states that there was a 600% increase in IOT attacks from 2016 to 2017 and that the #1 country of origin is China at 21% while the next highest country of origin is 10.6%. Given these statistics and the fact that 60% of small and mid-sized businesses that have been hacked have to shut down within 6 months of a cyber-attack, it will be important for the U.S. government to be aware that it must have more concrete plans in place to safeguard this incredibly important industry sector.