Are Your Supply Chain Partners Ready for the IIoT?

Or causing cyber security risks?!

Thou Shalt Not Steal - Exodus

But the bad guys always do.

Malicious actors exist and cybercrime is rising exponentially. US infrastructure and core manufacturing are of particular interest with heightened risk. Thieves and hackers take the path of least resistance, not through the well-guarded front door. Are your core suppliers secure enough to protect shared information and prevent a weak-link backdoor to manufacturing?

POSSIBLE WEAK BACKDOOR TO THE PRIZE

80% of targeted attacks are directed at SME (small and medium enterprises).

These same companies lack the knowledge, resources and dollar commitment to put in place security systems to prevent infusion and attack, making them exceptionally vulnerable to attack. Many SME firms are Tier 1 or Tier 2 suppliers to serve the needs of infrastructure and core manufacturing. Are these SME suppliers' security measures, or lack thereof, adequate to protect critical shared information and plans?

THE TACTICS

Malware threats hit the 400 million mark in 1Q 2015 vs 200 million (1Q 2014), and 100 million (1 Q 2013) and are the #1 most common threat. Malware, or malicious code, is a catch-all term encompassing a variety of attack vectors from bot nets to viruses. Malware is software used to create or disrupt computer operation, gather sensitive information, or gain access to private computer systems. Examples of malware include: adware, spyware, Trojan, viruses and worms.

In 2014, the rate of growth of new mobile malware passed that of new malware targeting PCs (Source: McAfee). As both manufacturers as well as their SME

suppliers have BYOD (bring your own device), policies this threat poses a double risk.

THE TACTICS (CONTINUED)

Isn't it possible for malware to be planted into a SME supplier who advertises doing business with these targeted industries - on their web site, in advertising, word of mouth? Yes. Malware can be used without detection to allow the hacker to listen and collect information. Large manufacturers frequently share information with their supply chain - engineering data, pricing, strategic data involving new products and direction to name a few.

Bot nets are software programs that can automatically perform malicious actions. Bots can inflict substantial damage including stealing sensitive information to opening back doors to further attacks, the main threat in 2014. Over 83% of organization's had at least one bot infection in 2014 (Source: McAfee), representing an increase of over 95% since 2012 (Source: Checkpoint).

Bad guys also use toolkits, root kits, and exploit kits comprised of software designed to remotely access or control a computer without detection. Exploit kits and root kits often target software vulnerabilities associated with common software plugins such as Oracle Java, Adobe Reader, Flash, and Microsoft Silverlight.

All of these tactics can be used by malicious actors to gain access to the SME.

THE IMPACT (THINGS THAT MAKE YOU GO HMMMM)

This information in the wrong hands can cost manufacturers millions in damages - causing reputation damage and still worse, possible theft of trade secrets and intellectual property. The stakes are high.

A PATH FORWARD - SO WHAT TO DO?

Does your company's procurement team demand that your Tier 1 and Tier 2 suppliers have adequate security measures in place to safeguard your corporate interests? If not, why not?

Is security top of mind as a procurement metric, as important as product "commodity" pricing trends? If not, are the tracking metrics for successful selection and management of supply chain partners adequate, in keeping with possible cost?

Have your Tier 1 and Tier 2 suppliers conducted a comprehensive security assessment with an implemented security program that is adequate to protect their and your corporate interests? If not, why not? More importantly, are your Tier 1 suppliers forward thinking, learning organizations who have already put in place security programs before you place the requirement onto them? It's a difference between being proactive versus reactive, strategic versus tactical, with much at stake.

Does your procurement organization prioritize security as a core metric to meet the ongoing threats, risks and impact to your organization? If not, why not?