TRUSTING YOUR SUPPLY CHAIN

For manufacturers, securing an operations technology (OT) network is an issue that is largely under the direct control of the enterprise. In contrast, securing an information technology (IT) network with a supply chain that extends from a line of suppliers that might be two, three or four-tiers deep and may even extend to a customer or customers is a very different problem.

In the case of a supply chain, only the largest companies have the clout to force their suppliers to modify their behavior to suit the requirements of the enterprise. For smaller companies, securing the supply chain is very difficult because most of the supply chain is in the hands of other companies. A large company has the economic power to force vendors to comply "or else."

However, rather than doing nothing, there are actions that can be taken by smaller companies. Smaller players can focus on business intelligence and business continuity planning in an effort to see trouble coming as soon as possible to give the enterprise as much time as possible to find a way to cope. They can also build awareness of the supplier market and build relationships with alternate suppliers.

Supply Chain Security/Trust Issues

The "National Strategy for Global Supply Chain Security," states that to manage supply chain risks, the Federal government needs to "understand and address vulnerabilities to the supply chain that stem from both exploitation of the system by those seeking to introduce harmful products or materials and disruptions from intentional attacks, accidents, or natural disasters." Proper understanding and addressing of vulnerabilities can lead to improved trust.

Trust in the supply chain is based on several factors. One is market intelligence. This is awareness of what is happening in your market, and your supplier's market. It's also necessary to be aware of economic, socio-political and environmental issues that affect you, your suppliers and your customers. Sounds like a lot, and it is, but this is the job of market analysts and small players can use them to help fill this intelligence role.   Your vendors can be affected by natural disasters, social upheaval and recession or other economic turmoil.

In terms of protecting the enterprise supply chain, consider where your supplier's factories are located. Is there one factory, or several that are all located close to one another? These are risks. Geographic location of production can be a point of consideration in selecting a vendor, or an alternate vendor. For example, vendors for required products in China could be in both Shenzhen and Beijing 1500 miles away. Having vendor alternatives in each of those cities is much less risky than having vendor alternatives in Shenzhen and Hong Kong that are only10 miles apart.

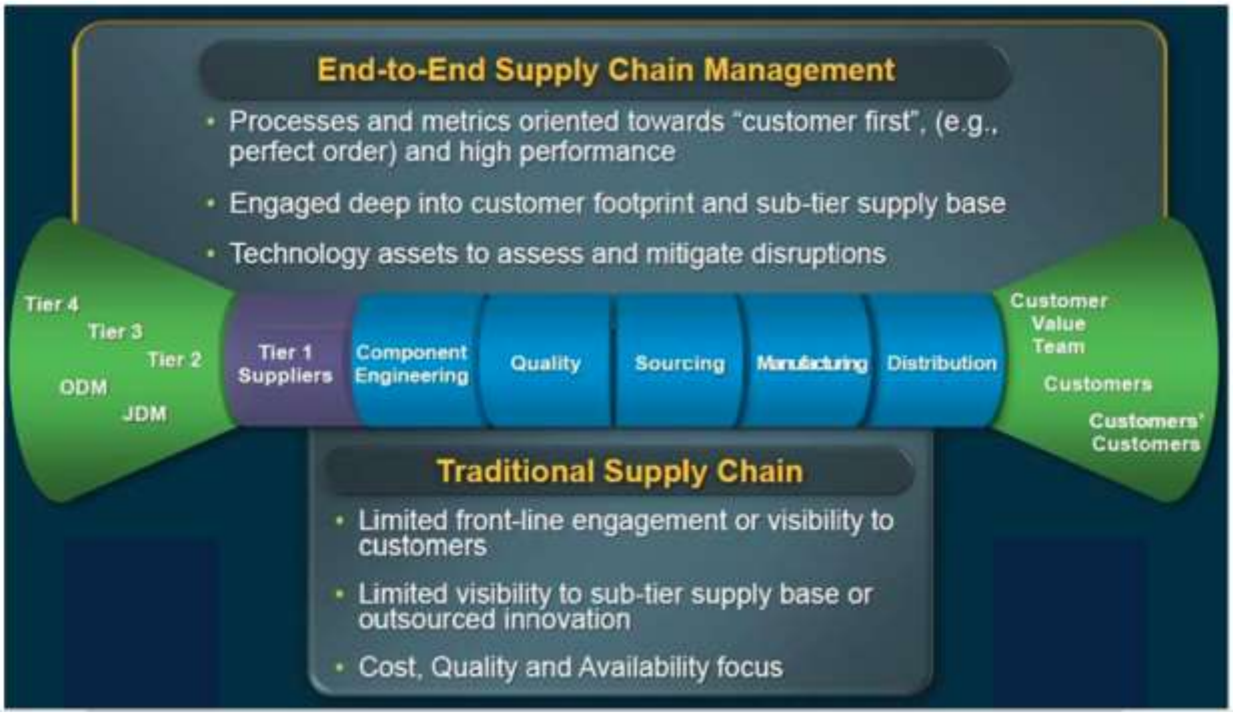
Another kind of threat to the supply chain is poor quality of supplier product. This is usually handled by QA testing that is rigorous early in the relationship and only somewhat eases with time and trust in the relationship, but as a former president once said, "trust but verify." This is basically the same thing that must be done if security is important, but the testing will be different. The test plan must be constructed based on the threats and risk the buyer worries about.   It can include source code review, a requirement for the supplier to sign their code, reverse engineering of code and hardware purchased from the supplier, and hiring hackers to attack the hardware, firmware or software. On a smaller scale, the buyer might speak to market analysts that focus on security for those vendors. Or they might go to local universities and offer to hire cybersecurity graduate students to hack samples from suppliers.

Addressing the Issues

The Trusted Computing Group's Trusted Platform Module (TPM) and Trusted Network Connect (TNC) standards can play important roles in supply chain security. These tools can be applied by both small and large companies.

There are many incidents of large companies being brought down by hackers who hacked a small supplier (with weak defenses) rather than the hard shell of the big company. The objective is to steal userid/passwords that were given by the large company to the small company for access to large company's network. For a small company acting as a supplier, it might be a terminal disaster for them if their large vendor is taken down because of lack security in the supplier shop. This is a real reason for the small suppliers to pay attention to the trustworthiness and security of their own environment. This is a matter of multi-factor identity (like a password and a TPM integrity report or TPM-protected certificate. The ability to track the integrity of the platforms involved is also important. So is the ability to know what machines are connecting and that they are clean.

For a small company buying from suppliers, the guidance is a bit different. Network access by employees of one side into the network of the other side is dangerous for both companies. For the small company buying from vendors, the vendors must be kept away from the small company machines. This might be done by the small company using a cloud service for vendors, one that does not connect back to the company servers. This is a matter of implementing TNC or other ways of carefully fencing off vendor access to the buyer's production network.



End-to-End Supply Chain Management

- Processes and metrics oriented towards "customer first", (e.g., perfect order) and high performance
- Engaged deep into customer footprint and sub-tier supply base
- Technology assets to assess and mitigate disruptions

Traditional Supply Chain

- Limited front-line engagement or visibility to customers
- Limited visibility to sub-tier supply base or outsourced innovation
- Cost, Quality and Availability focus

Figure 1. End-to-End Supply Chain management has several aspects that TCG standards can address.[1]

[1] http://www.zlc.edu.es/content/files/Cisco%20SC%20Risk%20Man_FT.pdf

While factories should be concerned and taking action to prevent weaknesses in the supply chain that cause disruption, monetary loss and wreak havoc, any organization with suppliers and partners who have remote access to the enterprise's IT network should actively be implementing a trust plan. In 2013, attackers gained access to a large national discount retailer's network not by defeating its network security, but through a small heating and air conditioning firm in Pennsylvania that worked with the company and had suffered its own breach[2]. This large retailer is by no means alone. Hospitals are being increasing targeted for their data with a sudden increase in healthcare-related data breaches. Who is next? Don't let it be your organization due to lack of recognition and proactive response to one of today's most serious business issues.

[2] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/