Supply chain risks associated with vendors, partners, hardware & software systems that facility managers should be aware of

The Center for Development of Security Excellence (CDSE) defines supply chain as 'a system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.' As the definition states, supply chains involve different organizations small or large, typically interconnected and transferring data and products.

In this article, we will focus on two aspects of the supply chain: (1) managing suppliers, vendors and partners, and (2) understanding and managing the sourcing of complex hardware and software systems. Specifically, we will discuss the risks associated with managing vendors, purchasing hardware and software systems used in facility operations and maintenance and possible ways to mitigate these risks.

The Threat to Supply Chain – Vendors & Partners

As organizations are increasingly more interconnected, the vast array of business benefits also come with security risks. These digital connections between buyers and sellers combined with robotic process automation create vulnerabilities to cybersecurity and data breaches if not managed properly.

Today every organization, small or large, has a digital ecosystem and interacts with other organizations through electronic communication systems; vast amount of data is transferred between organizations. These digital ecosystems from individual applications to entire data centers have moved to cloud providers providing ease of access and common platforms. This digital collaboration between facility managers and suppliers brings efficiency improvements, shortens response times and provide fast and accurate data processing. However, all the benefits of electronic collaboration come with some cybersecurity risks.

A supply chain attack happens when someone infiltrates the organization through a third-party partner or service provider. As an example, the 2014 Target data breach took place because one of the company's vendors was compromised. An employee of one of Target's refrigeration contractors opened a phishing email which allowed Citadel, a variant of the Zeus banking trojan, to be installed on the vendor's endpoints. The company did not have an anti-malware solution in place at that time that offered real-time protection to prevent and stop this kind of threat and as a result, they became a victim. Target never specifically mentioned which system was used, but security experts thought Ariba to be the main candidate ([i] "*Anatomy of the Target data breach: Missed opportunities and lessons learned*", ZDNet, February 2015)

We should not forget about third-party partners who conduct surveys, perform research, or store our documents in electronic formats. In many cases facility managers use third party systems to get feedback from the end user after performing maintenance work. The Verizon breach, which involved six million customer records, was caused by a provider of customer service analytics who placed six months of customer service call logs, which included account and personal information, on a public storage server ([ii] "Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts", UpGuard, July 2017)

These examples are reminders that even when an organization has the most sophisticated security tools in place, one can never be certain the suppliers and vendors also have the same methods implemented. To avoid this, both parties must have robust security processes that block and avoid any potential attacks from the outside. Unfortunately, supply chain attacks are getting more widespread and growing in frequency and sophistication.

The Threat to Supply Chain – Hardware & Software Systems

Automation systems and electronic hardware come web-enabled with the capability to send diagnostic data to the manufacturer and to perform remote maintenance or adjustments. Over the last few years, the cost of IoT devices has significantly decreased along with an increase in their capabilities and data gathering. Many facility managers and their maintenance teams have been installing sensors and other IoT devices to either improve the workplace experience of employees or to become proactive in their maintenance activities. These systems and devices, if not configured properly, can become a backdoor into the organization's network. The risk associated with these systems and IoT devices can be easily mitigated by following good IT protocols and security policies. But what if the automation system has compromised components or software, or a security flaw built into it?

Traditional IT security practices don't address issues when components are inserted to send data outside of the network, or to create a back door for potential intruders. Detecting these security flaws is difficult because they are usually masked by the proper operation of the system. For example, this can happen when buying remanufactured electronic drive systems or control boards from unknown sources and installing these in automation systems connected to the organization’s internal network.

Therefore, understanding the entire supply chain is an important part of a cybersecurity program. The risk is not only in installing new systems, but also in replacing and maintaining components —these should be subject to the same requirements and analysis. From August 2014 through early 2015, Lenovo sold laptops bundled with the Superfish software, which was presented as an add-on used to insert ads into Google search results. Superfish intercepted all secure communication (https) traffic using a self-signed root certificate that was stored in the local certificate store, which proved to be a serious security concern ([iii] *“How Lenovo's Superfish 'Malware' Works and What You Can Do to Kill It”*, Forbes, February 2015.)

The way a product or service is purchased is as important as the type and selection of the product or service provider. When procurement focuses on providing the lowest cost solution that meets technical requirements, the risk can be higher than working with a trusted provider.

How to Mitigate the Risks

Some actions that can be taken to eliminate the risks related to supply chain include:

- Training employees and vendors in security best practices
- Developing a risk evaluation methodology and understanding the risks associated with every supply chain process
- Reviewing internal and external security procedures
- Pre-qualifying suppliers that meet the risk management criteria
- Requiring suppliers to follow operating standards for cybersecurity in the supply chain
- Mapping the supply chain and identifying cybersecurity risk exposures

The IBM Cyber Security Intelligence Index report stated that 95 percent of all security incidents involve human error, from following links to phishing scams to visiting bad websites and enabling viruses. **Training and education in protecting our networks from these types of attacks is the best defense.**

Vlad Bacalu is SVP Strategic and Technical Solutions for Amentum. He has over 30 years extensive hands-on experience in creating and implementing strategic and technical solutions to drive bottom line performance across diverse manufacturing and process industries. He led numerous maintenance and reliability programs in a variety of technically diverse environments. He is the Past-Chair of the Society for Maintenance and Reliability Professionals (SMRP), and currently serves as the Chair of the Global Forum on Maintenance and Asset Management (GFMAM).