SPOTLIGHT / FEATURE

Securing the Keys to the Kingdom

Hardening the IoT-connected supply chain

In the IT community, it is often said that the best defense against a cyber-attack is to "think like a hacker." This tactic may work when an attack is directed at network infrastructure, and the goal is to protect technical information from exfiltration or exploitation. But, when the threat reaches into the realm of industrial technology, cybersecurity is a very different kind of problem. The union of the digital world with a variety of automation, control and safety systems in the "Factory of the Future" has dramatically expanded the cyberattack surface. This has shifted the economics of cybercrime "by facilitating hacking at scale," according to Lior Div, CEO and co-founder of Cybereason (https://www.cybereason.com), in a recent CSOonline (https://www.csoonline.com/article/3244261/hacking/more-cybersecurity-drama-but-some-hope-for-defenders-in-2018.html) article. "Attackers can target one organization and, in the process, gain a foothold to compromise hundreds or thousands more." Supply chains have, in essence, become the gift that keeps on giving for cybercriminals, he explained.

To harden the IoT-connected supply chain, cybersecurity strategies need to move beyond a single enterprise's digital infrastructure and encompass all the players within the value chain. In other words, it's time to stop thinking like hackers and start bringing the risk-based, end-to-end perspective of supply chain professionals to the resistance.

"To address cybersecurity comprehensively across an entire value chain, we must look at the 'who, what, where and how' of our connected ecosystem," said Edna Conway, chief security officer for Cisco's global value chain. Conway is responsible for driving cyber and operational

security throughout Cisco's vast global ecosystem of partners and suppliers. "People who have not run a supply chain do not necessarily think about the full end-to-end spectrum of the ICT value chain, from design to end of life, the way supply chain practitioners do."

"Applying risk-based physical, digital and cyber-physical security throughout the third-party ecosystem is paramount. No one node can independently protect itself."

-Robert Metzger

For example, Conway offered that printed circuit board testing is a fundamental step in validating the quality of an ICT system. "The fidelity and security of such testing and the integrity of the test data can be impacted by a variety of factors," she noted. She suggested that to be comprehensive we should ask: "Has the test software been designed and developed pursuant to a secure development lifecycle? Is the testing conducted in a secure facility, with trusted personnel on secure systems? Is the test data being shared via a secure method?"

The difficulty of maintaining visibility into the many tiers of the extended supply chain is certainly not new. But, the rapid proliferation of IoT-connected systems now pushes an enterprise's digital boundaries well beyond direct and second or third tier indirect suppliers, noted Robert Metzger, shareholder at Rogers Joseph O'Donnell law firm in Washington, D.C., and an active voice in the cybersecurity arena. An organization may, therefore, be completely unaware that their systems have become connected to, and dependent on, the digital integrity of some unknown entity.

As a result, today's enterprises are at distinct disadvantage in the battle against cybercrime. While a business must endeavor to protect systems with undetermined reach, attackers need only exploit a single vulnerability to garner the keys to the proverbial kingdom. "This is why applying risk-based physical, digital and cyber-physical security throughout the third-party ecosystem is paramount. No one node can independently protect itself," said Metzger, who has worked closely with government agencies including the DoD and recently participated in the Defense Science Board Cyber Supply Chain Study (https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf). "Every company has a duty to act responsibly to protect the public against physical or economic harm resulting from poor cyber hygiene." Unfortunately not all do.

"The market is not populated only with the smartest and best companies who create and follow best practices," he said. "There are all kinds of enterprises, all over the world, who seek to exploit emerging technologies or new areas of consumer demand to try to get to market first, with little concern for security."

"Too many enterprises are not paying attention to these basics. This makes it cheap and easy for bad guys to do bad things."

-Emile Monette

Emile Monette, cybersecurity strategist, Department of Homeland Security (DHS) Office of Cybersecurity and Communications echoed Metzger's observation. "Too many enterprises are not paying attention to these basics. This makes it cheap and easy for bad guys to do bad things."

Monette shared a few common sense cyber hygiene practices both federal and commercial organizations should adhere to:

- Don't buy software with known vulnerabilities
- Don't buy hardware for sensitive applications from non-authorized resellers
- Ask suppliers for reasonable assurances about the security measures built into their practices
- Consider the security implications of trading visibility in the supply chain for fast, low-cost production

Cisco's Conway, one of the most well-known and respected professionals in cybersecurity today, added that a common misconception is that robust cyber defense can be achieved with technology alone. "Security is an inherently human challenge," she said. "Installing antivirus software and conducting penetration testing are but a few of the basic practices in cyber defense." She believes a holistic, risk-based security approach must be embedded through existing people, processes and tools of both internal and external stakeholders.

"The goal isn't to implement the most technologically sophisticated solution, but to assure the right security is deployed in the right place, at the right time."

-Edna Conway

"The goal isn't to implement the most technologically sophisticated solution, but to assure the right security is deployed in the right place, at the right time. We don't approach partners with a prescriptive method to implement security," she explained. "Instead, we ask them how they run their business and collaboratively determine how our architecture can be implemented within the people, process and technologies that they already use. So, a successful process is rigorous, but it is also flexible."

Conway related a theoretical scenario where the security concern is a focus on role-based access control. Two partners ensure that access to certain factory areas or confidential information is limited only to those who are pre-approved. One may leverage biometics and RFID. The other, a smaller operation, have a physically segregated room, secured with electronic locks and monitored by a security guards checking people entering against photos of those authorized to enter. "These are two very different approaches to security," she said. "But in the context of the business each of those partners is doing for us, both are equally managing concerns about the risks of counterfeit, taint, manipulation or disruption."

NIST Cyber Supply Chain Best Practices

1. Before they are fully integrated into the supply chain, new suppliers are required to undergo an assessment period to test the capabilities of the supplier and its compliance with various requirements.
2. Standard cybersecurity terms and conditions are included in all requests for proposals

Another key to effective cyber risk management is understanding the things you can control, and those you cannot, said Metzger. One aspect of supply chain cybersecurity Metzger believes industry can, and must, do a better job of controlling is incident reporting.

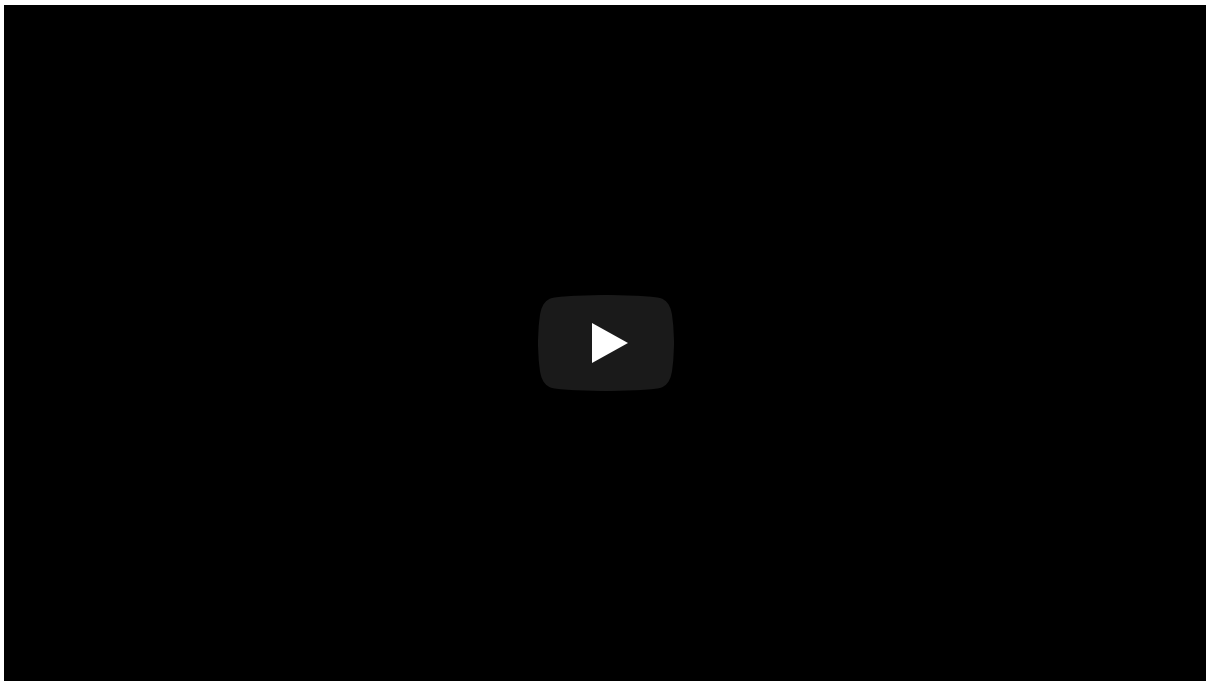
"When a cyber-attack is mounted through the supply chain, we know for a certainty that this attack can proliferate and impact many other organizations," he said. "We live in a situation where there are many more attack surfaces than ever before, and the consequences of an attack can be more severe than a bruised brand image or financial loss. In this environment,

effective security must go beyond the things we do to safeguard our systems. We need to share what we have learned about an attack or vulnerability with everyone who has or could buy the same part, or operate the same software or rely on the same system."

Though there is a general consensus that incident sharing is crucial to combatting cyber breaches – research from AlienVault (https://www.alienvault.com/who-we-are/press-releases/new-alienvault-research-finds-76-of-security-professionals-believe-sharing-threat-intelligence-is-a-moral-responsibility) found that 76 percent of respondents believe they have a moral responsibility to share threat intelligence – a recent report (https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/) from The Council of Economic Advisers entitled "The Cost of Malicious Cyber Activity to the U.S. Economy" indicates that the number of companies that publicly report malicious cyber breaches may be as low as three percent of all those who are actually affected. The stigma attached to a cyber-attack and fear of potential liabilities are among the most commonly cited reasons for either failing to report, or underreporting an event.

If this sounds familiar, it should. These are the same concerns many tech companies often cite for their reluctance to report the discovery of counterfeit components in their pipeline. As a result, billions of dollars of counterfeit components continue to flow through the global high tech supply chain. The financial loss, brand damage and health and safety repercussions of this ongoing menace are incalculable.

So, as the industry faces another, even greater security threat, will history repeat itself? Maybe not. Consider Schneider Electric's handling of the 2017 malware attack (https://www.automationworld.com/cyber-attack-hits-safety-system-critical-infrastructure) that targeted its Triconex safety-instrumented systems (SIS) at an undisclosed facility in the Middle East. The malware, dubbed Triton, is one of only a handful of known variants designed to breach industrial control systems (ICS), and the first to specifically target systems responsible for protecting human life, according to Robert Lee (https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/), founder of cybersecurity startup Dragos Inc.



Schneider Electric's aggressive response and candor about the attack is said to have set the bar for incident response in the ICS sector. "They didn't do the marketing dance," according to cybersecurity evangelist Dale Peterson (https://youtu.be/f09E75bWvkk). Rather, the company analyzed the systems, found out what the problems were and have since shared their findings with the community through a variety of outlets, including industry events like the S4 Security Conference in Miami, where Schneider Electric executives offered a "deep analysis" of the incident. "This is what we need to help solve these problems and move things forward," Peterson stated.

Defense in Depth
Defense in depth is defined in the Schneider Electric white paper, "Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications," as the coordinated use of security countermeasures to protect the integrity of information assets in a network. The following are the six steps required to implement a defense in depth strategy, according to Schneider Electric.

As concerns about the possibility of attacks on industrial systems in the era of the IIoT escalate, the global industrial process and manufacturing industry must heed the Triton attack as a warning, noted Schneider Electric's Jay Abdallah in a recent blog post (https://blog.schneider-electric.com/cyber-security/2018/03/23/strengthen-cybersecurity-

through-a-united-industry/). "This problem isn't limited to a single company, industry or region. It's an international threat to public safety that can only be addressed and resolved through collaboration-collaboration that goes beyond borders and competitive interests," he wrote. "The message has never been more clear: when it comes to cybersecurity, the industry needs to come together."

A sign of progress on this front is the recently formed "Charter of Trust (https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-online-2018-02-13-sbi-en.pdf)" alliance. The nine founding Chart of Trust companies -Airbus, Allianz, Daimler Group, Deutsche Telekom, IBM, MSC, NXP, Siemens Ag and SGS-have outlined the key principles considered essential to protecting "democratic and economic values against cyber and hybrid threats." In signing the charter, member organizations commit to making "every effort to protect the data and assets of individuals and businesses; prevent damage from people, businesses, and infrastructures; and build a reliable basis for trust in a connected and digital world."

To promote this collaboration and establish a more unified cyber risk defense, the National Institute for Standards and Technology (NIST) has released version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity. In a statement announcing the release of the updated Framework Secretary of Commerce Wilbur Ross noted, "The voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must do for all CEO's."

DHS's Monette agrees. "We have a shared problem, and we need a shared solution," Monette concluded. "The Framework is a quick and easy baseline for businesses without a robust cybersecurity process to address cyber risk in a way that is understandable."

Supply chain professionals interested in learning more about the NIST Framework can download the NIST Fact Sheet (https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework) or view a free public Webcast (https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview), hosted by NIST on April 27, 2018, at 1 p.m. Eastern time.

Related Resources:

- Community (https://www.alienvault.com/open-threat-exchange): The AlienVault® Open Threat Exchange®
- Article (https://www.kaspersky.com/about/press-releases/2017_kaspersky-labs-threat-predictions-for-2018): Supply chain nightmare: Threat actors backdoor third-party software for enterprise targeting
- Community (http://veriscommunity.net): Vocabulary for Event Recording and Incident Sharing (VERIS)
- Article (https://ics-cert.kaspersky.com/reports/2017/11/30/industrial-enterprise-and-iot-security-threats-forecast-for-2018/): Criminals Will Take Advantage of Threat Analyses Published by Security Researchers
- Organization (https://www.nationalisacs.org/): National Council of Information Sharing and Analysis Centers (ISACs)
- IBM White Paper (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03133USEN): Security Trends in the Manufacturing Industry