automotive IT international
The B2B magazine for automotive IT strategists

"When under attack, stick to the plan"

Who We Are
CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.
PROACTIVE CYBER PROTECTION
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
EMERGENCY COMMUNICATIONS
Automotive LOGISTICS
THE SUPPLY CHAIN CONFERENCE
In collaboration with
automotive IT
International

As industry becomes ever more connected, the risk of cyber attacks is increasing, Klint Walker, a senior US Department of Homeland Security (DHS) official, told the&nbsp;Automotive Logistics Supply Chain Conference&nbsp;in Atlanta last month.

Walker’s comments underlined how the growing complexity of industrial cooperations, interconnected supply chains and wider digital networks is raising the threat level.

“The security for your organization is only as good as the security of every other person you do

"When under attack, stick to the plan"

business with," said Walker, who serves as a cyber security advisor to DHS, working in the department's Cyber-security and Infrastructure Security Agency (CISA).

DHS is charged with protecting 16 critical infrastructure sectors in the US, and the automotive industry covers more than one of those. It is part of the manufacturing sector but is also involved with transport systems, commercial facilities, IT and the chemicals sector.

Walker painted a picture of a broad and varied manufacturing landscape with many potential areas of vulnerability.

Thanks to the growth in device connectivity and internet communications – the internet of things (IoT) – each business has multiple channels of entry through which hackers can gain access to important information and exploit it to their gain through theft or ransomware. &nbsp;As Walker put it, the 'attack surface' is getting bigger all the time.

By way of example, Walker said that when carrying out penetration testing on companies to assess their vulnerability, his favorite method was to go through the heating, ventilation and air conditioning (HVAC) systems of a location to get into the corporate network.

"Or I have used the elevator control systems to get access to private data," he said. "It is all interconnected; you are using one network to connect everything."

Technology mismatch

One of the main problems in making manufacturing operations and logistics networks secure is the need to marry IT and operational technology that were never designed to work together. The biggest issue: The different lifecycles. New IT systems are typically introduced in three-to-five-year update cycles, while operational systems can be in place for 40 years or more.

Walker said that the ways companies reduce risk to operational technology differs from the controls that can be easily applied in the IT environment. There are constraints that can make reducing cyber-security risk much more difficult; he gave the example of anti-virus protection, something that is commonplace in IT networks but can be difficult to deploy and maintain in an operational system.

Walker said critical manufacturing systems were designed as self-contained networks, separate to IT, where an engineer had to be physically present to administer any changes.

"When under attack, stick to the plan"

“Today [however] we have integrated them so that a person in a plant on one side of the country can administer the critical systems in a plant on the other side of the country, or link them with a business partner for real-time data flow for inventory control management,” Walker pointed out. That opens up the operational systems, the critical running of the plant, to attack, he added.

What is more, the people tasked with securing operational technology are now more likely to be IT specialists.

“Colleges are putting out IT specialists every year but there are not many operational technology experts coming out of trade schools any more, and certainly not many security operational technology specialists,” said Walker. “We are asking IT people to secure a technology they are not familiar with – and this is causing hardships through the organizations.”

There are lessons to be learned from the airline industry, which is subject to daily attacks on its security, Walker said.

“People are using thumb drives to hack airplanes and it is happening every day around us,” he said. “The ‘bad guys’ know what to do and are looking for a way to make money out of it.”

Stick to the plan

One of the most vulnerable channels for nefarious access to corporate networks is the employee and his own personal online activity. “How many of you use your home network to connect to your corporate one to work from home?” asked Walker. “The bad guys will attack your home network to get to your corporate network. The only thing protecting your corporate network is the VPN session and if you log on they have the tunnel right back to your network too.”

Walker also pointed to the vehicle itself as a risk point. “Think of the American automobile and all the things we are trying to put in it,” he said. “We are trying to make the car an extension of our home life. Those are all new attack vectors for the bad guys. The moment we put it in there is the moment they start looking at how they will break it and use it to their advantage.”

There have been recorded cases of autonomous vehicles being hacked already and the cyber-physical risks of large-scale hacking of internet-connected autonomous vehicles is now a cause for real concern.

Walker said it was crucial for company managers to know about their cyber-security processes and how they were integrated into the operational environment. It was also crucial to convey that to those working with data across all divisions of a company.

"When under attack, stick to the plan"

To deal with cyber attacks, every company needs to have a plan of action and needs to stick to it. “Know exactly what you need to do and who to do it with, because it is hard to make friends in a foxhole,” Walker said. “Make those friends now and know who to reach out to and how you are going take care of your business partners and your organization, and do it securely.”

-By Marcus Williams