Plant Services

Trust is not a strategy for cybersecurity

Let’s talk seriously about industrial cybersecurity: What you don’t know can hurt you.

By Sheila Kennedy, contributing editor

Jan 15, 2018

Industrial cybersecurity is all over the news, and not in a good way. Our most vital industries – including power, water, nuclear, oil and gas, chemical, food and beverage, and critical manufacturing – are under attack. The gravity of the situation became clear when the FBI and the Department of Homeland Security went public in October about existing, persistent threats. Virtually or not, bad actors are among us.

Unlike physical attacks, cyberattacks are nonstop. Cyber hackers have graduated from simple mischief and denial-of-service attacks to ransomware, theft of competitive information, interception or altering of communications, the shutdown of industrial processes, and even knowledge manipulation through the news and social networks (it’s bigger than just politics). Who knows what’s next?

Digitalization and connectivity are heightening cyber risk, though they are foundational to the Internet of Things (IoT), cloud computing, Big Data analytics, and artificial intelligence. Breaching a single connected operational technology (OT) device or system puts everything on the network at risk.

Low-security and small networks provide easy access for bad actors, whether they’re traditional hackers, black-hat hackers making money on the dark web, nation-states, or malicious insiders. Human error and negligence also are cyber risks.

To establish and sustain cybersecurity and restore the confidence of the public, greater awareness of threats and ownership of risks are imperative. In addition to mastering basic security measures, industry needs to detect and respond to attacks with persistence and resilience. Trust is not a strategy.

Fortunately, industrial software, technology, equipment, and service providers are fast ramping up their defenses, and dozens of new cybersecurity technology and services firms are offering to help. Consultants, legislators, regulators, and standards bodies also have prominent roles, but it is the end users, ultimately, who must put the cybersecurity puzzle together.

Here, several industry and cyber professionals weigh in about industrial producers’ cybersecurity risks and responsibilities and offer their actionable recommendations.

How bad is the problem?

When companies are surveyed about their top business risk, the answer increasingly is cybersecurity, says Alan Berman, president and CEO of the not-for-profit Disaster Recovery International Foundation (DRIF). The IoT – now a $3 trillion to $6 trillion industry – is opening new doors to cyber hackers. An estimated 50 billion connected devices (handhelds, sensors, etc.) are in use already.

Speaking at the Society of Maintenance and Reliability Professionals (SMRP) 2017 Conference, Berman noted that cyber hacking has matured to become a sophisticated industry seeking to penetrate devices and systems through the weakest link in the chain, with the goal of profitability. “It is a business and we have to deal with it as a business,” he explains.

The weakest link could be a vending machine in the plant, Berman says. “Once hackers get on the network, they can get into everything,” he says. “When that happens, it could be months before the breach is discovered. What looks like a malfunction could actually be a hack.”

Until there’s awareness within the maintenance organization of the security risks associated with adding or replacing a connected device, the number of cyberattacks an organization sees will continue to rise, says Howard Penrose, president of MotorDoc.

Penrose has easily uncovered industrial cybersecurity gaps using Shodan.io, a search engine for finding internet-connected devices. In one case, “We found numerous points of access to different IoT devices using (the organization’s) default passwords, including links to the documents with those passwords,” he says. “In another case, an OEM had installed software on wind generation systems that allowed them to be turned on or off with a smartphone app.”

Most people equate cybersecurity to the network or IT, but the things that go “boom” in the night are on the industrial control system (ICS) side, says Joe Weiss, managing partner at Applied Control Solutions. “Not enough people are looking at this,” he says.

Weiss has been compiling a nonpublic ICS cyber-incident database that he says already contains more than 1,000 actual incidents, representing about $50 billion in direct costs. Each new entry serves as a learning aid or reminder; often they’re logged in his cybersecurity blog.

“People worry about the IT/OT divide, but the real divide is what comes before and after the Ethernet packet,” suggests Weiss. “Before the packet is where the Level 0,1 devices live (sensors, actuators, drives), and that’s where cybersecurity and authentication are lacking.”

Related Content

Cybersecurity: Arm yourself

Thomas Wilk says the focus on cybersecurity has taken a sudden turn toward the processors…

It's a lock: Secure your network

Sheila Kennedy says vendors are joining forces to offer more-robust industrial network…

4 things you need to know about building a secure, IIoT-ready network infrastructure

How to get yourself connected.

Most Popular

Past 7 Days | Past 30 Days | Past 6 Months | All Time

01 **Trust is not a strategy for cybersecurity**
Let’s talk seriously about industrial cybersecurity: What you don’t…

02 **What to watch for in automation in 2018**
In this installment of Automation Zone, advances in robotics and analytics…

03 **Leverage coaching to get you in the game**
There are three distinct components that I consider necessary for the…

04 **DMDII opens its floor to manufacturers looking to test process improvements**
DMDII says it is "alleviating a bottleneck in the manufacturing R&D…

05 **Number of OSHA workplace safety inspectors declines under Trump**
In Mississippi, number of federal OSHA inspections fell by 26% from…

PlantServices

About

Contact Us

Advertise

Media Kit

Privacy Policy

Legal / T&C

Content

Blogs

White Papers

Webinars ▸

Special Reports

Events

Products

Magazine

Subscribe

Digital Edition

Issues Archive

Articles

Reprints

Site Tools

Site Map

Resource Centers

Training / Consulting Center

CMMS Review

Stay Connected

My Account

Newsletters

Social Media

RSS

Contact Us | Advertise | Privacy Policy | Legal Disclaimers, Terms & Conditions

P: 630-467-1300 | 1501 E. Woodfield Road, Suite 400N, Schaumburg, IL 60173

Chemical Processing | Control | Control Design | Food Processing | Pharmaceutical Manufacturing | Plant Services | Smart Industry

PutmanMedia®