THE WALL STREET JOURNAL.

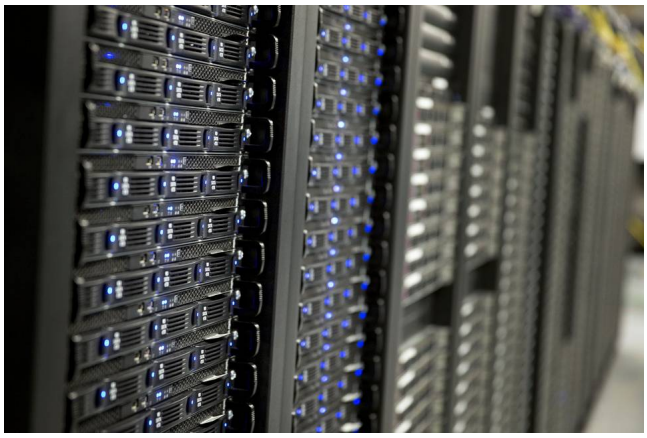


http://www.wsj.com/articles/cyber-risk-isnt-always-in-the-computer-1443125108

TECH

# Cyber Risk Isn't Always in the Computer

Vulnerable industrial systems that support data centers can open a back door to hackers



Networked computers are upgraded frequently, but the underlying equipment—backup generators, thermostats, air conditioners, and the like—are often vulnerable. Servers in a computer room. *PHOTO: ANDREW HARRER/BLOOMBERG NEWS*

By **ROBERT MCMILLAN**
Sept. 24, 2015 4:05 p.m. ET

On a sweltering summer day in San Jose, Calif., Scott Noteboom launched a cyberattack by exploiting a networking system vulnerability: the cooling system.

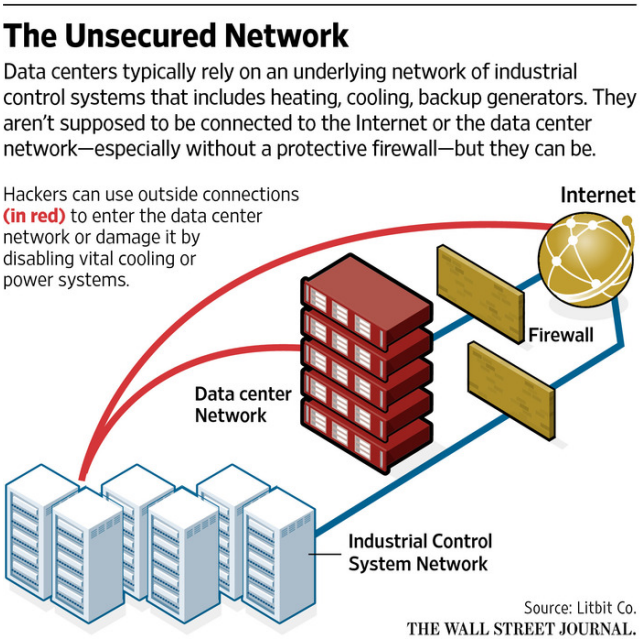
An assistant, standing before a collection of networked computer gear plus a cooling fan, plugged a cable into a laptop. Soon a light on one of the boxes started flashing: The fan was in trouble. It clicked, then stuttered, then moaned to a halt. The equipment soon would have melted down—literally—had the attack occurred in a real data center.

Mr. Noteboom isn't a hacker. He is the founder of Litbit, a startup launched two years ago to address a widespread security threat that

generally has gone unrecognized: The underlying equipment that typically supports data-center networks—backup generators, thermostats, air conditioners, and the like—are vulnerable to a cyberattack that would have the potential to take down the entire operation.

These "industrial control systems" are fixtures not only in data centers but in commercial buildings and factories. While networked computers are upgraded frequently, the equipment in this underlying layer may be on a refresh schedule measured in decades. They use hoary communication standards that lack basic security features such as password protection.

Information-security personnel don't expect those industrial systems to be wired to the computer networks they power or cool, yet they are often connected.




"If you talk to these companies, they'll swear up and down that their [industrial controller] networks are isolated" from their computer networks, including the Internet, said Seth Bromberger, owner of NCI Security LLC, which advises clients on network issues. "But many, many times, there's a connection that the engineers are not aware of."

Indeed, companies often configure the systems deliberately for remote access over the Internet. This lets workers retrieve data or adjust settings from a distance, but it also opens potential security holes in both the industrial controllers and the computer networks they support.

A recent survey by the security consultancy WhiteScope found nearly 20,000 such systems—including some for schools, hospitals, retailers

and others—accessible through the Internet, no username or password required.

Although few attacks on such equipment have been reported publicly, the problem isn't just theoretical. In late 2014, the U.S. Department of Homeland Security reported an "ongoing sophisticated malware campaign" that had "compromised numerous industrial control systems" from several manufacturers. Also last year, the German government said hackers had severely damaged a steel plant in that country by causing furnaces to malfunction. Similar methods were implicated in the 2010 Stuxnet attack, which The Wall Street Journal and others have attributed to U.S. and Israeli spy agencies, that destroyed approximately 1,000 uranium-enrichment centrifuges at Iran's Bushehr nuclear power plant.

"Is [the concern] overblown? I don't think so," said Jason Brvenik, a principal engineer at networking hardware maker Cisco Systems Inc. "I think there is a little bit of alarmism, but we just saw a Jeep get disabled [by hackers] on a highway. That is not trivial."

Some equipment makers have beefed up security. Rockwell Automation Inc. offers products that can log network activity and block instructions from unauthorized computers. General Electric Co. and Siemens AG have added similar capabilities to their industrial control products.

RELATED

- Cyber-Sleuths Track Hackers to China's Military (http://www.wsj.com/articles/cyber-sleuths-track-hacker-to-chinas-military-1443042030) (Sept. 23)
- Apple Targeted as Malware Infects Chinese Apps (http://www.wsj.com/articles/apple-targeted-as-hackers-infect-popular-chinese-mobile-apps-with-malware-1442750168) (Sept. 20)
- Startups in the Forefront of Battle Against Hackers (http://www.wsj.com/articles/startups-in-the-forefront-of-battle-against-hackers-1440381699) (Aug. 24)

But many facilities don't use the latest hardware, and existing equipment is designed to last 20 or 30 years, according to Matthew Fordenwalt, a director at Rockwell. "So you do have a lot of aging infrastructure out there."

The issue is on Washington's radar. This year alone, Industrial Control Systems Cyber Emergency Response Team—a part of the Department of Homeland Security—has documented 86 previously unrecognized security flaws.

Dale Peterson, CEO of Digital Bond Inc., a security consultancy that specializes in these systems, thinks the government could do more to

raise awareness of the vulnerabilities. "If the government were clear on that message, a lot of the C-level [executives] would jump into action."

Mr. Noteboom worked on a series of server farms for Yahoo Inc. in the late '00s; after that he was involved in infrastructure strategy, design and development at Apple Inc. He left Apple in 2013 with a list of network problems that needed to be solved in the data center industry and a plan to start a company to solve them. Problem No. 1: Security. "Every data center can be broken," he said.

Rich Kropfl, Yahoo's vice president of data center operations, said his company is testing Litbit's software. The issue is "absolutely top-of-mind for major companies," he added.

Apple said Mr. Noteboom didn't build or operate the company's current data centers and doesn't know about its network infrastructure or security protocols.

Founded in 2013 on $10.5 million from Jerry Yang's AME Cloud Ventures LLC and others, Litbit is developing RhythmOS: software designed to make industrial control systems easier to secure and manage. RhythmOS, which is still in the testing phase, communicates with such equipment through a special hardware interface that walls it off from the rest of the network.

The company plans to give away RhythmOS under an open-source license while selling support and updates—an entrée to a market for industrial controller software and services worth $8 billion according to Transparency Market Research.

Beyond the enhanced security, RhythmOS offers programmable control and management functions that cut costs, Mr. Noteboom said. At Litbit's headquarters, Mr. Noteboom showed off an iPhone app that gathered temperature, humidity and air pressure readings from a sensor on a computer rack. The app would notify him of vibrations in the room—an early sign that a hard disk was about to fail.

Vincent Hu of Zhongwei, China, is overseeing the construction of a large data center for a leading U.S. cloud-computing company. Before starting the project, Mr. Hu tried to find another product that could help him boost efficiency and lock down the data center's security, and so far seems satisfied with the test version of the software. "The Litbit software platform enables our data center to be the most efficient and it does this with high performance and security," he said.

*—Daisuke Wakabayashi contributed to this article.*

**Write to** Robert McMillan at Robert.Mcmillan@wsj.com