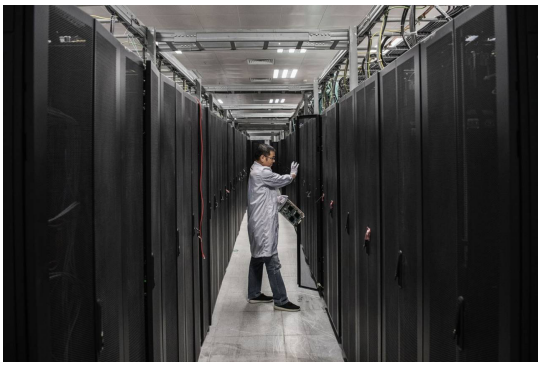
THE WALL STREET JOURNAL.

https://www.wsj.com/articles/companies-struggle-to-protect-their-technology-supply-chains-11559700240

BUSINESS | JOURNAL REPORTS: TECHNOLOGY

Companies Struggle to Protect Their Technology Supply Chains

The dizzying global network of components and suppliers makes it hard for companies to even know who their suppliers are



An engineer at Huawei Technologies, which has raised U.S. suspicions. PHOTO: KEVIN FRAYER/GETTY IMAGES

By Robert McMillan
June 4, 2019 10:04 pm ET

Three years ago, technicians at an Apple Inc. AAPL **-0.19%** ▼ laboratory discovered a worrisome problem with a server that was used by the company's data-analytics division. The server, built for Apple by a company called Super Micro Computer Inc., SMCI **-0.49%** ▼ was infected with malicious software.

Apple was a big Super Micro customer, with more than 2,000 of these servers in its data centers, but it quickly determined that the problem didn't affect any servers outside of the single machine in its lab. The company said in a statement posted to its website last October that the incident was "accidental and not a targeted attack."

Apple's experience, however, points to a question that is keeping executives in many industries awake at night: How can we protect our supply chain? More specifically, what should a company do if some kind of access point to its corporate data was planted in its network hardware—either through incompetence or malice—by one of the array of parts makers and assemblers of the complex systems that run today's computers?

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

Apple suppliers are scrutinized, and the hardware the company uses is subject to "ongoing vulnerability scans, patching, and security reviews," the company said in a letter to Congress last year. "Concern for supply chain security is absolutely central to the way we run our business," the letter stated.

In a statement, Super Micro said it was unable to find the malware that Apple had identified, and that the company works "closely with our customers on industry-wide concerns of this nature." After the incident, Apple stopped doing business with Super Micro, according to a source familiar with the incident.

The federal government has shown heightened concern about vulnerabilities in supply chains of U.S. tech companies, especially when components are built in countries whose governments theoretically could lean on the parts makers to use their products for spying. The U.S. government has clamped down on federal use of gear built by Chinese networking giant Huawei Technologies Co. and Russian antivirus maker Kaspersky Lab ZAO.

Huawei makes telecommunications equipment that U.S. government officials fear could be used to spy on the internet and on communications traffic that it carries.

"Huawei is a manifestation of a broader concern with supply chain," says Chris Krebs, director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.

In Kaspersky's case, U.S. government officials suspect that Kaspersky's antivirus software has been used to spy on the U.S. When installed, Mr. Krebs says, Kaspersky antivirus software has access to a broad range of data on personal computers that can then be sent back to Moscow for analysis by Kaspersky's researchers. The Russian government could then pressure Kaspersky to share this data, Mr. Krebs says.

A Kaspersky spokeswoman says that the company now stores some customer data in Switzerland and that Kaspersky does not believe that it could be compelled to hand over data under Russian law. Huawei has previously denied that it provides inappropriate access to user data and did not respond to messages seeking comment for this article.

The federal government is worried about Chinese efforts to access sensitive U.S. data in general, Mr. Krebs says. Last month, the Department of Homeland Security issued a memo about Chinese-manufactured drones and their ability to collect sensitive data that could then be sent back to China.

Russia and China have denied allegations that they conduct cyber-espionage on the U.S.

Concerns about vulnerabilities in U.S. supply chains, however, led the DHS late last year to form a special task force to share information on supply-chain-security problems and develop strategies to reduce the risk, Mr. Krebs says. Members of the group include such companies as AT&T Inc., T -0.26% ▼ Cisco Systems Inc. CSCO +0.15% ▲ and Microsoft Corp. MSFT -0.65% ▼ , along with government agencies and industry associations.

"Supply-chain management—logistics, sourcing, diversity—that's something that's been in play since pretty much the dawn of trade," says Mr. Krebs. "But the risk-management piece, with diversified global supply and value chains—it's an emerging discipline."

To be sure, the complexity of today's dizzying global network of components and suppliers is a big part of the problem. For most big companies, even understanding who their suppliers are can be a challenge. In a 2018 survey, the consulting firm Deloitte Touche Tohmatsu Ltd. found that 65% of corporate procurement officers had little or no visibility into the subcontractors for their direct suppliers.

For printer and personal-computer giant HP Inc., HPQ -0.12% ▼ Tommy Gardner, chief technology officer of HP Federal, says the key to mitigating supply-chain risk is to identify the critical components—the microprocessors and firmware, for example—and personally know not just who builds them, but the subcontractors who supply the builders as well.

"It's all based on personal relationships and getting to know people," Mr. Gardner says.

Worries about supply-chain vulnerability go beyond malware threats and spying. Last month,a Japanese maker of industrial control systems, Yokogawa Electric Corp. 6841 2.73% ▲ , warned that some of its customers had received counterfeit products that were disguised to look as if they came directly from Yokogawa. According to the company, the products—copies of instruments for measuring pressure—were shipped by Chinese counterfeiters in fake Yokogawa boxes. The counterfeit devices are "severely inferior in quality" and "pose a serious safety risk," Yokogawa said in a note to customers.

In the U.S., meanwhile, it is worries about computer and networking supply chains that dominate the headlines.

The idea that information-stealing software could be inserted into a computer or piece of networking equipment at some point in the supply chain is inspiring U.S. corporations to take a closer look at the security of their product designs and ensure that they are tested and reviewed, says David Burg, the head of Ernst & Young's cybersecurity consulting practice in the Americas.

But many security experts say the bigger danger is from hackers getting access to U.S. computer systems by exploiting devices that ship with bugs in their software or substandard parts that make them vulnerable to attack.

"That's what's blowing people's minds," says Frank Heidt, chief executive of Leviathan Security Group Inc., a computer-security consulting firm that evaluates the security of computer systems. The real danger, Mr. Heidt says, is suppliers who insert low-quality components to slash costs. "It's not getting a motherboard with a rigged chip on it; it's getting a motherboard with ridiculously outdated drivers."

Experts agree the risk of inferior components adds another significant layer to the more general challenge of securing supply chains and protecting U.S. data networks at the same time.

For Mr. Krebs, the Homeland Security official, the challenge is nonstop.

"There are moments where I wake up in the middle of the night in a panic," he says, "just given the scope of the problem that we're trying to get our arms around here."

Mr. McMillan is a reporter for The Wall Street Journal in the San Francisco bureau. He can be reached at robert.mcmillan@wsj.com.

Appeared in the June 5, 2019, print edition as 'Companies Struggle to Protect Data From Vulnerabilities in Complex Supply Chains.'

- **College Rankings**
- **College Rankings Highlights**
- **Energy**
- **Funds/ETFs**
- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**