The New York Times

Manufacturers Remain Slow to Recognize Cybersecurity Risks

By Ellen Rosen

Nov. 21, 2018 Published in https://www.nytimes.com/2018/11/21/business/manufacturers-remain-slow-to-recognize-cybersecurity-risk.html

They have names like Notpetya, Samsam and perhaps the most cynically named WannaCry.

These are just some of the most recent cyberattacks that have not only affected financial institutions, retailers and shipping companies but have also plagued manufacturers, like Merck & Company, the pharmaceutical firm, and the snack company Mondelez International.

Whether they come from ransomware, phishing or more arcane, highly sophisticated means, manufacturers are increasingly vulnerable to attacks that can shut down production and have ramifications throughout a supply chain.

And it is not just the giants that get hacked; external threats can be agnostic, affecting manufacturers regardless of size.

Thomas Siebel, the chairman and chief executive of C3, an artificial intelligence platform based in Redwood City, Calif., and the founder of Siebel Systems, puts it more bluntly, “Manufacturers are sloppy when it comes to cybersecurity.”

The Taiwan Semiconductor Manufacturing Company learned that the hard way in August. A third-party vendor shipped software to the chip maker without pre-screening it. An engineer at Taiwan Semiconductor failed to scan the software, which was infected with the WannaCry ransomware, installed it and then connected it to the company’s operating system. The undetected virus then spread.

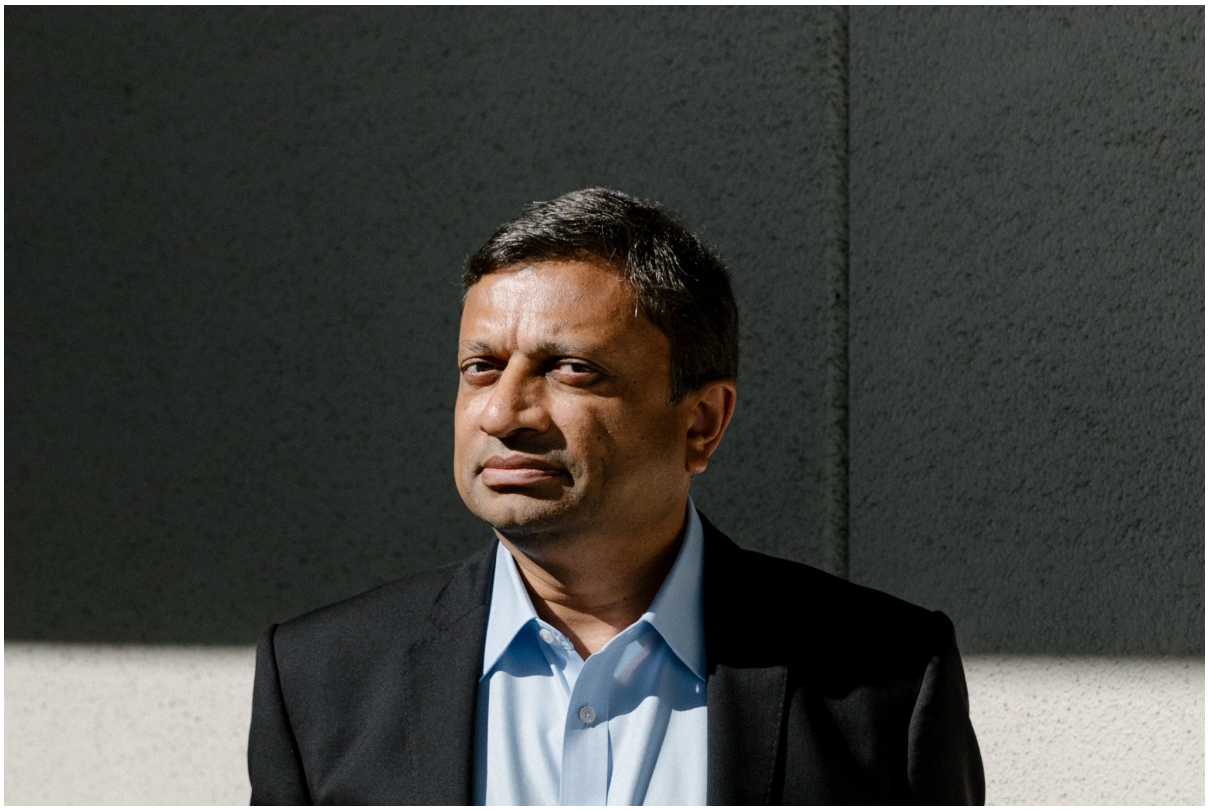
The chief executive, C.C. Wei, speaking at a news conference at the time, rejected rumors of hacking. Instead, he acknowledged, it was “purely our own act of negligence.”

But the company was lucky. A full recovery took only a few days, and while initially it seemed that third-quarter revenue would be off by 2 percent, Elizabeth Sun, a company spokeswoman, said in an email that the revenues did not suffer because Taiwan Semiconductor fulfilled some of the delayed orders, while “increases in demand in other areas” helped to offset the losses.

Mondelez International and Merck suffered much more significant losses after the 2017 Notpetya attack, although they described them differently in filings.

In its annual report for 2017 filed with the Securities and Exchange Commission, Mondelez stated that the “malware affected a significant portion of our global sales, distribution and financial networks.” The net revenue loss, the company said, was less than 1 percent of the company’s global net revenues of $25.9 billion. That still amounts to $103.6 million. In addition, the company incurred “incremental expenses of $84 million predominantly during the second half of 2017 as part of the recovery effort.”

Merck, in its S.E.C. filings, stated that the attack “led to a disruption of its worldwide operations, including manufacturing, research and sales operations.” The fallout was significant: a $260 million loss in sales for 2017 with an expected additional loss for 2018 of $200 million. The total costs for expenses and remediation are $285 million, a net amount after insurance.



Manesh Patel of the Sanmina Corporation. He said many I.T. organizations focused on operations such as human resources, but still weren’t as well connected to the manufacturing side of the business. Jason Henry for The New York Times

Unlike Taiwan Semiconductor, neither Merck nor Mondelez described how the malware infected their operations.

Boeing was said to have been attacked by WannaCry as well in March, but the company downplayed the hacking.

While manufacturers weren’t traditionally at risk when hackers sought troves of individual data that could be sold for financial gain, motives have become more complex.

Some using ransomware hope to extort money — sometimes in the form of cryptocurrencies — from companies whose systems are shut down. Others seek to steal intellectual property — a host of trade secrets including patent information and formulas, as well as blueprints and schematics.

And last year's NotPetya attack, which overall inflicted more than $1 billion in damage worldwide, was linked to the Russian military, the C.I.A. found.

Irrespective of method or motive, the costs can be high, whether resulting from the ransom demands or the ensuing business disruption. Michael Tanenbaum an executive vice president of insurer Chubb, said attacks "have gone from being a nuisance to significant, with some demands exceeding seven figures."

Apart from the disruption to business, public companies that are hacked may also face scrutiny by the S.E.C. for failure to have a sufficient system of internal accounting controls, the agency warned in October.

It doesn't need to be that way, Mr. Siebel said. "It's amazing what you can do with off-the-shelf cybersecurity products. Ninety percent of penetration can be stopped with fundamental practices that most people aren't following, like employee training, two-factor authorization, changing passwords and fixing USB ports so they can't download."

The vulnerabilities run from the mundane to the high-tech. Despite training and repeated warnings, employees still open phishing emails that can disrupt a company. Mr. Tanenbaum said that, according to a Chubb index, 50 percent of manufacturing losses in 2018 had resulted from phishing attacks or those known as "spear phishing," which used some specific information to trick the recipient.

"It means that individuals are clicking on links more readily in manufacturing than other industries," he said. "This can cause real harm."

But there's much more. A manufacturer's exposure exists throughout a facility. Rare is the employee who punches a clock at the beginning of the day; instead, workers log in with passwords or biometrics.

The vulnerabilities can be surprisingly simple and can emanate even from outdated equipment. John Reed Stark, president of John Reed Stark Consulting, a cybersecurity advisory firm, said a company, could, for example, have an old printer remain on a network even if it's not used. A hacker could, through a phishing scheme, pick up the administrative passwords and then gain network access through the obsolete, but still connected printer. "And it can be difficult to know exactly what's been exfiltrated — or stolen — from the network."

Employees inspecting computer chip boards at the Sanmina Corporation.
Jason Henry for The New York Times

That was the vulnerability with the Notpetya attack — outdated Windows XP for which there hadn't been updated security. While Microsoft did release a so-called patch to fix the problem, other outdated technologies still in use can result in exposure.

So-called ntracontrol systems can connect aging as well as newer equipment, and frequently it's difficult to shut some down without disrupting production. But if a manufacturer doesn't take equipment offline to update security, there's a risk that a ransomware attack, for example, could take an entire production line down, Mr. Tanenbaum explained.

The growth of the Internet of Things — the direct connecting and communicating of disparate pieces of equipment — makes the potential for abuse even worse. While it is not yet considered an immediate concern, as hackers develop more sophisticated methods, the exposure could grow exponentially.

"Manufacturing equipment is getting smarter, and we're now moving into the information technology world in the manufacturing space," said Manesh Patel, the senior vice president and chief information officer of the Sanmina Corporation, a Fortune 500 maker of optical, electronic and mechanical products based in San Jose, Calif. Many I.T. organizations, he added, focus on operations such as human resources, but still aren't as well connected to the manufacturing side of the business.

MForesight an independent, nonprofit manufacturing consortium focused on “technology, policy and the work force” has sounded the alarm and among other recommendations, suggests establishing organizations to “facilitate fault-free, anonymous sharing of incidents, threats, vulnerabilities, best practices and solutions.” The group also suggests developing a “comprehensive framework specifically for manufacturing supply chain cybersecurity, similar to existing frameworks on cybersecurity and cyberphysical security.”

While comparing information seems at odds with companies that often compete, Mr. Patel, for one, stressed the importance of superior cybersecurity measures over a perceived competitive advantage.

Mr. Patel, who said his company’s investment in cybersecurity measures has “increased 100 percent over the past three years,” also recommended segmenting, which means keeping systems on a network separate from each other. This can permit vendors to regularly update its equipment without having access to other parts of the system.

Segmenting, he explained, secures a network so that it is not exposed to a potential breach from the vendor. It’s a relatively new area and if done incorrectly, can cause its own headaches. “We’re at the early stages of getting the grips of it.”

Mr. Siebel has also asked known hackers to test his system by trying to infiltrate it. “We have hackers beating up our systems, and so far only one guy has gotten through, and we paid him a reward. He found a vulnerability, and we fixed it.

Another approach is to adopt something called whitelisting. For years, Mr. Patel said, most companies had software that excluded known viruses, essentially blacklisting potential problems. But that was too reactive and sometimes exposed systems to unknown attackers. Now, he said, the better approach is to whitelist — that is specify approved software applications that are permitted to be active on a computer system. “It’s increasingly become one of the most important types of defenses.”

Manufacturers also need to know the precautions that others — whether suppliers or customers — are taking, especially as they have increased access to equipment.

“You are only as strong as your weakest link,” Mr. Stark said. “Hackers will find that weakest link and can break in and attack others in the supply chain. Companies are connected in ways that are extremely complex, and anyone in the supply chain can be vulnerable and could be the source of an attack.”