These are the cyberthreats lurking in your supply chain

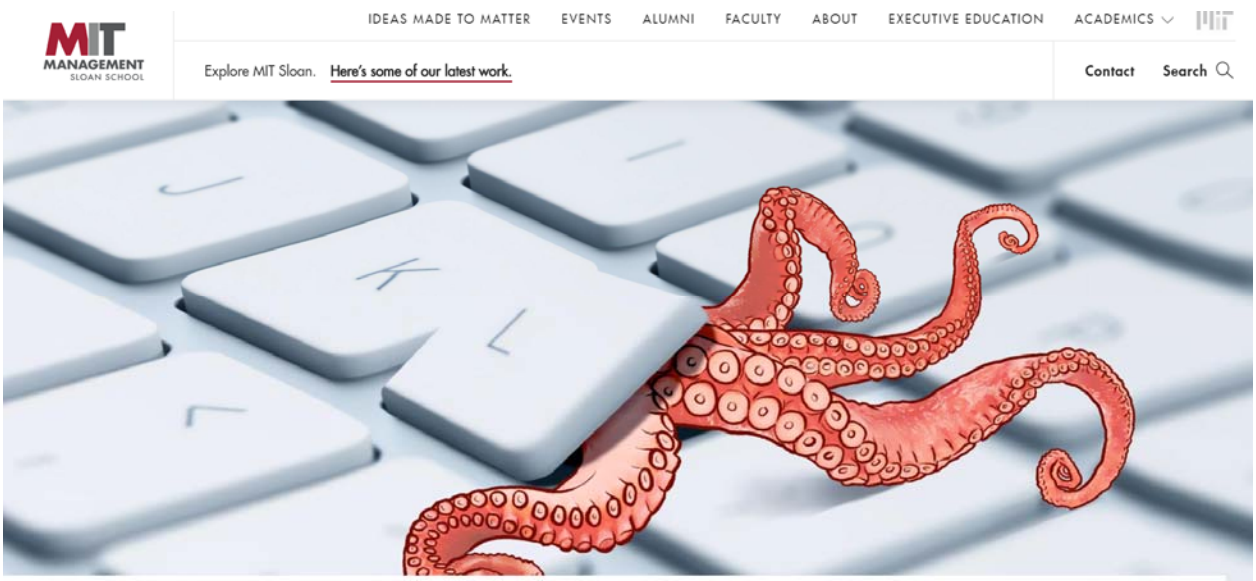
Tom Relihan

Working Paper CISL# 2019-04

February 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

IDEAS MADE TO MATTER
CYBERSECURITY



These are the cyberthreats lurking in your supply chain

By Tom Relihan, Feb 19, 2019

Why It Matters

Effective cybersecurity involves more than just erecting a firewall. You have to clean up your supply chain, too.

You've got firewalls in place. You have a team dedicated to keeping a careful watch over your networks, 24/7. Everything is under two-factor authentication. Your cyber defenses must be bulletproof.

Then your screen goes dark, and it doesn't light back up. Soon, your company is offline entirely, and you're losing money — fast. You didn't account for the contractor that you hired to upgrade your point-of-sale network last month, which required accessing your systems — or what the state of their own cybersecurity looked like.

Turns out, it's not good.

The vast majority of firms approach cybersecurity from a perimeter-defense mindset, focusing on keeping out hackers and other bad actors who shouldn't be able to access their systems,

according to Stuart Madnick, a professor of information technologies at MIT Sloan. But organizations often fail to consider attack vectors originating, intentionally or unintentionally, with outside individuals, contractors, firms, or groups that *are* authorized to access those systems — so-called third-party or supply chain cyberattacks.

"The thing they aren't thinking about are people who somehow, one way or another, can slide right in," Madnick said. "Because once you've slid in, then all those perimeter defenses are next to useless."

Madnick, a founding director of Cybersecurity at MIT Sloan, said these types of attacks typically come in one of five forms: through physical parts or components bought from suppliers; through use of network service providers; from external software providers or partners; from physical service providers and outside contractors; and through mergers and acquisitions.

Here's how to defend against them.

Software service providers and outside contractors

For shipping giant A.P. Møller-Maersk, the installation of a single piece of accounting software in an office in Ukraine saw global operations grind to a halt and thousands of company computers rendered completely useless. That's because the smaller company that made the software, Linkos Group, had been compromised by a powerful piece of ransomware called NotPetya, which hijacked its update servers and used it as a beachhead to squirm into their client's networks. The results were devastating for firms across the globe, whose shipments were delayed.

The exploitation of smaller, typically less-secure companies who have access to or credentials for the networks of larger corporations for the purpose of either providing software services or contracted work is becoming increasingly common. Supply chain attacks rose by 150 percent between 2016 and 2017, according to cybersecurity company Symantec.

150

Supply chain cyberattacks rose by 150 percent between 2016 and 2017.

At Maersk, "It started off with a supply chain, which was the supplier of their accounting software, and that got it through the firewall," Madnick said. "More and more software services are providing automatic updates, so it's not an uncommon phenomenon."

In recent years, such methods have been attributed to major breaches at companies like Target, where hackers gained access through a contractor that performed ventilation work for the retail

chain and made off with reams of customers' personal data. The U.S. electric grid has been targeted through similar tactics.

"A lot of these companies are vulnerable," Madnick said. "[Contractors] will come to your plant, and they may have their own laptops that they plug in to do diagnostic work, and you don't know what else they're bringing in when they plug into your network."

Any firm that plans to partner with a contractor or service provider would be well-served by conducting a security audit of that partner prior to entering into a contract or allowing any work to happen, Madnick said. Organizations could create a framework for evaluating and scoring a potential partner's security operations, or conduct "stress tests" on their networks. "You could then say, 'We will only partner with software providers who are level eight or higher,'" he said.

For the smallest of partners, like independent contractors who might not even have an IT or cybersecurity department, Madnick recommends they work with a consultancy to bring their defenses up to par prior to the partnership.

"This can be a tough one, because you're talking about small organizations using unsophisticated systems and who don't have a lot of resources, and of course, the country is made up mostly of that," Madnick said. "You say, 'What's the big deal, why would Russia or North Korea want to hack into a company with four employees?' Well, that guy with the four employees is the access point to the U.S. power grid or Bank of America."

Mergers and acquisitions

Another potential point of complication for a company's cybersecurity landscape presents itself when a firm acquires a smaller firm or startup, or when two firms merge.

"A company maybe feels relatively good about security, but they've just acquired a company, typically a smallish one, and they want to, of course, get economies of scale and synergies. The question is, how good is the security in that company?" Madnick said.

The solution is similar: Do your homework before the merger or acquisition, don't wait until it's too late.

Physical components

Madnick said a third potential supply chain cyberthreat could be baked into the supplies themselves, either in the form of hidden "backdoors" embedded in software to allow secret, remote access, or through equipment outfitted with malicious hardware designed to steal information or hijack the system it's part of.

Last year, concerns about this sort of attack led the heads of the U.S.'s major intelligence agencies and House Intelligence Committee to advise Americans not to use products designed or sold by two Chinese telecommunications equipment makers, ZTE and Huawei, labeling such

products as national security threats. In August, the Trump administration outright banned use of the companies' products by the U.S. government or any government contractors. Such concerns have been voiced by government officials for nearly a decade.

Global supply chains are also extremely complex, Madnick said, and it's hard to tell whether a particular piece of equipment has either been compromised by the manufacturer itself, or by other actors intercepting and tampering with it along the chain.

The best way to prevent such attacks is to keep close tabs on your supply chain, with the goal of being able to determine the provenance of each component, so that you'd be able to identify any points of contact that could pose a risk. "There are a lot of reasons you might want to do that, and there are lots of reasons why it's not easy to do," Madnick said.

Why would Russia want to hack a company with four employees? Well, that guy with the four employees is the access point to the U.S. power grid.

"Why would Russia want to hack a company with four employees? Well, that guy with the four employees is the access point to the U.S. power grid."

Stuart Madnick
Professor

Network services

Do you know the route your digital traffic takes from one point to the next over the internet? It's hard to be entirely sure, Madnick explained: Information sent across the internet from a computer in Cambridge, Massachusetts, to another in Washington, D.C., tries to find the fastest path there, not necessarily the shortest. That means your data could be routed through a hub in New York City, or it could pass through one in Beijing, if it reports faster speeds — where malicious actors could get their hands on it. This has actually happened, though allegedly only by accident, Madnick said.

Madnick says one way to defend against threats of data being intercepted and read during transmission over networks is to use encryption technologies like virtual private networks. Special browsers like Tor, designed to hide the location and other information about its user, can make it harder to tell when a lot of internet traffic is passing between two points, which could in itself be revealing, Madnick said.

Future threats

Looking forward, Madnick said a likely sector for future cyberattacks is the emerging “internet of things” — devices that connect to the internet for increased functionality, like home security cameras and lighting systems, and can be accessed remotely via smartphone or industrial equipment.

Any device that can be connected to the internet can pose a cybersecurity risk, and “the number of internet-connected devices is exploding,” Madnick said. “The worst is yet to come.”

Even more troubling, he said, companies tend to prioritize time-to-market for these products rather than than moving more slowing to ensure they’re up to security standards. “IoT gives the hacker many more access points, and they’re typically weaker access points, at least initially.”

But, by incorporating cybersecurity into the design from the beginning, you can end up with more secure and higher quality products, Madnick said.

FOR MORE INFO

Tom RelihanNews Writer(617) 324-7793 trelihan@mit.edu