MITSloan MANAGEMENT

INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

(IC)³

Interview: "What Executives Get Wrong About Cybersecurity" Sloan Management Review

Stuart Madnick

Working Paper CISL# 2017-01

January 2017

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

[RISK MANAGEMENT]

What Executives Get Wrong About Cybersecurity

If you think the biggest cybersecurity threat most businesses face is credit card theft and the most important part of the solution is better prevention technology, think again.

STUART E. MADNICK, INTERVIEWED BY MARTHA E. MANGELSDORF

Cyberattacks are in the news. All kinds of organizations — ranging from Target Corp., Yahoo Inc., Sony Pictures Entertainment, and Bangladesh Bank to the Democratic National Committee in the United States — have fallen victim to them in recent years. To gain a better understanding of cybersecurity threats — and what executives should do to better protect their companies — *MIT Sloan Management Review* sought out cybersecurity expert Stuart E. Madnick.

Madnick has been studying computer security for a long time. He coauthored his first book on the subject in 1979 and today is the director of MIT's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³, a consortium that brings together academic researchers, companies, and government experts. Madnick, who is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management and a professor of engineering systems at the MIT School of Engineering, spoke about trends in cybersecurity recently with *MIT Sloan Management Review* editorial director Martha E. Mangelsdorf. What follows is an edited and condensed version of their conversation.

ALEX NABUAM/THEISPOT.COM

***MIT SLOAN MANAGEMENT REVIEW:* Why did the MIT cybersecurity consortium you lead choose to focus on the nation's critical infrastructure?**

MADNICK: Much of the attention about cybersecurity has been focused on things like stealing credit cards — which is important, and we don't neglect that. But surprisingly little attention has been paid to cyberattacks on critical infrastructure. You don't hear much about the Turkish pipeline explosion or the German steel mill meltdown. You may have heard a little bit about the cyberattack on the Ukrainian power grid that happened around Christmas in 2015. Generally, these events involving attacks on infrastructure do not get much attention; they're not quite as sexy as movie stars' emails being revealed. But they have the potential to have far bigger impact.

Our feeling is that we need to increase the attention we pay to cybersecurity for important infrastructure. It doesn't mean we're going to ignore everything else, but there are some things that are particularly unique to those kind of attacks.

Think about preparedness. For example, what if it turns out that a cyberattack causes the New England power grid to go down — and remain down — for three months? What preparation has the governor of Massachusetts, the mayor of Boston, or MIT made for going three months without power? The answer is probably "not enough."

Losing power for such a long time is not out of the question. How is this possible? If your personal computer goes dark, what do you do? You reboot it. If worse comes to worst, you wipe it clean and reload it. But imagine if your turbine breaks down due to a cyberattack. You can't just go to a local turbine store. For example, MIT's cogeneration facility had a turbine failure recently — not because of a cyberattack, but because of mechanical failure due to a simple defective nozzle. Still, it took three months to repair the turbine; these things are huge, and many of the parts aren't readily available.

Let me tell you about the attack on the Ukraine power grid in 2015, because it's a fascinating story. The Ukraine is divided into a number of separate power grids, much like the [United States]. Three of the power grids were attacked and went down, and about 225,000 people lost power for several hours.

I attended a briefing about the attack; there were a number of people, particularly from the [United States], who went over to Ukraine to understand exactly what happened. And I was surprised by two of the investigators' conclusions.

The first conclusion had two parts:

1. The attack was low in sophistication. The attackers used seven different techniques to down the grid, but all of them were readily available for sale on the internet. No new weapon had to be created; there is a huge cybercrime ecosystem operating on the internet.
2. But the attack was high in organization. The hackers had to go and assemble the seven weapons together. And they did some very clever things. Not only did they down the power grid, they also shut down the backup system, so even the power company had difficulty getting back online. They also erased all the disks, so it was hard to track down what they had done.

And then to add insult to injury, they overloaded the power company's call center so that customers couldn't call in to tell the power company that they lost power. How is that for being malicious? This was not a teenager doing a casual hack.

The second conclusion that investigators came to as they looked into the attack was: This was only a demonstration. The hackers could have done much, much more damage. This was a political statement, saying in effect: "We're here. We're not going away." And, in this case, the finger is pointing to the Russians.

But we can't be sure about that. I met someone who does hacking for governments. He happens not to work for the [United States], Russia, or China. He says that, in all of the software he and his colleagues develop, they make sure that all of their comments are in Chinese. The point being: If you're really good at hacking, you'll make sure all the evidence points to someone else. So if you think you know who is behind a hacking attack, most likely that isn't who it is.

"If you don't address the managerial, organizational, and strategic aspects of cybersecurity, you're missing the most important parts."

— STUART E. MADNICK

What are the most important things business executives can do to decrease their companies' cybersecurity vulnerabilities?

MADNICK: If you don't address the managerial, organizational, and strategic aspects of cybersecurity, you're missing the most important parts. A lot of people are working on developing better hardware and software, and that's good. That's important. But that's only a piece of the puzzle.

Estimates are that between 50% and 80% of all cyberattacks are aided or abetted by insiders, usually unintentionally — typically through some kind of "phishing" expedition [involving emails containing a link or attachment to click on]. Untargeted mass phishing emails have an open rate of 1% to 3%. But highly targeted "spear phishing" is much more effective, with an open rate of about 70%. With spear phishing, you'd get an email that appeared to come from a high-ranking executive at your company, that referred to you personally and that asked you to take some specific action consistent with your job, such as authorizing a new employee or transferring funds to a new vendor.

So if you don't address the people issues, you're missing the really hard cybersecurity problems. A lot of the vulnerabilities that exist in organizations come from the corporate culture we create and the practices we have. I'll give you some examples.

We work with energy companies. I was talking to someone who had visited the headquarters of one of them, and he said that if you're going up or down the stairs and not holding the railing, someone will actually stop you and say, "Please hold the railing, for safety." That's how ingrained they have gotten the idea of safety. I was told that if you're walking down the hallway texting on your phone, someone will say, "Stop. Either do your texting, or do your walking. Don't do both." Because they understand that if they do something wrong in oil refining, plants can blow up, and people die. That safety mindset permeates the organization.

Another example is: When you walk into an industrial plant, you will often see a sign that says, "520 days since the last industrial accident." If you walk into a data center, do you ever see a sign that reads, "520 milliseconds since the last successful cyberattack?" Do you even know how many attempted cyberattacks there are on your company on a typical day?

Companies need to develop that kind of safety culture and mindset about cybersecurity. Think of it this way: I could put a stronger lock on my door, but if I'm still leaving the key under the mat, have I really

What Executives Get Wrong About Cybersecurity

(Continued from page 23)

made things any more secure? Although that's an oversimplification, that's the phenomenon in organizations: We're building stronger doors but leaving keys all over the place. That's why the organizational and managerial aspects of cybersecurity are so critical.

But cybersecurity has to be done across the value chain, doesn't it? Because it's not enough if your company has great cybersecurity policies, if they don't extend to your suppliers.

MADNICK: You're right. People often use the expression "e2e" — end to end. Your piece of the puzzle may be perfectly secure, but nowadays, everybody is interconnected in one way or another.

For example, the break-in that Target experienced took place through a heating, ventilation, and air conditioning maintenance company, which had access to some Target systems. Likewise, the SWIFT messaging platform for financial institutions was exploited through vulnerabilities at Bangladesh Bank, which lost $63 million.

Is there any industry that you see doing a really good job at managing cybersecurity issues?

MADNICK: I'd rate industries from poor to terrible. On that scale, financial services is probably doing a better job than most other industries. On the other hand, they're the ones who are probably the targets of the largest number of attacks. So they may be twice as good at cybersecurity, but if they have four times as many attacks, that doesn't mean they're in great shape.

I don't know which industry is the poorest, but hospitals clearly are vying for that position. According to one recent report, 88% of all detected ransomware attacks [where computers are "held hostage" unless the user pays] on organizations are targeted to hospitals, because they're easy targets. If you're a hospital and you're held up for ransomware, would you pay it or not? If your hospital's computers are held hostage, the patients in the hospital are now to some extent at increased risk. You no longer have access to up-to-date medical records, such as test results and changes to medication. So by not paying, you are possibly putting people's lives at risk.

What cybersecurity advice would you like to give to *MIT SMR*'s audience of business executives?

MADNICK: Think in terms of a three-pronged approach: prevention, discovery, and recovery. Gartner recently came out with a report entitled "Prevention Is Futile in 2020." This is consistent with our viewpoint that if the Pentagon can be broken into, if the NSA [U.S. National Security Agency] can be broken into, if the Israeli Defense Forces can be broken into, why do you think you can't be broken into?

That's why you need to think in terms of all three steps. Of course, you want to do as much prevention as you possibly can, within reason. But the next two steps are detection and recovery. According to several studies, the average cyberintrusion can go on for more than 200 days before it is discovered. I also read a recent report that says in the Asia Pacific region it's 520 days — more than double.

So our ability to detect that something funny is going on is pretty poor. By the time you discover the attack, the hackers have probably been rummaging around, stealing documents, and doing things for a long time.

I joke that if at 5 o'clock every day, one of the people leaving the bank walks out with a wheelbarrow full of money, do you think someone would notice after a few days? Yes, probably! But things like that happen all the time in computer systems, and nobody is paying attention. Maybe it's not quite as visual, but there are funny things going on, and often no one is even looking to see if there's anything suspicious.

And then finally, recovery is very happenstance. By and large, CEOs are caught unprepared when someone shoves a microphone in front of them to talk about the cyberattack that was just discovered at their company. And that's just part of the recovery. Other questions to figure out: Have we actually cleansed our system, or is the attack still going on? How do we make sure it doesn't happen again next week?

Much like my comment that industries range from poor to terrible on cybersecurity, the same thing applies to the three prongs. Most organizations are poor at prevention, pretty bad at detection — and probably terrible at recovery.

I jokingly say that not that long ago, cybersecurity was a task you assigned to the junior assistant programmer trainee, and his job was to go desktop to desktop loading the latest Microsoft patches. Now you're having the CEO of the company being interviewed by the news station when a cyberattack is discovered. So it's been a total inversion, if you will, up to the highest level of the organization. Until recently, most CEOs barely even knew how to spell cybersecurity! So there are lots of issues to deal with. What is the cybersecurity education needed at each level of the organization? What is the preparation needed? How do we deal with these attacks? Executives need to take these questions seriously.

Back in 1979, I coauthored a book called *Computer Security*. What's interesting is that the conclusion to one of the chapters was, essentially, that if you don't address the people issues in computer security, you're missing half of the problems. When I repeated that message at a recent meeting with executives and said that I thought that was still true today, I was criticized because, as one executive put it: "You greatly understate the human contribution to the problem — it is far more than 50%!"

Reprint 58232. *For ordering information, see page 4.*