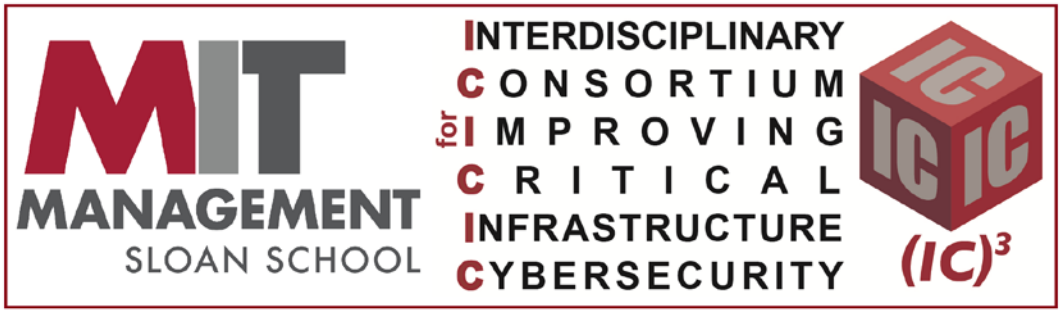

Stuart Madnick: Taking a Management Approach to Fighting Cybercrime

Meghan Laska

Working Paper CISL# 2017-05

April 2017

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

STUART MADNICK: TAKING A MANAGEMENT APPROACH TO FIGHTING CYBERCRIME

Preventing a hack takes more than a software patch.

By Meghan Laska

Have you ever had the nightmare where you log in to your bank account and discover that the bank has been hacked and it looks like your money is gone? At the recent Cambridge Cybersecurity Summit, hosted by MIT in conjunction with CNBC, the question for panelists was: Could this really happen? Stuart Madnick, the John Norris Maguire (1960) Professor of Information Technology, answered, "Not only could this happen, it is inevitable." He says, "If you haven't been hacked yet, it's only a matter of time." Madnick has been studying cybersecurity issues since the late 1970s and coauthored one of the first textbooks on the topic, *Computer Security*.

When it comes to cybersecurity, Madnick's key message to businesses is that this is a management issue, not just a software or hardware issue. He explains, "As recently as five years ago, cybersecurity largely involved a junior assistant walking from desk to desk with the latest security patches from Microsoft. This issue is starting to get more attention, but management still has a lot of work to do."

According to several studies, attackers can operate inside an organization's computers for an average of 243 days before they are detected. In the Asia-Pacific region, that number jumps to more than 500 days. Also concerning is the statistic that up to 80 percent of breaches are aided or abetted by insiders, often unintentionally from an employee who opened an attachment in an email.

"You may be under attack now and just not know it. It is important to address the managerial and strategic aspects of cybersecurity, and we are uniquely positioned to do that at MIT Sloan," says Madnick, who is the academic director of MIT Sloan's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, also known as (IC)^3. "Our goal at (IC)^3 is to raise awareness and build a safer world."

POOR INCENTIVES

At (IC)^3, a major focus is on the incentives and disincentives for organizations when it comes to the cybersecurity of infrastructure. Within that umbrella, an important question involves partnering and data sharing.

"If a cyberattack knocked out power to your business, what is your reporting obligation? Who would you contact? There are many business reasons you may not want to report the hack: to protect your reputation, fear of encouraging copy cats, and fear of legal liability. Decisions about who to call, what to say, and what information to share are management issues. It comes down to understanding incentive systems and goals," explains Madnick.

In a recent paper on this topic, Madnick and fellow researchers identified about 120 organizations around the world focused on data sharing. "We found a cobweb of organizations that is dusty, messy, and not well organized. There is a lot of information sharing happening, but it's not effective."

For example, he points to the creation of Financial Services Information Sharing and Analysis Centers (FS-ISACs) set up for specific industries like financial services. If a major bank is attacked, the bank should contact the FS-ISAC. Yet when the SWIFT funds transfer network was attacked, SWIFT created its own information sharing initiative, separate from ISAC.

Several of the top banks, says Madnick, also meet privately to share information with one another—not the entire banking community.

"This is a trust issue, and it shows there is a fundamental problem with the incentive system. We know what isn't working, so we are looking at what can be changed to make the information sharing process work better," he says.

PUTTING SAFETY FIRST

Another $(IC)^3$ project involves changing corporate culture—and incentives—to increase cybersecurity internally. "We want to take research on how industrial organizations have improved safety over the past decade to see how we can apply those lessons to improving cybersafety in companies," notes Madnick.

He points to ExxonMobil as an example of how this can work. "If you walk down the stairs at Exxon's headquarters, someone will ask you to hold the handrail. The idea is that if you focus on doing certain tasks more safely, you will take a safer approach in all your actions. It's a safety-first corporate culture."

In the realm of cybersecurity, this safety-first mindset could be very helpful, especially when it comes to suspicious emails. A financial services firm, notes Madnick, conducted a test to see how many employees clicked on phishing emails. Even when the email clearly stated that it was a phishing email and opening it would cause harm, at least one executive clicked the link, "just to see what would happen."

He says, "There is a different mindset when it comes to cybersecurity at companies that needs to be changed. We're trying to understand what works and what doesn't when it comes to changing the corporate culture around cybersecurity."

CROWDSOURCING SECURITY

A different mindset is also needed when it comes to detecting and defending against threats. Too many companies are focused on the latest attack, preparing for it to happen again instead of thinking about what is to come, explains Madnick.

"We need better ways to optimize the workforce to ensure employees' skills can match the threats that are forthcoming," he says, noting that some strategies are common sense, but are nonetheless resisted by managers.

Bug bounty programs are a good example. These originated at software companies and use crowdsourcing to find bugs for rewards. Madnick says even an organization like the U.S. Pentagon benefited from a bug bounty program. After spending $5 million for a consulting firm to identify bugs—and discovering only 10 flaws in three years—the Pentagon invited 1,400 white hats—ethical computer hackers—to do the same thing. Within six months, they found more than 120 bugs at a cost of $150,000.

"Organizations need to consider using these types of programs because we're anticipating a shortfall of 2 million cybersecurity specialists in the next five years," says Madnick. "We need to be creative in how we leverage the cybersecurity workforce. A bug bounty program is one way to do that. Our research attempts to understand how companies can most effectively address their workforce needs."

AN INTERDISCIPLINARY APPROACH

Throughout all the projects at $(IC)^3$, Madnick is taking a collaborative approach by working with faculty across MIT's campus and with academic and industry partners. He is looking at conventional information systems, as well as the cyber-physical infrastructure and Internet of Things—the computer-controlled facilities, such as electric power, manufactured goods, financial services, telecommunications, healthcare, autonomous vehicles, etc., that form the infrastructure of a safe and secure world. His team seeks to produce metrics and models that organizations can use to measure all facets of cybersecurity and to make the best possible decisions about allocating resources to protect themselves.

"Together, we can identify and develop the strategies, models, and processes that will improve cybersecurity and protect our critical infrastructure," he says. ● ● ●