Interview:
"At Cybersecurity Summit, Warnings For Biz, And All"
Poets & Quants

Stuart Madnick

Working Paper CISL# 2016-18

October 2016

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

At Cybersecurity Summit, Warnings For Biz, And All

BY: MARC ETHIER ON OCTOBER 03, 2016 | 0 COMMENTS (HTTP://POETSANDQUANTS.COM/2016/10/03/CYBERSECURITY-SUMMIT-WARNINGS-BIZ/#DISQUS_THREAD) 286 VIEWS

Stuart Madnick

When long-time MIT Sloan professor Stuart Madnick talks to his MBA students about cybersecurity, he doesn't frame it as a national security issue — though it certainly is that. He frames it as a management issue.

The average cyberattack on a business has been going on for 270 days before it's discovered, says Madnick, the John Norris Maguire professor of information technologies. He cites the 2014 hack of personal details from as many as 1 billion Yahoo accounts to show that in most cases, cyber crime catches business leaders flat-footed.

"When people in the industry talk about cyberattacks, they usually talk about three key phases: the penetration, the detection, and the recovery," Madnick tells *Poets&Quants*. "By and large we do a poor job at prevention, we do a terrible job

at discovery, and we're doing a godawful job at recovery. And when someone shoves the microphone in front of the CEO of Yahoo and says, 'What are you going to do about this, what are you going to say about this? Has she developed an action plan six months ago already?' — the answer is probably not. Almost always they are caught flat-footed, and almost always the initial responses are embarrassing."

Madnick's message will get a broader airing Wednesday (Oct. 5) when he serves as a panelist at the **Cambridge Cyber Summit (http://www.cnbc.com/2016/09/06/the-cambridge-cyber-summit-presented-by-the-aspen-institute-cnbc-and-mit-to-be-held-on-october-5-on-mit-campus.html)**, a collaboration between CNBC, **the Aspen Institute (https://www.aspeninstitute.org/about/)**, and various departments of MIT in the Kresge Auditorium on the school's campus. CNBC will cover the event live.

'MOST PEOPLE HAVE NO IDEA OF THE RISK'

To his students, Madnick, director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, offers a somewhat grim outlook of the fight to thwart cyber criminals. He doesn't plan to pull any punches for the expected audience of 300 to 400 middle to upper managers at Wednesday's summit, either.

For one thing, he says, for every widely read story about Yahoo's security breach or the theft of $81 million from the Bank of Bangladesh, which happened in February, many other potentially more dangerous events were barely noticed: a Turkish pipeline that was attacked in 2008, or the German steel mill that sustained massive physical damage in late 2014. Around the holidays in 2015, two Ukrainian power companies were infiltrated, and power was cut to 80,000. "There is a huge disconnect that most people have no idea of the increasing amount of risk that organizations are facing and that individuals are facing," Madnick says.

"I have a number of viewpoints on the issue and one of the more controversial ones is that the worst is yet to come," he says. "That's partly because of the amount of automation in many forms: autonomous vehicles, increasingly automated factories, especially with the various renewable energies, and so on. We're becoming increasingly dependent on automation and computerization to run more and more of our world. The number of attack surfaces is going to increase at least tenfold, if not fifty-fold, in the next five years."

CRIMINALS, BAD ACTORS & MISDIRECTION

It won't only be big, splashy attacks that cause corporate or industrial damage in the tens of millions, Madnick says. Smaller, individual attacks — he cites a recent case in which a computerized refrigerator was used as a botnet to send out pornographic spam — will become more common. Then there's what's called ransomware. Imagine getting a text message in the morning that your coffee maker is being held hostage, Madnick says, and you won't get your morning cup of Joe "unless you deposit $10 into this account."

There are thousands of other examples of ransomware going on this year, Madnick says.

Don't (necessarily) blame it all on the Russians, he adds. "The Russians, the Chinese, the North Koreans — there are a lot of countries, including the United States, that have invested a lot in what are called cyber weaponry, by which I mean various techniques and methods by which they can break into people's systems — refrigerators and coffee makers, whatever the case may be. But to attribute all of it to the Russians is probably an overstatement," he says, adding that "from our research, our view is that in cyber crime, a criminal network is probably much more active in most of these matters."

Moreover, **while the FBI seems convinced (http://www.bloomberg.com/politics/articles/2016-09-02/putin-says-dnc-hack-was-a-public-good-but-russia-didn-t-do-it)** that the highly publicized hack this summer of the Democratic National Committee was the work of Russian agents provocateur, Madnick is not so sure. Why, he asks, wouldn't someone who knows what he's doing leave evidence that a hack was the work of someone else? "This is an issue we call attribution," he says. "If you're really good at it, you try hard to misdirect."

MESSAGE TO MANAGEMENT: DON'T LEAVE THE KEY UNDER THE MAT

Such sophisticated threats "require a multi-pronged response," Madnick wrote in **a Sept. 24 story for CNBC (http://www.cnbc.com/2016/09/24/the-real-and-growing-threat-of-cyber-crime-to-corporations-.html)**. "And while each organization will fashion its own customized response, we believe that all companies, institutions and government agencies should think holistically e2e, end-to-end.

"It is up to senior business leaders to take the lead in protecting their organizations; and in the dark and complex world of cyber crime, that can only be accomplished by working together with government, industry, and academia."

In his class this fall, Managing Web 3.0, Madnick and his MBA students discuss managing the whole new world of Internet-controlled everything, especially the allocation of resources to different activities of cybersecurity. Five lectures are dedicated to the subject, he says. In January he'll teach a short course on cybersecurity ethics.

At heart, he says, cybersecurity is a management issue. "If you look at various studies that have been done about cyberattacks, you'll find that between 50% and 80% of all attacks are aided or abetted by insiders — usually unintentionally. I can put a stronger lock on my door, but if I keep leaving the key under the mat, I haven't made my office more secure. So exactly what policies, procedures, and methods are you putting in place?"

DON'T MISS THE TOUGHEST CHALLENGES MBAs FACE IN BUSINESS SCHOOL (http://poetsandquants.com/2016/07/04/hardest-parts-business-school/) and FROM BUSINESS ANALYTICS TO REAL ESTATE, AN EXPLOSION IN SPECIALIZED DEGREES (http://poetsandquants.com/2015/12/04/rise-b-school-specialized-masters-program/2/)

TAGGED: ASPEN INSTITUTE (HTTP://POETSANDQUANTS.COM/TAG/ASPEN-INSTITUTE/), BUSINESS SCHOOLS (HTTP://POETSANDQUANTS.COM/TAG/BUSINESS-SCHOOLS/), CNBC (HTTP://POETSANDQUANTS.COM/TAG/CNBC/), CYBER CRIME (HTTP://POETSANDQUANTS.COM/TAG/CYBER-CRIME/), CYBERSECURITY (HTTP://POETSANDQUANTS.COM/TAG/CYBERSECURITY/), MIT SLOAN (HTTP://POETSANDQUANTS.COM/TAG/MIT-SLOAN/), STUART MADNICK (HTTP://POETSANDQUANTS.COM/TAG/STUART-MADNICK/), SUMMIT (HTTP://POETSANDQUANTS.COM/TAG/SUMMIT/)

YOU MIGHT ALSO ENJOY