MITSloan
MANAGEMENT

INTERDISCIPLINARY
CONSORTIUM
for IMPROVING
CRITICAL
INFRASTRUCTURE
CYBERSECURITY

(IC)³

Interview: "Security of IoT-enabled devices remains low priority for developers" Tech Target

Stuart Madnick

Working Paper CISL# 2016-16

April 2016

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

Conference Notebook

Security of IoT-enabled devices remains low priority for developers

1

by
Linda Tucci
Executive Editor

Published: 30 Apr 2016

MIT Sloan cybersecurity expert Stuart Madnick talks about clear and present dangers in an IoT-enabled world.

THIS ARTICLE COVERS
Security Management

RELATED TOPICS
Compliance
Data privacy
Risk management
Legal issues
Asset management

LOOKING FOR SOMETHING ELSE?
- Stuart Madnick: Dark Web hackers trump good guys in sharing information
- Balancing user experience and mobile data security
- Cybersecurity experts: 'Brittle' security systems need overhaul

TECHNOLOGIES
Cyberattack IoT Security risk management

Editor's Note: This is part 2 of a SearchCIO interview with Stuart Madnick, the John Norris Maguire Professor of Information Technologies at the MIT Sloan School and director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)^3. In part 1 he explains why dark Web hackers continue to have the upper hand in the cyber war against enterprises. Here he talks about how marketplace pressures, the newness of the technology and human error make IoT-enabled infrastructure vulnerable to attack.

You are moderating a session at the upcoming MIT Sloan CIO Symposium on mitigating

cyber risks associated with Internet-connected devices. Talk about the ways in which IoT complicates the threat landscape.

Stuart Madnick: Various estimates are that within a few years, there will be over 100 billion Internet-connected devices, IoTs. It's one thing to go and try to lock 1,000 doors, imagine trying to lock 1 million doors or 100 billion doors. So the number of attack surfaces is rapidly increasing.

There's another problem that will hurt us in several different ways. A year ago, I was on sabbatical and I spent part of my time at the University of Nice working with some people in the automotive telemetrics group. They were trying to do things that have never been done before, like autonomous driving and so on.

Stuart Madnick

What I learned is that doing those things is extremely difficult. They are under tremendous constraints regarding the cost of the components, regarding the amount of energy they can consume, regarding the size of space they can take up. There's a whole long list of extremely challenging engineering problems they are wrestling with. If you have the top list of N priorities, cybersecurity, at least a year ago, was N+1. There were just so many things they had to deal with that they had to say, "We'll focus on these now and worry about these others later."

So part of the issue is the IoTs are so new, and there are so many challenges for the good guys in terms of trying to get them to work at all, that thinking really hard about cybersecurity is extremely difficult to factor into that.

So the IoT security component is not built in from the beginning and more an afterthought at this point?

Madnick: It is slowly changing. But as of a year ago, that was the case, and I think that's still probably the case of the majority of IoT work.

Our concern though is that a lot of the effort is ... not adequately being directed because of a fantasy that if only I could come up with a better cryptographic code all the problems will go away.

Stuart Madnick
director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)3

One of my colleagues works as a consultant. He worked for a company that was coming out with some IoT device. They were coming out with this device and they had just come to the realization that it was subject to certain types of cybersecurity attacks they hadn't considered before.

They realized that the computing power they had in their design would not allow them to make the software changes that would make the product more secure. They were faced with a decision. Do we release the product as planned this month or do a redesign which could take six to eight months and possibly lose the market?

I'll let you speculate what decision they made. Hint: the product came out.

Security cameras as access devices

People like you are thinking hard about attacks on IoT-enabled infrastructure. Can you give me an example?

Madnick: One example is the Turkish pipeline explosion, which once again Turkey denies was a cyber-attack and claims it was just a malfunction. But according to other analysts, it was a cyber-attack. But what's interesting about it was the cyber-attack apparently originated through the security cameras that had recently been added to the pipeline.

So the security camera, rather than being a security device actually was the access device. Ironically, amongst the things the intruders did besides cause the pipeline to explode was allegedly they erased the security tapes as well and they cut down the alarm system. I was told that the only reason why the Turkish central control people knew a fire had broken out, was when someone saw the fire blazing in the sky four miles away.

I mention this incident because one of the hot items being sold nowadays are these Internet security cameras you can put outside your house or inside your house or as part of your baby monitoring and so on. I was told that 50% of all those devices still have the default pass code on them.

Is the U.S. government investing enough in protecting critical infrastructure?

Madnick: Well, on the positive side, you may have seen that President Obama just announced ... an increase to $19 billion on cyber. So at least there's more and more money being spent.

Our concern though is that a lot of the effort is -- maybe misdirected is going to be too strong a term -- is not adequately being directed because of a fantasy that if only I could come up with a better cryptographic code all the problems will go away. And so they're not addressing hardly any of the organizational, managerial, cultural problems.

Human element in protecting IoT-enabled ecosystem

The organizational and cultural issues linked to cybersecurity is a big research focus at the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity or (IC)3, where you serve as director.

Madnick: What we're focused on very much is the human element. Various reports have indicated that 50-70% of all cyber-attacks are aided or abetted by insiders. Now, I can take that broadly. If you, as a homeowner, don't change that security code on your security camera when you buy it, I would argue you were a contributor to the cyber break-in. The actions or inactions of humans are by far the major issue. Putting a stronger lock on your door doesn't help if you're giving keys away or leaving a key under the mat.

So that's why in our research, we're looking much more at the managerial and organizational aspects which don't get much attention at all.

Like what?

Madnick: Let me answer that by giving a couple of examples of things we're working on along that line. I'm at the Sloan School at MIT, and the adjacent building to us has been going through renovations for the last year or two. And for a long time there was scaffolding on the outside. If you had been at MIT four or five months back, you would have seen on the scaffolding a big 10 foot-by-10 foot poster mounted. It had a picture of a worker, and in his hands he's holding a photograph of his family. And above him is a sign that reads, "I know why safety is important." The implication being is "My family relies upon me. If I'm not safe, I'll be injured and that will harm my family."

If you go into a factory, most likely you will see over the door a sign that says something like "570 days since last industrial accident." When was the last time you went to a computer room and saw a sign over the door "50 milliseconds since last successful cyber-attack?"

That's a long introduction to saying what we're doing is trying to create what we call a cyber-safety discipline.

I read that your work on cyber safety is based on an MIT model called STAMP (Systems Theoretic Accident Modeling and Processes) -- an approach to minimize and mitigate industrial accidents.

Madnick: Yes, STAMP is obviously one of the main sources. STAMP is something MIT had been working on for approximately 20 years. It was used to analyze the Challenger space shuttle explosion.

How does STAMP apply to cyber safety?

Madnick: There's several aspects of it. When you look at most mini cyber break-ins, or any kind of accident in general, you'll often hear the end result being human error. "She left her password written on a note on her desk" or whatever it might be. And the issue stops there.

We believe, in most cases, people don't deliberately want to create either industrial accidents or cyber events. Usually it is the incentive systems and organizational structure and organizational culture that surrounds them that really has a lot to do with how people operate. That's the overarching thing of what STAMP started off doing and we're doing in cyber safety.

Linda Tucci asks:

What is your enterprise doing to ensure the security of IoT-enabled devices?

0 Responses

Join the Discussion

Next Steps

More on security risks of IoT-enabled devices

Who will tackle IoT security?

Essential guide: 7 IoT security risks

Legal issues related to the IoT-enabled enterprise