Interview:
"Dark Web: hackers trump good guys in sharing information"
Tech Target

Stuart Madnick

Working Paper CISL# 2016-15

April 2016

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

SearchCIO.com

Stuart Madnick: Dark Web hackers trump good guys in sharing information

By null

In the ongoing and increasingly [vicious cyberattacks](#) against the world's best-known brands, the bad guys have it easier. So says Stuart Madnick, the John Norris Maguire Professor of Information Technologies at the MIT Sloan School and a speaker at the upcoming [MIT Sloan CIO Symposium](#). Madnick, who currently serves as the director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, [(IC)](#)^3, explains how dark Web hackers use technology and information to their advantage.

How are businesses doing in the fight against cyberattacks? They have to be getting better.

[Stuart Madnick](#): It is true, people often observe that we are getting better. The thing that we often don't take note of is the bad guys are getting better even faster. That's the challenge. So I guess indeed things are getting better, but unfortunately the worst is getting worster, if there's such a word. (Actually, I'm from Worcester, Massachusetts, so I suppose that's appropriate.)

What is allowing the bad guys to get better and preventing the good guys from keeping up?

Madnick: One of the things is that badness is getting commoditized, and that is the thing that used to be extremely exotic, requiring a PhD in computer science to break into systems and so on. Now it is available for sale on the [dark Web](#) for $14.95. The tools and techniques that the hackers have available are increasingly available, and becoming more powerful at an increasing rate.

Stuart Madnick

Another thing I have observed in our research is the good guys actually do a bad job of sharing information. Now, when places like Target get attacked, they are required by law -- because personal data is disclosed -- to have to report it. And so it tends to get out into the press. But if, for example, a [German steel mill is attacked](#) and partially melts down, there's no obligation to report that publicly. In fact, even though Bloomberg reported it, they denied it ever happened.

The good guys keep it quiet for lots of reasons. They don't want the bad reputation. They don't want to encourage what I call copycat intruders. On the other hand, the bad guys have fantastic information-sharing arrangements on the dark Web, so that's part of the reason why the bad guys are getting badder faster than good guys are getting gooder.

So the dark Web hackers have the upper hand. You'd think there would be a [mechanism for easily sharing information](#) without risking damage to a company's reputation or setting up copycat attacks.

Madnick: I don't want to say there aren't attempts. In fact, if anything, there is a plethora of organizations trying to do the sharing. Unfortunately, they are extremely fragmented. What I'm about to say I'm not sure if I'm allowed to repeat publicly, but apparently the big oil companies actually do get together and share information, but only the bigger ones. They won't share it with the next level down because they just want to keep it in a closed community.

It's the same reason why the FBI doesn't like sharing with the CIA because they assume the CIA has moles in it and they'll leak everything out. The CIA doesn't want to share with the FBI because they're afraid the FBI has moles in it and will let their stuff leak out.

Not that there aren't people trying to do it, but they're constantly getting tied up in these knots: "If I reveal this, it will get exposed to the public. Will bad things happen to me?"

It's a bit ironic, if you think about it. The bad guys actually like reputation. "I'm the one who broke into XYZ Bank and stole the billion dollars." That's an ego thing to some extent. So there are lots of reasons that those on what I'll call the dark Web actually seek, if you will, publicity.

Can you give an example of an information-sharing network in the dark Web ecosystem?

I don't know the name of it, but there actually is a website where the people of the dark Web rank the most hated companies in the world. And you see a correlation: As your rating goes up to the top, the number of cyber-attacks goes up, because a fair number of people don't attack for personal gain or [for a nation-state](#). They just happen to like to show their anger about things. As your rank goes up, you find the number of these people in their spare time saying, for example, "Monsanto is an evil company. I'm going to teach them a lesson. I'm going to bring them down."

I was told that some companies actually hire other people to go in the dark Web to vote them down lower as one way to reduce the number of attacks they see.

Editor's note: *In [part 2](#) of SearchCIO's interview with Stuart Madnick, the cyber security expert previews his session at the upcoming MIT Sloan CIO Symposium, "[Mitigating Cyber Risks in the Growing World of Internet-connected Devices](#)."*

30 Apr 2016