Interview:
"Sloan research: CISOs enter the boardroom"
Tech Target

Stuart Madnick

Working Paper CISL# 2016-14

April 2016

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

SearchCIO.com

MIT Sloan research: CISOs enter the boardroom

By Linda Tucci

Stuart Madnick

One of the questions Stuart Madnick will ask of a panel of CIOs at the upcoming MIT Sloan CIO Symposium is who should the company's CISO report to. Madnick, a professor of information technologies at MIT Sloan, is interested in the organizational and managerial factors that give rise to cyber break-ins, including the role CISOs and CIOs play in security.

MIT Sloan research shows that while CISO reporting structures "are all over the place," with security officers reporting to CIOs, CFOs, chief risk officers and directly to the CEO, one trend seems firmly fixed: more board interest in cybersecurity.

"I'll give you a quote I had from a CISO recently. He said that in the previous 10 years, he had met with his company's board of directors once. In the past year, he's had three briefings with the board," Madnick said. "We're actually seeing in a few cases where the CISO reports directly to the board."

MIT Sloan research: TJX Cos.

The fact that boards are focusing on cybersecurity roles and relationships is a positive sign. Madnick, who is also the director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)[3], believes that companies — and federal government security programs– pay too little attention to the organizational structures and incentives that make companies vulnerable to cyber attacks.

"I'll give you just one quick example," Madnick said. "We did a detailed analysis of the TJX break-in, which was at that time the largest credit card break-in in 2005." His group compared its analysis with analysis coming out of the FTC and other investigations and "found all kind of issues in the organization that had not been covered."

Such as?

"There was an email from the CIO of TJX to his staff. And the email said something to the effect that, 'We are currently not PCI [Payment Card Industry Data Security Standard] compliant. It will take quite a bit of effort and cost to do so. This is now November. We're entering into our Christmas rush. This has been a tough year financially. Don't you all think it would be fine if we deferred becoming PCI-

compliant until next year?"' Madnick recounted, referring to an email sent by then-CIO Paul Butka in 2005.

"This is called an email where the answer is embedded in the question. It may shock you to realize that almost no one on the staff saw any problem with doing that," Madnick said.

30 Apr 2016

All Rights Reserved, Copyright 2007 - 2016, TechTarget | Read our Privacy Statement