Report warns of hacking risk to U.S. electric grid, oil pipelines, and other critical infrastructure

March 29 2017, by Adam Conner-Simons

An MIT report urges the Trump administration to develop a coherent cybersecurity plan that coordinates efforts across departments, encourages investment, and removes parts of key infrastructure, like the electric grid, from the internet. Credit: Shuttershock

In a world where hackers can sabotage power plants and impact elections, there has never been a more crucial time to examine cybersecurity for critical infrastructure, most of which is privately owned.

According to MIT experts, over the last 25 years presidents from both parties have paid lip service to the topic while doing little about it, leading to a series of short-term fixes they liken to a losing game of "Whac-a-Mole." This scattershot approach, they say, endangers national security.

In a new report based on a year of workshops with leaders from industry and government, the MIT team has made a series of recommendations for the Trump administration to develop a coherent cybersecurity plan that coordinates efforts across departments, encourages investment, and removes parts of key infrastructure like the electric grid from the internet.

Coming on the heels of a leak of the new administration's proposed executive order on cybersecurity, the report also recommends changes in tax law and regulations to incentivize private companies to improve the security of their critical infrastructure. While the administration is focused on federal systems, the MIT team aimed to address what's left out of that effort: privately-owned critical infrastructure.

"The nation will require a coordinated, multi-year effort to address deep strategic weaknesses in the architecture of critical systems, in how those systems are operated, and in the devices that connect to them," the authors write. "But we must begin now. Our goal is action, both immediate and long-term."

Entitled "Making America Safer: Toward a More Secure Network Environment for Critical Sectors," the 50-page report outlines seven

strategic challenges that would greatly reduce the risks from cyber attacks in the sectors of electricity, finance, communications and oil/natural gas. The workshops included representatives from major companies from each sector, and focused on recommendations related to immediate incentives, long-term research and streamlined regulation.

The report was published by MIT's Internet Policy Research Initiative (IPRI) at the Computer Science and Artificial Intelligence Laboratory (CSAIL), in conjunction with MIT's Center for International Studies (CIS). Principal author Joel Brenner was formerly inspector general of the National Security Agency and head of U.S. counterintelligence in the Office of the Director of National Intelligence. Other contributors include Hal Abelson, David Clark, Shirley Hung, Kenneth Oye, Richard Samuels, John Tirman and Daniel Weitzner.

To determine what a better security environment would look like, the researchers convened a series of workshops aimed at going beyond the day-to-day tactical challenges to look at deep cyber vulnerabilities.

The workshops highlighted the difficulty of quantifying the level of risk across different sectors and the return on investment for specific cybersecurity measures. In light of facility-directed attacks like the Stuxnet virus and the sabotage of a Saudi oil refinery, attendees expressed deep concern about the security of infrastructure like the electric grid, which depends on public networks.

"Connecting [these operations] to the Internet has brought undoubted efficiencies to electricity generators and other industries, but it has also created dangerous vulnerabilities in the systems that keep the lights on and power the economy," the MIT team writes, echoing concerns that were raised in a Department of Energy report published in January.

Brenner and his colleagues also contend that the technical challenges

could actually be easier to address than the legal and economic ones. To align incentives with better security, they call for tax and regulatory policy that rewards cybersecurity investment, including investment to convert to a more secure Domain Name System (DNS) for websites.

The authors are optimistic that President Trump's team will be receptive to the report, given the shared desire to fix America's vulnerable infrastructure. "Our recommendations complement their attention to federal systems," Brenner says. "Our current cyber insecurity is a national disgrace, and we must defend the networks that the safety of our nation depends on."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology