

VOICES OF THE GOVERNING INSTITUTE

The Gravity of the Cyber Threats We Face

We need to be better prepared for the attacks that are happening every day. Above all, that means we need to collaborate.

BY RICK SNYDER | DECEMBER 7, 2015

Rick Snyder

Governor of Michigan

Connect with Rick  



It is very likely that the next devastating attack on the United States won't be like any other we've experienced. It will come through the computers on our desks at work, the laptops we set on the kitchen table, or even the mobile phones and tablets we scroll through while standing in line at the coffee shop. And most of the time, people won't even realize they're being attacked.

I'm convinced that cyberattacks are quickly becoming the greatest threat to the security of our communities, our states and our nation. That's why I recently hosted the North American International Cyber Summit and delivered the keynote address at similar gathering at the University of Michigan.

A catastrophic cyberattack might be difficult for people to visualize. But let's start with issues we deal with almost every day, such as our very identities. I asked people attending the university cybersecurity conference if they'd ever been a victim of identity theft. About 80 percent of the hands went into the air -- mine included.

A few years ago, I began receiving phone calls and letters from debt collectors who demanded that I pay bills generated in my name even though I had no idea what they were talking about. I then learned there was a cellphone contract for a phone I never owned and an apartment in my name in Washington, D.C., both acquired with my stolen identity. And I'm sure many of the people reading this have seen a mysterious charge on a credit card bill for a store they've never been to in a town hundreds of miles away.

These are disturbing and stressful problems. But imagine the trouble we would face if these cyberattackers were not merely seeking to steal merchandise or get some easy cash. What happens if cyberattackers are intent on bringing down government functions, our economy and our very way of life?

The truth is that we are already under siege. Take my state of Michigan: Every day, there are 2.5 million cyberattacks on our state-government computers. More alarming, that's a million more attacks each day than a year ago.

That number is only going to grow. Michigan is an inviting target as a large state of 10 million people that serves as the global hub for automotive design and manufacturing along with three major research universities. That's why we've made cybersecurity a priority. We've developed a statewide Cyber Disruption Response Plan, a comprehensive blueprint for organizing a rapid response in the event of a significant cyber disturbance. The plan includes strategies for information sharing, criminal investigation, response and recovery from a significant disruption to our state's critical infrastructure.

But this effort requires collaboration. We've partnered with cyber experts from the military, government and the private sector to establish a model for how government and business can come together for the greater good of our respective customers. Better, it can be used as a template for any city, township, village or county, or for businesses both large and small.

Our Michigan National Guard plays a growing leadership role, with five installations of the Michigan Cyber Range to conduct first-class training exercises. And our National Guard was selected to work with Ohio and Indiana to form one of the Army National Guard's first cyber protection teams. Our Michigan State Police also have created a Cyber Crime Command Center, a public-private partnership for the prevention and investigation of cybercrime incidents throughout the state.

And we've tapped expertise from a growing number of dedicated volunteers. The Cyber Civilian Corps' mission is to work with government, the private sector and educational institutions to provide rapid response in the event of a declared state of emergency due to a cyberattack. We've nearly tripled the number of volunteers in the past year. In addition to 10 regional teams, we are adding three specialty teams in the fields of automotive, finance and education.

I'm proud of what we've done in our state. But traditional state boundaries could mean very little in the event of a widespread, aggressive cyberattack. While cybersecurity doesn't often make it onto the front pages of the newspapers and rarely gets attention on cable news, it is potentially the single greatest threat we face. Yet it's hardly mentioned in presidential politics or candidate platforms.

We need to recognize the gravity of cyber threats, and I encourage you to reach out not only within your local and state governments but also to the federal government to get informed about what is being done to protect our vital institutions. We all, as a nation, need to be better prepared. To accomplish that, we need to work together.

More information about cybersecurity and a link to the Michigan Cyber Disruption Response Plan can be found at www.michigan.gov/cybersecurity.

[Rick Snyder](#) | Contributor

rick.snyder@michigan.gov | [@OneToughNerd](#)

1 comment

ABOUT VOICES

VOICES is curated by the Governing Institute, which seeks out practitioners and observers whose perspective and insight add to the public conversation about state and local government. For more information or to submit an article to be considered for publication, please [contact editor John Martin](#).

LATEST HEADLINES

[Philadelphia Mayor Considers Banning Donald Trump](#) 1 hour ago

[Why State Legislatures Are Still Pretty White](#) 1 hour ago

[FBI to Start Tracking More Than Just Fatal Police Shootings](#) 15 minutes ago

[Redistricting Case Appears to Divide U.S. Supreme Court](#) 5 minutes ago

[Outgoing Kentucky Governor Pardons 200 Prisoners](#) 4 minutes ago

[Tax Cuts Fail to Garner GOP Support in Connecticut](#) 14 minutes ago

[MORE NEWS](#)

**GET GOVERNING NEWS
DELIVERED TO YOUR INBOX**

Email Address

