Cyberattack—the silent nightmare

December 24 2012, by Melissa Maynard

In Michigan's worst techno-horror story, the state's major utilities get hacked in the wintertime. Power in the state shuts down, and nobody can figure out how to regain control of the systems needed to turn it back on. Millions of people are left in the dark and in the cold.

Cybersecurity, the business of protecting the Web-based systems that now run much of the world, has emerged as an important function of state governments. States have to worry not only about the safety of their own networks and the data that is housed there, but also about the security of privately owned systems that control critical infrastructure within their borders.

It's the kind of low-profile problem for which it's often difficult to rally public support until it's too late. But Michigan has enlisted the help of everyone from the major utility companies to the state police to launch what it sees as a multi-pronged pre-emptive strike. Gov. Rick Snyder used to be the president of Gateway computers; he is leading cybersecurity efforts for the National Governors Association. That has brought key players to the table from both the public and private sectors.

"You will fail if you're an island," says Dan Lohrmann, Michigan's chief security officer. "You've got to be working with other states, you've got to be working with the feds, you've got to be working with the private sector, you've got to be looking at new tools, because the bad guys, you might stop them today, you might stop them tomorrow, but you might not stop them the next day. They're always getting better. They're looking at your castle and they're always trying to get across your moat."

In fact, it's no longer precisely accurate to call Michigan's anti-hacking efforts pre-emptive. The state is already experiencing 185,000 cyberattacks on its state-owned infrastructure every day, says John Nixon, director of the state's department of technology, management and budget. The vast majority of those attacks are thwarted, and some are multiple attempts from the same source. "Now what are we housing as a state?" Nixon asks rhetorically. "We're housing tax records, health records, pretty much everything there is about people and their lives. Cybersecurity is the number one issue for us."

Information technology managers in Michigan can't help noticing scary events that are taking place around the country almost all the time. The scariest took place in South Carolina this October, when a hacking at the department of revenue compromised social security numbers, bank account numbers and other data for 3.8 million residents. It is widely believed to be the largest computer breach any state government has faced. Mandiant, the security firm hired by the state to investigate the breach, told South Carolina legislators this month that the techniques used by the hackers were "not that sophisticated." The incident was likely the result of a state employee clicking on an attachment in a bogus "phishing" email.

Over the course of the next year, all 50,000 Michigan employees will be completing a series of interactive, video game-like training modules aimed at preventing them from making equally costly mistakes. In one session, employees have to find missing laptops in an airport terminal - an exercise aimed at reminding them not to leave technology behind on airport shuttles and in bathrooms, as many travelers do.

Michigan is the only state to have completely merged cybersecurity with physical security, though such practices are fairly common in the private sector. The same state unit is responsible for providing the security guards who oversee access to state buildings and the cybersecurity

professionals who monitor state networks for suspicious activity.

"The merger of the physical and cyber world is happening at all levels," says Lohrmann, who oversees both functions and blogs about cybersecurity for Government Technology magazine. "Any kind of crime that you may want to commit in the real world, you can now use cyber to gain information to support that crime, to enhance that crime, to multiply that crime in the cyber world."

In a similar way, the state has focused on sharing information between cybersecurity professionals at private companies and government cybersecurity personnel. The state will soon be physically centralizing these efforts in a Cyber Command Center housed with the state police.

"It's just like a serial killer in the old days," says Inspector Dean Kapp, assistant division commander of the Michigan State Police, Emergency Management and Homeland Security Division. "They'll kill one in California, Michigan and New York, and they were all separate until somebody figured it out. Well, we have systems in place now to link those."

Still, gathering evidence and finding hackers remains a huge challenge. Kapp jokes that for law enforcement personnel, even bank robberies are easier to tackle than cybercrimes. "Cybercrime is on such a tidal wave roll right now that it's going to overtake everything else," he says. "If I can sit back in my living room and commit a crime and not have to scale a catwalk or break into somebody's house to steal something, why wouldn't I do it that way?"

Federal cybersecurity legislation has repeatedly stalled in Congress because of sensitivities around asking private companies to share information that they say could put them - and their stock prices - at risk. But Michigan companies are willingly collaborating with the state

on a range of cybersecurity initiatives aimed at bolstering protections and developing coordinated response plans for when breaches happen.

One hope is that as cybersecurity becomes increasingly important in the global marketplace, state efforts will pay off not just in preventing disasters but in economic development opportunities. Michigan economic strategists are particularly excited about the potential of the Michigan Cyber Range, a public-private partnership launched in November that allows for hands-on training and testing of real-world cybersecurity scenarios.

"Aside from giving the good guys and fake bad guys a safe place to shoot at each other, it's giving companies a safe place to test their products," says Gary LaRoy, vice president and chief information officer of the Michigan Economic Development Corporation. "That could be a big economic development advantage for us."

The range, the first of its kind anywhere in the country, will eventually be accessible both remotely through a secure network and on-site at various higher education and military facilities around the state.

"You have to be able to outthink your adversary as a team, so (the Range) goes one step further," says Don Welch, president and CEO of the Merit Network, which hosts and operates the Cyber Range. "This is really where the focus of the range is, to get people practicing outthinking someone. The other part is to get them to do it as a team - because you don't want to work on your teamwork when your normal modes of communication are under attack."

Merit Network is a nonprofit governed by Michigan's public universities, and key partners include other academic institutions, the federal department of homeland security, the Michigan Economic Development Corporation and private-sector companies. All will be able to tailor the

range to their own needs by building off the curriculum developed by Merit. Sharing and building on lessons learned in the Range is a core requirement for all who use it.

"I can use it to help grow the talent on my team," says Jim Beechey, cybersecurity manager at Consumers Energy, a major power company that is a key state partner. "We can use the range for exercises and simulations and testing. We can do things in a safe environment rather than exposing some of our operational systems to risks."

Beechey also hopes the Range and accompanying academic program development will help him identify and recruit talented cybersecurity professionals, an ongoing challenge. The Range may eventually be used to screen job applicants by testing how they would react in the real world.

Five Michigan higher educational institutions currently are recognized as Centers of Academic Excellence by the National Security Administration for their cybersecurity programs, and the Cyber Range is aimed at further boosting those numbers by making it easier for universities and community colleges to launch programs making use of infrastructure already in place. "The exploits and the vulnerabilities change fairly quickly, and there's a lot of work for instructors and professors to keep those up to date and keep it viable," Welch says.

LaRoy, of the Michigan Economic Development Corporation, says that while companies aren't routinely making location decisions based on cybersecurity considerations now, that will be likely to change if a major incident disrupts peoples' lives and explodes onto the national news, something many in the field consider inevitable.

His pitch to companies considering where to locate or expand includes assurances that Michigan's infrastructure is more secure because of what

the state has done to protect it through the Cyber Range and other initiatives.

"It's not enough to have their data in their data center safe if they don't have power to that data center because somebody hit our power grid," he says. "They're at risk. If we can truly make ours more immune or better defended against cyber threats then it's a safer place to do business."