TEMPTING TARGET

STATE COMPUTER SYSTEMS FACE NEARLY CONSTANT CYBER ATTACKS.

BY SUZANNE WEISS

On the morning of April 30, 2009, state officials in Virginia were greeted with a nasty surprise: A ransom demand, posted on the website of the Department of Health Professions, for the return of more than 8 million patient records that included addresses, Social Security numbers and prescription drug information.

Hackers had broken into the website, bundled the data into an encrypted file and then deleted the original records. The ransom note demanded $10 million in exchange for the encrypted file and the password to unlock it.

State officials were tight-lipped about the incident, except to say that they wouldn't pay the ransom, the thieves hadn't managed to steal backup files and the FBI had been called in to investigate.

The breach was a particularly shocking reminder of the vulnerability of state governments to cyber attacks ranging from website defacement and interruption of online services to theft, extortion and terrorism.

"States hold the most comprehensive collection of personal information about individuals, spanning from birth to death," notes a recent report by the National Association of State Chief Information Officers. "They know where you work, what you earn, where you live, the taxes you pay, your date of birth, your Social Security number, your medical conditions."

And the collection, storage, sharing and use of people's personal information is certain to increase as states rely more and more on the Internet to better serve constituents and improve efficiency, the report said.

MILLIONS OF ATTACKS

The magnitude, frequency and sophistication of attacks on state government information systems are mind-boggling.

"There are millions of automated network probes every day, looking for cracks in the dam," says Doug Robinson, executive director of the chief information officers group.

In Michigan, for example, more than 75 percent of the 120 million e-mail

Suzanne Weiss is a freelance writer in Denver and a frequent contributor to State Legislatures.

"There are millions of automated network probes every day, looking for cracks in the dam."

DOUG ROBINSON, EXECUTIVE DIRECTOR OF NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS

messages the state received last year were either spam or viruses, said Dan Lohrmann, the state's chief technology officer.

"On an average day, we see probably 20,000 or 30,000 different entities scanning our networks, trying to break in," Lohrmann says. "These attacks are happening on a daily basis, and we have to constantly be ready for them."

Many computer hackers are motivated solely by a desire to make mischief, acquire restricted information or cripple certain sites. But many others are fulltime professionals, motivated by profit and increasingly connected to organized crime or government-bankrolled hacking rings in countries such as Russia, China, Brazil and Estonia. Profit-motivated attacks typically don't involve demands for ransom, as in the Virginia incident. Instead, blocks of stolen data are sold on the Internet.

Traditionally, states have focused on strengthening the perimeters of their networks to keep cyber criminals out with anti-virus programs, firewalls, spam filtering and detection/prevention systems.

But unintentional or malicious acts from inside state government are potentially just as dangerous as external breaches. The theft or accidental loss of an unencrypted laptop or hard drive, for instance, can result in costs that run into millions of dollars—not to mention the erosion of public trust, Robinson points out.

Perhaps the most significant internal threat is employee inattentiveness, lack of training or failure to comply with basic security procedures—such as installing software updates or regularly changing passwords.

"Think of state information networks as a house with a whole lot of windows, all of which you need to be sure are locked," Robinson says. "All it takes is one unlocked window. Once a burglar is in the house, he has access to everything."

At the same time, information is more and more mobile, contained on laptops, flash drives, smartphones and various other hand-held devices, all of which increase the risk of security breaches.

STATES TAKING ACTION

In the face of these challenges, states have made notable progress on several fronts.

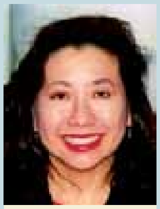
During the past several years, all but a handful of states have established the position of chief information security officer, a person responsible for identifying and reducing risks, responding to breaches and establishing appropriate standards and controls. States also have adopted, to varying extents, security-focused strategic plans, frameworks and timetables.

In addition, all 50 states and the District of Columbia are participating in the Multi-State Information Sharing and Analysis Center, a 7-year-old cybersecurity collaborative focused on prevention, protection, response and recovery.

A number of states have been recognized by the information officers

BOLSTERING DIGITAL SECURITY

Thousands of cyber attacks hit state information resources every day, interrupting or halting business operations and causing revenue and property loss. To fend off the growing number of attacks, a couple of states have formed committees aimed at bolstering cyber security defenses as well as attracting the growing cyber security industry to their states.

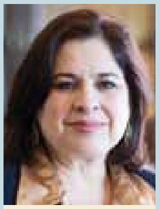


DELEGATE
SUSAN LEE
MARYLAND

Maryland Delegate Susan Lee decided it was time to create a commission to review state and federal cyber security laws, policies and standards and come up with a comprehensive plan of defense for the state.

"Cyber attacks have had the potential to wreck havoc on, paralyze and devastate the operations of our government, economy, infrastructures, transit systems, public utilities and first responders," she says.

The legislature agreed with her and this year passed her bill, which directs the commission to develop recommendations that include ways to attract private investment. Along with state lawmakers, state and federal officials, and representatives from businesses and higher education will serve on the commission.



SENATOR
LETICIA VAN DE PUTTE
TEXAS

As the need grows to protect electronic systems, so grows the cyber security industry. The federal government's demand for cyber security is estimated to grow to a price tag of $11.7 billion by 2014, and that figure is likely to be surpassed by the private sector.

"The state that invests in and makes cyber security one of its top priorities," Lee says, "will become the national epicenter of cyber security innovation and excellence."

Maryland already is a hotbed of this kind of technology. It's home to the National Security Agency, the Intelligence Advanced Research Projects Activity, the National Institute of Standards and Technology, and the Defense Information Systems Agency headquarters. In addition, it's soon to be home of the U.S. Cyber Command headquarters and other activities of the Department of Defense.

Texas, too, has entered the cyber security battle. Senator Leticia Van de Putte sponsored legislation to create an advisory committee to increase cyber security awareness and improve the security of critical Texas infrastructure.

She believes it is essential for all levels of business, government and education to work together to combating the growing and sophisticated threat of cyber attacks.

Her bill created the Cyber Security Education and Economic Development Council, made up of government officials and business and higher education representatives. They will recommend improvements to cyber security technology and identify ways to foster the growth of this rising industry in Texas.

"The cyber security industry presents a new field of economic growth that will be essential in the future," says Van de Putte. "Researching new opportunities will help us tackle the most serious economic and national security challenges we face. This council will help Texas become a leader in cyber security technology and set an example for the rest of the nation."

—Jo Anne Bourquard, NCSL

WEALTH OF INFORMATION

So why are state governments such a tempting target for cyber attacks? It's because agencies hold a wide variety of personal information about individuals, including:

◆ Social Security numbers
◆ Credit card information
◆ Tax records
◆ Birth, marriage and death certificates
◆ Medical records
◆ Vehicle registration and driver's license records
◆ Entitlement program data—Medicaid, food stamps, unemployment insurance
◆ Voting records
◆ Criminal justice information
◆ Unemployment insurance records
◆ Occupational and professional licensing information

> *"We're all struggling with how to stay one step ahead of the bad guys."*
>
> MICHAEL ADAMS, DIRECTOR OF INFORMATION SERVICES FOR THE COLORADO LEGISLATURE.

association for innovative approaches to cybersecurity. For example:

◆ Michigan has developed a national model for addressing risks associated with consolidation, shared services and Internet-based "cloud-computing" environments.

◆ West Virginia is setting up a layered defense system that includes firewalls, filters and other tactical operational controls, access and authorization controls, encryption, vulnerability management, employee awareness training, and enforcement.

◆ Pennsylvania has reduced costs associated with data breaches, remediation and risk mitigation by building security controls into applications as they are being developed, rather than trying to apply such controls after the fact.

But the results of the association's most recent survey of its members underscore the need for greater attention to cybersecurity on the part of governors, legislators and other state officials.

Nearly 90 percent of chief information security officers listed "lack of resources" as the major barrier to information security, yet a large majority reported that spending on cybersecurity had been reduced in 2009 and again in 2010.

"Ideally, 5 percent of a state's IT budget should be focused on security, but the average, unfortunately, is more like 1 percent," Robinson says. "The fact is that [chief information officers'] authority and resources aren't commensurate with their responsibility to keep bad things from happening."

Given the significant shortcomings of states' cybersecurity efforts, Robinson says, "it's remarkable that we haven't had a digital Pearl Harbor—a massive disruption of systems."

South Dakota chief information officer Otto Doll echoes Robinson's concerns about the lack of priority given to protecting state government information systems. "It's like when we don't put the traffic light at an intersection until somebody gets run over," he says. "The problem with cybersecurity is that it's not just one person—the whole town can be run over in just one of these attacks."

HIGH-PROFILE TARGET

Although executive branch agencies are the primary target for hackers, data security is a big challenge for legislative staff, too, says Michael Adams, director of information services for the Colorado legislature.

"A lot of legislators come in thinking that working in the Capitol will be like their own workplace, in their private lives," Adams says. "So it's a matter of trying to get them to understand that it's different—much more high profile."

As in most states, Colorado's legislative IT staff is responsible for the systems for bill production and document management, public access to legislative information, and support for economists, auditors, researchers, the House and Senate chief clerks and others involved in legislative business.

Although legislative data aren't as much of a target for invaders and intruders, the stakes are still high, he says. "If our Web page gets hacked, it might not do as much harm, but it's more likely to get press attention—and it has the potential to be politically damaging to legislators."

Over the past several years, security has become a critical element of the job for legislative staffers like Adams.

"We're all struggling with how to stay one step ahead of the bad guys," he says. "I spend a lot of time keeping my eye on the horizon."