Ready or Not
The Challenging Cybersecurity Realities for State Governments

A Route Fifty Special Report
Government Executive Media Group
May 2017
The bad news? Year over year, state governments will undoubtedly see cyberattacks and breaches escalate.

The good news? Many of these cyber threats are not only known but understood.

Take, for example, the 2018 midterm elections. Experts say there will likely be a successful attempt by a foreign actor to hack the vote, but there are also bonafide ways to preserve the integrity of the process—if only states will implement them.

No government is immune to hacktivism by a dedicated attacker, but there are frameworks in place to mitigate damage and boost response. Training is key at the state level, as is establishing a hiring pipeline of talented IT personnel.

The following Route Fifty special report identifies the most pressing threats to government cybersecurity and outlines a path to preparedness.

Fair warning: These challenges are fast approaching, if not already upon us, and what improvements states implement within the next year will undoubtedly make the difference.
The Cybersecurity Risks U.S. Election Systems Face Heading Into the 2018 Elections

The international cyberattack that infected computers with malware in at least 150 countries on May 12, including 48 National Health Service trusts in the United Kingdom, exploited an old vulnerability first used by the National Security Agency. NHS was particularly hard hit because most of its hospitals use Windows XP, the same software most U.S. voting systems run on.

A total of 42 states still rely on voting systems more than a decade old—close to the end of their projected lifespan.

Among counties with such systems, a disproportionate number fail to back them up with a paper ballot and mandated, risk-limiting audits of the final vote.

“Come 2020, we’re going to be sitting ducks,” said J. Alex Halderman, a computer science professor at the University of Michigan, at a congressional briefing on May 15.

Time can make all the difference for a kidnapping victim or a family in the path of a tornado.

By Dave Nyczepir
News Editor
The decision of which of the 52 available voting technologies to use generally falls to counties, and not a single one tested by security experts—direct-recording electronic or optical scan—has withstood the spread of vote-stealing malware, which interferes with the records as they’re created to change the result.

Simply diversifying and decentralizing voting tech and disconnecting machines from the internet isn’t enough to stop even a middling hacker, Halderman said.

In a close race, diversity is a weakness because attackers will likely have several key jurisdictions to choose from, using pre-election polling as a guide, when affecting the outcome. And even if voting machines are disconnected from the internet, the election management system that programmed the ballot design onto their memory cards prior to the vote wasn’t—meaning the hack could have occurred ahead of time.

Memory cards still offer a faster, cheaper tally, but thoroughly auditing a statistically significant sample of backup paper records is the only way to ensure electronic results.

Vote-stealing malware can be coded to alter only 10 percent of the vote so as to stay below the radar. That said, there is no proof any previous U.S. election has been compromised this way.

“Last election wasn’t hacked,” said retired Army Lt. Col. Tony Shaffer, a senior fellow at the London Center for Policy Research. “Elements of different cyber issues were presented.”

Who would want to hack a U.S. election? China for starters, said James Scott, senior fellow at the Institute for Critical Infrastructure Technology. Also, Iranians actively sought a toolkit on the “dark web,” during the last presidential election, to hack Pennsylvania’s central tabulator, Scott said.

The biggest threat remains Russia, which revealed in 1989, when the Soviet archives were briefly opened, that its disinformation officers outnumbered military personnel.

“The Russians are good at cyber,” said James Woolsey, former CIA director and chair of the Foundation for Defense of Democracies. “They have always been good mathematicians.”

Cyber helps Russia magnify the effects of their disinformation campaign, and they gladly share their knowledge with other enemies of the U.S., such as when they gave North Korea the details on an extremely fast torpedo. Many of the U.S.’s own cyber techniques from the 1990s and 2000s have been subverted and expanded, Shaffer said.

Current tactics to co-opt the vote involve spear phishing email and social links that, when clicked, initiate the drive-by download of compiled tools: remote-access Trojan viruses;
virus droppers; keyloggers; screen grabbers; camera and mic capture tools; network mappers; code injectors; innovative malware like Russia’s HAMMERTOSS, which uses Twitter to relay commands and extract data; tabulation manipulators that weigh the vote to appear legitimate; and geo-targeting only activated in swing states or regions.

Should an attacker steal network credentials, they can lay the groundwork for future attacks by securing remote access and then selling, on the dark web, that backdoor “access as a service.” By the 2018 midterm elections, access to state tabulators will be purchasable, Scott said.

Local elections are naturally the most vulnerable, with state and local employees notorious for checking their social media accounts from the office. All it takes is clicking the wrong bit.ly link.

“Twitter will continue to be the main distribution vector, and the most successful vector, for all of this stuff,” Scott said.

Waiting until the next presidential to address vulnerabilities that have been public for years is a mistake, Woolsey said.

But currently all state bills seeking resilient systems that can withstand cyberattacks, paper ballots and mandatory audits have been sponsored and cosponsored solely by Democrats, said Lawrence Norden, deputy director of the Brennan Center for Justice at the New York University School of Law.

Part of the problem is state and county officials are defensive of their power to run elections as they see fit. Yet those elections are “chronically underfunded,” Norden said, which provides an opening for the federal government to offer innovation grants or some sort of match to replace machines and invest in a thorough audit.

Most states want new voting machines, but 80 percent of the states looking informed the Brennan Center they were unsure of where the money would come from, according to “Americas Voting Machines at Risk.”

Shaffer said he was surprised the Freedom Caucus, who he works with, hadn’t come to the table on the issue. Partisanship being at an all-time high, Woolsey suggested seeking financial assistance from wealthy benefactors or foundations might be a more feasible funding approach.

“It absolutely should be a bipartisan effort because we’re...talking about systems that are essential to the functioning of our democracy,” Halderman said.

Constituents want security by design in new tech and improved cyber hygiene, Scott said. The Cyber Shield Act, which ICIT supports, is a start.

Cyber paranoia surrounding the 2016 election continues to be felt, as the reality of an impending threat mounts. Even the perception of an election hack is dangerous at this point.

“This is a chess game. We have to play this as a chess game,” Shaffer said. “A well-funded, well-versed adversary, simply by thinking things through, could undermine the process without using any new technology.”
All states are vulnerable to cyberattacks if even one ignores National Institute of Standards and Technology cybersecurity protocols, a framework only 20 of 35 states the National Governors Association surveyed have implemented.

The other 15 states are in the process of aligning with NIST. But five governors have made no progress toward receiving regular cyber threat briefings, two haven’t initiated risk assessments, five haven’t implemented a three- to five-year strategic plan based off those assessments, and three lack a disruption response plan.

While Virginia Gov. Terry McAuliffe, who chairs the NGA’s executive board, didn’t call any governors out by name during his Meet the Threat session at the association’s winter meeting in the nation’s capital in February, he did privately issue a color-coded card to all present indicating their state’s cyber risk level.

“If you have red and yellow, you really need to do something about it,” McAuliffe, a Democrat, said.

State governments have more data than the feds, he said, and Virginia alone saw 86 million cyberattacks in 2016, he said. A recent attack attempted to access the governor’s email from a state account.

A talented hacker can use an unprotected health care provider in a smaller state as a backdoor into Virginia’s systems, and the same is true of infrastructure, power grids, water utilities and police dispatch centers. If an energy grid goes down, “that impacts our cost, our response to the state” and threatens not only government systems but those of the private sector, said Arkansas Gov.
Asa Hutchinson, who chairs NGA’s Homeland Security and Public Safety Committee.

A former Homeland Security undersecretary under President George W. Bush, Hutchison said a denial-of-service attack was successful in shutting down his state’s website within the last two weeks, though no data was lost or personally identifiable information stolen.

Before being elected governor, Kate Brown served as Oregon’s secretary of state and saw its business registry and campaign finance websites hacked in 2014. Since then, she’s worked to increase Oregon’s security posture by auditing structural gaps and moving forward with a Center for Cyber Excellence to identify best practices and facilitate information sharing between agencies and other jurisdictions.

“I think we can do this in Oregon by bringing companies together like Intel and Hewlett-Packard and bringing universities together,” Brown said.

“The Governor Was Responsible.”

Last year low-level, Kosovar hacker Ardit Ferizi was sentenced to 20 years in U.S. prison, after being extradited from Malaysia. What appeared initially to be an unsophisticated breach of a U.S. retail company’s server, yielding around 1,350 names and addresses and a $500 ransom request, took a dark turn when a federal investigation found Ferizi was in contact with British-Pakistani hacktivist-turned-terrorist Junaid Hussain.

Ferizi had combed through the names he’d obtained and placed those of U.S. soldiers and government workers on an Islamic State kill list.

Hussain was killed in a U.S. Central Command drone strike on Raqqah, Syria, in 2015. A seemingly harmless cyberattack had, in fact, been part of a larger terrorist plot spanning five countries.

“The person responsible if something goes wrong will be you,” said John Carlin, a partner with the international law firm Morrison & Foerster. “If it’s your state and your system, they’re going to say, ‘The governor was responsible.’”

“There is no internet system that is safe from a dedicated nation-state or criminal group, if they’re determined to get in right now,” he added.

“Bad actors” are exfiltrating trade secrets from state universities and companies for the
benefit of other countries, and the close-mouthed approach to dealing with Cold War espionage is being traded in for public information sharing to disrupt future cyberattacks—mainly through the U.S. Department of Justice’s National Security Cyber Specialist network.

Carlin said many foreign entities have the desire, but only four are considered capable of causing a full-scale cyber incident in the U.S.: China, Iran, North Korea and, most recently, Russia. In fact, these countries prefer to avoid open military confrontation in favor of fighting online.

In Beijing, military officers work eight-hour days attempting to steal secrets from U.S. companies, and Iranian hackers could’ve caused flooding in New York in 2013 had the dam sluice gate they took control of not been down for maintenance.

North Korea’s 2014 Sony hack—thought to be triggered by “The Interview” film’s comedic portrayal of the assassination of Kim Jong Un—was an interesting case, Carlin said, because until the country was named responsible 28 days later, press coverage focused entirely on what the victim did wrong.

As a result, then-President Obama issued an executive order outlining consequences in the event of future cyberattacks. That’s what made sanctions possible when U.S. intelligence agencies confirmed Russia stole Democratic National Committee emails in 2016.

Still, the stolen emails are what people remember.

“These are vulnerable spots that will be there somewhere in your state system,” Carlin said.

‘Fatherly’ Advice

Following the advent of the internet, there was a several-decades-long rush to move everything from analog to digital and get it connected to the web without any thought as to the risks. Everything from pacemakers to drones to automobiles is hackable, so the latest Internet of Things trend requires “security by design” on the front end.

For their part, states must give serious thought to what hackers might do to cause them the most harm and how quickly their backup systems can be up and running because, unlike CEOs, governors must protect not just information technology but also operational technology.

Following a state cyber incident, incomplete information will be coming at a governor fast, so decisionmaking preparedness is key, said Mary Galligan, a Deloitte managing director.

Throughout government, administrators should also practice access management.

“You should only have access to what you should have access to,” Galligan said.

That’s even true of one of the “fathers of the internet”, Vinton Cerf, who isn’t granted unlimited access as chief internet evangelist at Google.

Breaches occur because software inevitably has bugs, Cerf said, and those mistakes get exploited even when developers attempt to patch known problems. “Moral suasion” shouldn’t be
underestimated by governors looking to deter cyberattacks, but in lieu of that, encouraging two-factor identification within government is also important—despite the inconvenience.

Fingerprint biometrics are being introduced as a form of identification, but governments shouldn’t rely solely on them because you can’t change your fingerprints. If a hacker gets a digital summary of an employee’s fingerprints and injects them into the system, they become them, Cerf said. Two fingerprints and a token that generates a one-time cryptovariable are preferable.

The https protocol is nice because it generates an encryption key, Cerf said, but that doesn’t necessarily securely authenticate you.

Cerf also warned against phishing emails: “If you get an email and it says, ‘Click here, this is really fun,’ don’t.”

More broadly, government agreements with outside jurisdictions are important for when governors discover a cyber attack was perpetrated outside their jurisdiction. As the “laboratories of democracy,” states and localities will be where replicable cybersecurity best practices emerge, Cerf said.

While large companies often have an in-house cyber expert for an executive or on their board, states should help educate small businesses, that lack the capacity, on proper cyber hygiene. That alone accounts for 85 percent of the issues on the internet, Galligan said, and along with patch management provides a good resiliency base.

“In addition to having a well-educated cyber workforce, it occurs to me that we ought to have a cyber fire department,” Cerf said.

By that, he meant a team of “response and attribution” experts capable of alerting companies when they’re at risk of or experiencing a breach and identifying the source. Safeguards would have to be implemented to prevent one company from sicking the department on a rival to disrupt their business, Cerf added, because “it’s easy in this space to pretend to be somebody else.”

Another tool states sorely lack is the ability to measure how well they’ve implemented the NIST framework. Internally, Google tests its disaster response once a week by running live operations off its backup systems—a metric state governments should work toward implementing, Cerf said.

Governors hoping to hear military information sharing is capable of preventing a chain of cyberattacks against states likely left dismayed. While it’s still valuable to know of a cyber attack on a neighboring state, what won’t be known or shared quickly is how the breach occurred and what information hackers sought.

“I agree that it’s not fast enough or on scale,” Carlin said.
When an Oklahoma state legislator proposed legislation making it illegal to hide one’s face with a hoodie in 2015, hacktivists took notice and responded. Oklahoma’s state government received threats via YouTube and hackers acquired botnets, pointed them at the state’s public-facing IT infrastructure and bombarded it with traffic.

The goal: To focus citizens’ attention on the hackers’ political views, and since then they’ve brought the similar types of disruptions on county and city governments protesting incidents of police-involved violence.

“They’re not going after the machines that you care the most about because, from a hacktivist perspective, they’re not going after you,” said former FBI special cyber agent Andre McGregor. “They’re trying to get their message out.”

So want to prove how bad a government is or how unsecure citizen data can be, said Andre McGregor, Tanium internal security director and a former FBI special cyber agent in New York City and Washington, D.C., handling intrusions from China, Russia and Iran. But hacking is hacking regardless of the motivation.

If a system has 250,000 to 350,000 machines and one is missing, McGregor said, that’s the one the hacktivist will use. Whether it’s in your finance enterprise resource planning system or another computer in another system doesn’t matter, so long as it’s accessible.

“They’re not going after the machines that you care the most about because, from a hacktivist perspective, they’re not going after you,” McGregor said. “They’re trying to get their message out.”

---

By Dave Nyczepir
News Editor
Oklahoma had a communications trailer sitting in a garage—the camera, heating and cooling, and voice systems for which were managed by a vendor—infiltrated by a self-proclaimed journalist streaming the hack on Twitter.

The hacker wanted to prove the government was vulnerable and was never caught.

“States aren’t there to mitigate, financially, every risk like this that comes about,” Reese said.

At the local level, Tulsa and Tulsa County were attacked separately but at least had the foresight to ask the state for help after detecting the impending threat.

The “hoodie incident” left Oklahoma with a playbook. It had the local governments scan for vulnerabilities, lock them up and shut down unnecessary systems to shrink the target.

All parties were quickly educated on the situation, with a focus on the most appetizing targets like police, citizen bank accounts and government emails.

Oklahoma is currently unifying its systems for added security, but as Kentucky has found, a consolidated data center doesn’t help with federated applications, which remain vulnerable.

The rising tide of hacktivism necessitates not just the onboarding of skilled security personnel but the establishment of a hiring pipeline to the private sector thereafter, McGregor said. The NSA hires the best cryptographers not because it pays better but because the on-the-job challenges are unparalleled, and that’s a selling point for those seeking experience before making a career move—which should be accepted and embraced.

“I was stolen,” McGregor said. “I had a really uncomfortable conversation with FBI Director Comey when I was leaving.”
Dave Nyczepir is a News Editor for Government Executive’s Route Fifty. He previously covered breaking news and local government for The Desert Sun newspaper in Southern California’s Coachella Valley and worked for Campaigns & Elections magazine. He is a graduate of the College of William and Mary and holds a master’s in journalism from the Merrill College of Journalism at the University of Maryland.