Security Will Get Harder — and Even More Important

Multiplying Risks: Protecting More of Everything

It's big and it's costly. Information security is now a top priority for states and counties for the simple reason that cybercrime is booming. Thanks to the growing sophistication of hackers, thieves and terrorists who operate similarly to tech-savvy companies, state and local governments are under digital siege. The already difficult task of protecting digital information and assets is ever-more difficult in a world where almost everyone and everything is connected.

U.S. data breaches reached a record high in 2014 — a 27 percent increase from 2013 — with the public sector third on the list of targeted industries, according to the Identity Theft Resource Center.[62] That's a huge jump in activity from just five years ago, when the subject of cybersecurity was low on the priority list for state CIOs.[63] Since then, the growing intensity and sophistication of attacks has turned cybersecurity into the No.1 IT concern for states and counties, according to surveys by the Center for Digital Government.[64]

Those attacks translate into huge costs. The financial impact of cybercrime on the global economy in 2014 was an estimated $445 billion, according to the Center for Strategic and International Studies.[65] More specifically, data breaches cost U.S. companies an average of $195 for each compromised record, with the cost to fix breaches rising at an annual rate of 15 percent.[66]

One way government agencies are responding to threats is to adopt cybersecurity frameworks based on national standards and guidelines. They are also developing security awareness training for employees and IT contractors. Government initiatives such as the county-led CySAFE (Cyber Security Assessment for Everyone) have helped agencies understand how prepared they are to ward off threats by identifying weak points for hackers and other intruders. Cyber analytics is another fast-growing strategy for evaluating weaknesses in the multiple layers of security now commonplace in any cybersecurity program.

Meanwhile, funding for cybersecurity has increased slightly at the state level, but most experts say it's not enough.[67] More funding is needed for the next generation of cybersecurity tools to augment traditional defenses such as firewalls, anti-virus and anti-malware software programs. Government needs to deploy a broader set of threat detection tools, along with real-time monitoring and risk management.

Obtaining more funding is never easy. Part of the problem is convincing elected officials cybersecurity deserves more attention at a time when budgets are still tight. One way is to recognize cybercrime is not an IT problem, but a government problem. Cybersecurity needs to be approached as an enterprise risk that must be addressed with support from the chief executive on down.

Moving forward, governments need the right combination of people, technology and policy to confront a new age of cybersecurity driven by an exponential environment. New security tools have proven effective in defending government computing systems, but they have to be backed by the right strategy that combines leadership, well-trained people and funding.

The platform of tomorrow demands new thinking around cybersecurity. Information protection becomes more complex — and even more crucial — at the intersection of widespread IoT-powered connectivity, massive data storage and sharing, and unprecedented growth in sophisticated cyberthreats.

A Prime Target for Security Threats

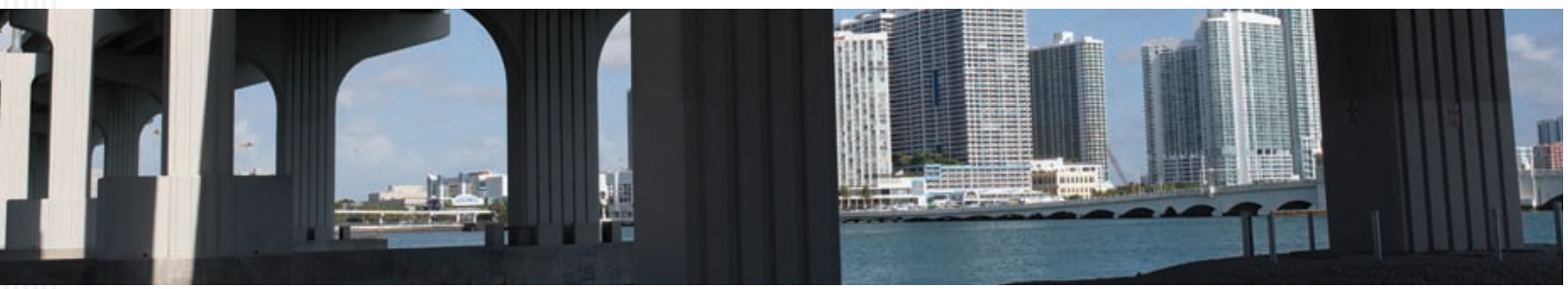
Security has remained the top priority for state CIOs for the past three years, according to NASCIO.[68]

The percentage of states with a cybersecurity strategic plan, compared to 61% in 2014.[69]

The increase in the number of U.S. data breaches in 2014 compared to 2013.[70]

50,000
security incidents

The number of public sector security incidents in 2014, making government the industry most affected by cyberattacks.[71]

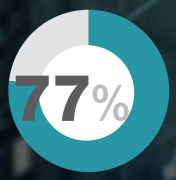


States Are Upping their Game

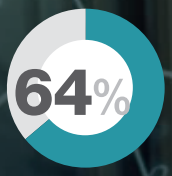
Colorado's cyber plan, Secure Colorado, has reduced malware infestations by more than 75 percent since 2013, the equivalent of $830,000 in cost avoidance and savings. With security tools across all 17 executive branch agencies, the state can monitor and report each agency's level of risk on a monthly basis.[72]

The Michigan Cyber Initiative 2015 builds on the state's existing security strategy, launched in 2011. The proactive, risk management-based initiative leverages the NIST Cybersecurity Framework and has driven the creation of a state cyber disruption response plan, cyber command center and emergency operations center.[73]

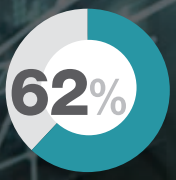
Top 4 Cybersecurity Challenges for State CIOs



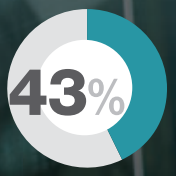
Increasing sophistication of threats



Lack of adequate funding

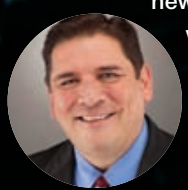


Lack of available cybersecurity talent



Emerging technologies[74]

What Can Governments Do?



Understand the environment. Our ultra-connected world is continuously changing, which means new, unprecedented cyberthreats will continue. According to **Tony Encinias**, the vice president of public sector strategy at ViON, "Five or six years ago, cybersecurity threats were not as prevalent as they are today. Now, we have a multitude of bad actors who are trying to take data for monetary purposes. Others are trying to make a statement through intrusions on websites. This is happening on a daily basis — actors all over the globe are trying to access government systems. Meanwhile, government has limited resources to fight this increasingly difficult battle."[75]

Turn to technology. According to **Robert Myles**, Symantec's national practice manager for state and local government, governments believe firewalls, intrusion detection, and anti-virus and anti-malware tools will protect them from potential threats, but they only tell you what's happening on the inside. "Internal security tools are great, but you have to apply outside detection tools to understand the full picture," he said.[76] Two technologies can help:

Predictive analytics. "It's hard to be really proactive when it comes to cybersecurity. That's where analytics comes into play," says Encinias. "It helps organizations look at data and be proactive; it helps them make management decisions about where to focus limited resources."

Automated risk management. "Organizations need real-time monitoring and risk management to combat around-the-clock threats," says Myles. "The only way to do that is through automated risk management. That's the next big piece that organizations have to tackle: automated, responsive security management strategies developed on an ongoing basis, with firewalls continuously monitored. If there's a spike or abnormality, it can raise a red flag and you can respond right away."

Follow state and national standards. NIST released a cybersecurity framework for public agencies in 2014. The NIST framework — deployed by a variety of agencies — provides a description of what's needed for a comprehensive cybersecurity program, ultimately helping to reduce cyber risk.[77]

80% OF STATES HAVE ADOPTED A CYBERSECURITY FRAMEWORK BASED ON NATIONAL STANDARDS AND GUIDELINES.[78]

Take security out of the IT department. "States have to stop thinking of security as an IT project," says Myles. "If cybersecurity is viewed as just a portion of the IT budget, it's going to continue to fail. Cyberthreats are a government problem, not an IT problem. Yes, it rides on an IT infrastructure and there are IT tool sets, but without understanding who the data owners are; without understanding what the assets are; without the training and all the things in play, you can't fully defend the state of your organizations."