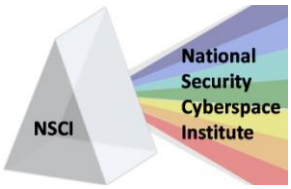

Cybersecurity at the State and Municipality Levels

Where Do We Stand?

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
February 25, 2011

One year ago, the National Governors' Association (NGA) released a statement on the importance of cyberspace security in protecting the ability of federal, state, and local governments to perform their vital functions. Recognizing the critical functions performed at the state level, the governors wrote: "Due to the breadth and scope of the state role in entitlement services, facilitating travel and commerce, regulatory oversight, licensing and citizen services, states gather, process, store and share extensive amounts of personal information. From cradle to grave, the states are the nexus of identity information for individuals. This makes the states prime targets for external and internal cyber threats."[1] Indeed, it is at the state and local levels that the preponderance of programs – including many funded by the federal government – are actually administered. This is an often-overlooked fact. The federal government provides funding for the states to execute any number of social service programs.

The concerns expressed by the governors are not unfounded. The use of web technologies to facilitate government services continues to rise. Consider the convenience and time savings arising from use of the internet to renew drivers' licenses and vehicle registrations, voting in elections, payment of utility bills, and registering for locally-provided recreation activities, just to name a few. Further, consider emergency services. Regardless of the magnitude of a natural or man-made disaster, the first responders – firemen, police, ambulance services, National Guardsmen – are provided by city, county, and state governments. Their ability to communicate and execute key command and control responsibilities are often solely dependent on cyber-based technologies. When the late congressman Tip O'Neill, former Speaker of the House, coined the phrase, "All politics is local," he was hardly exaggerating.

Last November, hackers believed to be from Russia managed to steal $200,000 in electronic fund transfers intended for delivery to schools and cities falling under the jurisdiction of Gregg County, Texas. The electronic transactions within the county had been a routine occurrence, with transfers taking place between a single bank used for tax monies collected and several other banks around the county with accounts used to dispense funds to operate the various cities and schools. Investigators in the case believe a county computer was infected with the Zeus Trojan disseminated via e-mail. Zeus, described in a Symantec-sponsored paper as "King of the Bots," [2] has been responsible for numerous thefts within the banking industry. It accomplishes this by stealing login credentials and diverting funds away from their intended accounts. Investigators in the Gregg County case have been able to trace the source of the attack to a Moscow-based website. In addition to the loss of $200,000, Gregg county has since taken a step backward by reverting to its former system of paper checks and deposit slips to transfer funds – a process that will certainly be less efficient and more costly.[3]

In July 2010, Poplar Bluff, Missouri, experienced a spike – from 500 to 45,000 per week – in attempts by hackers to disrupt municipal utility services. Unfortunately, this was not a one-week event; the higher numbers have continued, prompting the city to call in the FBI to investigate.[4]

There's also the case of the Northern California city of Morgan Hill, approximately 70 miles south of San Francisco. As reported by consultant Bruce Perens, attackers climbed down manholes within the city last April, cutting eight fiber cables and causing a massive disruption to life in Morgan Hill and parts of three surrounding counties. Residents in the region lost emergency 911 service, cellular telephone capability, land-line telephone, DSL internet and private networks, central station fire and burglar alarms, ATMs, credit card terminals, and monitoring of critical utilities. [5]

---

1 Policy Position from the National Governors' Association, Special Committee on Homeland Security and Public Safety, 22 February 2010
2 "Zeus: King of the Bots," by Nicolas Falliere and Eric Chien, Symantec, 2009; available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf
3 "Cyber thieves hit Gregg County for $200K," Longview, Texas News-Journal, 7 December 2010
4 "Poplar Bluff city internet service under cyber attack;" report by KFVS television, the CBS affiliate in Cape Girardeau, Missouri, 22 November 2010, available at http://www.kfvs12.com/Global/story.asp?S=13552821
5 "A Cyber-Attack on an American City" by Bruce Perens, 23 July 2010, available at http://perens.com/works/articles/MorganHill/

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
February 25, 2011

The state of Colorado hired a security firm last year to determine cybersecurity vulnerabilities. The results: Hackers "...easily gained access to thousands of documents containing Coloradans' sensitive personal information," according to a report on the covert penetration test and a statewide audit conducted from February through November 2010. The audit found that "12 of 20 agencies had failed to submit plans outlining their computer system security measures to the state's Office of Cyber Security as required by law. And while there had been 43 cyber security incidents reported to the office since 2006, auditors believed the number was higher, noting that some known incidents had not been reported."[6] The report went on to say:

> *"We conducted a penetration test of public agencies and found significant vulnerabilities throughout state government that allowed the assessment team to compromise thousands of records containing individuals' confidential information, such as social security numbers, birth dates, and income levels," auditors reported. "The assessment team also compromised several state networks and systems and identified hundreds of vulnerabilities in state systems."*
>
> *"Based on the results of our penetration test, prior information technology audits, and our review of the implementation of the Colorado Cyber Security Program during this audit, we concluded that the Office of Cyber Security has failed to successfully implement the Colorado Cyber Security Program, as specified by statute."*[7]

Further, there is certainly no shortage around the country of cases in which political "hacktivists" intrude on websites or transmit e-mail messages while impersonating government officials. These activities result in erroneous – and perhaps dangerous – information being distributed to constituents and have the potential to destroy both the careers and private lives of targeted politicians. The resulting publicity and unpleasantness are likely to discourage other qualified people from ever entering public service.

Finally, consider one of the more odious acts of cyber terrorism inflicted on a local community – this time a city within the Australian state of Queensland. A computer expert who had been rejected for a job with local government decided to seek revenge by hacking into the city's wastewater management system. During a two-month period, he repeatedly directed computers to spill raw sewage – hundreds of thousands of gallons of it – into local rivers, parks, and public areas before authorities were able to identify him as the perpetrator.[8]

These are only a few examples of the growing threats and vulnerabilities facing governments below the federal level. As the NGA policy statement on cybersecurity said:

> *"These threats are growing in numbers, as well as severity. Cyber threats facing state governments may be characterized as:*
>
> - *Constantly evolving due to rapidly emerging technologies and increasing demands on agency services*
> - *Growing ever more sophisticated, target-specific and virulent*
> - *Disruptive and profitable by organized crime and a preferred method for generating income through cybercrime activities*
> - *Escalating internal threats as employees fail to comply with security measures, internal controls are circumvented and data becomes increasingly mobile*

6 "Audit: State at 'high risk' of cyber attack," by Tim Hoover, the Denver Post, 13 December 2010
7 Ibid
8 "How Vulnerable is U.S. Infrastructure to a Major Cyber Attack?" by Glenn Derene, Popular Mechanics, 1 October 2009

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
February 25, 2011

- *Increasing availability demands of users to have constant access to data which increases the need for data loss prevention capabilities and protection"*[9]

Any notion one may have that cyber attacks can result only in mere inconvenience for a few hours or even a few days – described as "weapons of mass annoyance" by some – should have been permanently dispelled by the so-called Aurora experiment[10] and the Stuxnet worm. In both cases, malicious computer inputs caused very expensive equipment to literally destroy itself. In fact, it has been said that the Stuxnet attack on Iranian centrifuges may have set back the country's nuclear weapons program by two years.

So what are the states and localities doing to address their gaps and shortfalls? For starters, they're getting more serious about the problem and attempting to commit more resources. Beginning in the early 2000s, states have been adding a Chief Information Security Officer (CISO), usually reporting directly to the CIO. The National Association of State Information Officers (NASCIO), founded in 1969, has been an outstanding advocate on behalf of the states and has served as an excellent avenue for the states to collaborate and share best practices in cyber security. NASCIO conducts periodic surveys of state CIOs, conducts studies and analyses of current IT issues, and disseminates results and recommendations to the states and general public.

However, the situation from state to state appears to vary greatly. According to Dan Lohrmann, Michigan's Chief Technology Officer, the states can be divided into thirds – one-third that "get it," one-third that "don't get it," and a final third that seem to be somewhere in the middle. In a July 2010 opinion piece, Lohrmann suggests that a number of states are still stuck on security problems prevalent five years ago in spite of a wealth of information and solutions available from a variety of agencies and organizations. Lohrmann writes, "Meanwhile, DHS, the MS-ISAC, NIST, US-CERT, NASCIO and others have a myriad of documented policies, best practices regarding security, free training, case studies on what it takes to be successful, and more. Nevertheless, the implementation of these best practice processes, procedures, tools and expertise continue to lag in many states."[11] Citing a need to "build cybersecurity into the culture of government," Lohrmann offers three recommendations:

1. Using the state Homeland Security Advisors/Coordinators as a model, each Governor should create a CISO with real clout that can work across local/state/federal lines. Most importantly, cybersecurity authority needs to be in a centralized function in the states under a CISO that is recognized by both Governors and the legislative branches.

*2. Each state needs to build **a** comprehensive cybersecurity plan which is modeled after the Federal Cybersecurity Initiative (and currently mandated for all federal agencies.) State modifications will be needed, but federal funding should be made available that cuts across traditional funding silos and addresses enterprise-wide cybersecurity priorities – even helping local governments within states where feasible. This plan should encompass traditional law enforcement issues as well include cyber issues within new state and local fusion centers.*

3. Establish clear command and control for all cybersecurity incidents. Cyber emergency situations should follow the processes and procedures directed in our National Incident Management System (NIMS). A command and control structure must be established which will work to prepare and respond to a variety of different circumstances. This will allow local, state and federal efforts to be coordinated and escalated as appropriate in cross-boundary situations which cover multiple states

9 Policy Position from the National Governors' Association, Special Committee on Homeland Security and Public Safety, 22 February 2010
10 "Sources: Staged cyber attack reveals vulnerability in power grid," by Jeanne Meserve, CNN, available at http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US
11 "Cybersecurity Governance: State CISO Roles - Past, Present and Future," by Dan Lohrmann, 2 July 2010

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
February 25, 2011

and or government jurisdictions. Within states, this function must be centralized – in the same way as emergency management dictates response to pandemic health-related emergencies (such as the H1N1 virus) or other sector emergencies such as nuclear and transportation. [12]

Lohrmann goes on to recommend use of a cyber incident model similar to responses to weather and other emergency management situations conducted at the state level. As he says, these situations may start with a local response, but can often lead to a Governor-declared state of emergency or even a Presidential Declaration of a disaster area. [13]

In an example of like-minded thinking with that of Lohrmann, the city of Hampton, Virginia, plans to establish a lab that would simulate a municipality under cyber attack. According to Bruce Sturk, Hampton's director of Federal Facilities Support, "... municipalities have very robust teams and infrastructure to support emergencies of the physical type such as floods, hurricanes and fires. However, cyber attacks are usually addressed as administrative IT staff functions without the same level of attention, resources, and processes that are associated with physical threats. Risks to the community for cyber attacks are not identified nor incorporated in municipal emergency operations plans." [14]

In December 2010, Texas implemented a requirement that holds vendors accountable for their product feature and function claims, using the non-profit Underwriter Laboratories (UL) to certify hardware and software networking, data center, and security products. Servers, routers, firewalls, intrusion prevention systems and other equipment will be tested under realistic cyber attack scenarios. The requirement will apply to any equipment destined for state government or universities. In addition to Texas, there are six other states considering similar legislation.[15]

The 50 states, along with the District of Columbia, local governments, and U.S. territories, have joined together in standing up the Multi-State Information Sharing and Analysis Center (MS-ISAC), a collaborative organization charged with the task of providing a common mechanism for raising the level of cyber security readiness and response in each of the member jurisdictions. In November 2010, the MS-ISAC officially opened a state-of-the-art cyber security operations center in New York state, providing a 24-hour watch and warning capability. According to a press release in Government Security News, the center conducts "real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach..." In remarks at the opening ceremony, White House cyber coordinator Howard Schmidt commented on the importance of the center, saying, "The cybersecurity of our nation depends on collaboration across all levels of government and the private sector, and the launch of the new MS-ISAC cyber security operations center is a significant step forward towards enhancing the cybersecurity of our state, local, territorial and tribal partners."[16]

These and other similar initiatives around the country aren't cheap, and they come at a time when states and localities are reeling from the impacts of the current economic crisis. According to a 2010 survey jointly sponsored by Deloitte and NASCIO, 79 percent of state CISOs reported either declining or stagnant funding levels for cybersecurity from the previous year. Further, 88 percent reported being underfunded to provide proper cybersecurity for their systems and networks, especially when compared

12 Ibid
13 "Cybersecurity Governance: State CISO Roles - Past, Present and Future," by Dan Lohrmann, 2 July 2010
14 "Hampton gears up to become a center of excellence to fight cyber attacks," by David Macaulay, Newport News, Virginia, Daily Press, 21 February 2010, available at http://www.istockanalyst.com/article/viewiStockNews/articleid/3883448
15 "UL Seal of Approval Launched for Resiliency of Networking, Security Products," by Kelly Jackson Higgins, Darkreading, 9 February 2011, available at http://www.darkreading.com/vulnerability-management/167901026/security/perimeter-security/229209866/index.html
16 "New cyber security operations center officially launched in New York state," Government Security News, 18 November 2010, available at http://www.gsnmagazine.com/article/21860/new_cyber_security_operations_center_officially_la

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
February 25, 2011

to private-sector enterprises.[17] Because government supervisors always say their programs are underfunded, the 88 percent number is not really surprising. However, the fact that 79 percent received no increase in 2010 is cause for concern. Another alarming finding from the survey was this: 47 percent of state CISOs report having between one and five full-time equivalent (FTE) information technology professionals assigned to their staffs. Compare this with the typical similar-sized financial organization in the private sector, which, according to the Deloitte-NASCIO report, has about 100 IT professionals reporting to the CISO.[18]

In an April 2008 "Call for Action," NASCIO urged Congress and the Administration to provide federal grants to the states to strengthen cybersecurity. Included in their justification was this statement: "IT security is not only essential to preserve the states' ability to effectively serve citizens, but is also necessary to protect federal programs (such as Medicaid, TANF and others) administered by the state, preserve the privacy of personal and sensitive information, and to support mission-critical homeland security activities." [19]

The Homeland Security Grant Program (HSGP) contains provisions for the states to apply for federal funding to support cyber-related activities under any of the HGSP's component programs. DHS also serves as the lead federal agency providing funding for the network of state and local fusion centers that share homeland security information between the different levels of government. These centers have recently begun taking on an increased role in cybersecurity-related intelligence and information sharing. Given the current economic climate and the financial situations existing in local and state governments, a boost in current spending from Washington to work on a shared, national, and purely government responsibility might be a wiser use of federal tax dollars than some of the current federally-funded programs and entities we could name.

The following quote from the National Governors' Association statement from last year provides an excellent summary for this topic.

> *"Federal leadership alone will not be sufficient to enhance the protection and resiliency of cyber infrastructure. The federal government has made significant strides in ensuring state and local government inclusion. However, as the federal government works with the private owners and operators of cyber infrastructure, governors urge that the states' role evolves to be equal partners in this process. All levels of government depend on the same infrastructure, but state and local governments may be the first and most directly affected by the cascading effects of an attack or disruption and must be included in national efforts to protect cyberspace."*[20]

We wholeheartedly concur.

To achieve these goals, what specific actions can states and municipalities take? There is a lot of work going on at the federal level regarding cyber legislation, policy, law, defense, and intelligence. But similar to natural disasters such as Hurricane Katrina, a response to incidents within a state belong to the state – unless the state asks for federal help. So while government at the national level works from the "top-down," states and municipalities should work "bottom-up." Here are a few suggestions - perhaps low hanging fruit - on how to help prepare for these contingencies:

---

17 "State Governments at Risk: A call to secure citizen data and inspire public trust," Deloitte-NASCIO, 2010, available at http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.PDF
18 "State Governments at Risk: A call to secure citizen data and inspire public trust," Deloitte-NASCIO, 2010, available at http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.PDF
19 "Strengthening Cyber Security in the States: Providing Directive Grants to Address Critical Needs," NASCIO, April 2008, available at http://www.nascio.org/advocacy/dcFlyIn/callForAction08.pdf
20 Policy Position from the National Governors' Association, Special Committee on Homeland Security and Public Safety, 22 February 2010

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
February 25, 2011

- Work with schools – from middle schools through the college level – to ensure cyber awareness and education is available to all internet users.
- Consider establishing a local lab similar to the initiative being undertaken by Hampton, Virginia. Establish specific goals. Near-term goals could be tied to increased cybersecurity awareness of non-technical Internet users including small businesses and the public at large. Labs could also include " fly-before-you-buy" testing activities such as those being performed in Texas. In the long term, local labs might even play in federal exercises such as DHS's Cyber Storm and/or "Cyber Challenge" events.
- Establish a venue to work through scenarios related to cybersecurity incident prevention and response. Identify processes and establish trust. The first time these people meet should not be when responding to an actual cyber attack. Involve local law enforcement, businesses, academia, and government in everything from tabletop discussions to full-blown exercises.
- Consider, and exercise, use of National Guard cyber expertise as part of the state's cyber incident response team.
- The need to protect information is not solely a government responsibility. Ensure local businesses and the general public are included to provide both breadth and depth to your efforts. Cybersecurity is enhanced when significant segments of the population understand the threat and how to mitigate it.