GO Committee #3
July 9, 2012

Worksession

MEMORANDUM

July 5, 2012

TO: Government Operations and Fiscal Policy Committee

FROM: Dr. Costis Toregas, Council IT Adviser CT

SUBJECT: Cyber Security Plan Briefing

The following are expected to attend:

Sonny Segal, Chief Information Officer
Dieter Klinger, DTS
Keith Young, DTS

Staff Recommendation:

1. **Request that a full cyber security plan, including an organizational strategy and funding requirements, be included in the FY2014 budget as a separate and identifiable element.**

Overview

Cyber security is in the minds of most government employees, private industry, and the general public, given the tremendous degree of reliance we all have on information and the systems that generate, store, process, and make use of it. The article on © 1-4 from the Business of Government organization sponsored by IBM gives some of the definitions, key strategies, and organizational recommendations regarding cyber security from the state government level; these are very similar to the local government concerns and can act as a primer for subsequent discussions by the Committee. Of note is the strong emphasis placed on collaboration and organizational strategies that span across many agencies.

The Department of Technology Services was asked during the budget worksession of April 2012 to provide the cyber security plan within 90 days; in the interim, a new CIO has been selected for the County, and he is currently organizing the various reporting efforts of the Department. In order to allow him the time to properly review and develop plans that reflect his own interests and policies, it was agreed that a briefing will be presented now, with a full plan being presented in a subsequent GO worksession. The briefing notes are on © 5-21.

Discussion

There are several Guiding Principles that reflect good practice, as well as academic research, in the area of cyber security. These are presented here as a starting point for the Committee's considerations and questions to DTS staff:

- Cyber security must be addressed at the enterprise level. Every system connects to many others, and the only way to get a strong handle on secure transactions and secure information is to organize security efforts across as many organizations as possible that are involved in the service delivery system. In addition to ensuring a strong plan across all departments of MCG (beyond the DTS systems), this enterprise initiative might look at all agencies funded through Council appropriations. A welcome fact is that the ITPCC has organized one of the 2013-14 efforts around cyber security.
- Beyond software patches and coding, an effective cyber security plan must look at the human dimension and processes that define system outcomes.
- Training of MCG employees has not been a priority. The last Computer Based Training effort was pushed out to employees in 2009, and the last 3 years have seen a veritable explosion of threats. Employee training should be a priority once again.
- Many systems used in MCG are developed and maintained by vendors. This means that the cyber security plan must extend to public/private partnerships as well.
- The County is currently involved in many open government initiatives, which will bring their own brand of security issues - from technology to public access and platforms of data exchange and use. An aspect, therefore, of the cyber security plan must explicitly deal with the Open Government future state of IT systems.

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers

By Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams

This article is adapted from Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams, "Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers" (Washington, DC: IBM Center for The Business of Government, 2010).

The importance of safeguarding information created and shared on computers and the Internet has increased significantly in recent years, as society has become increasingly dependent on information technology in government, business, and in their personal lives. Both corporations and government have responded by creating a new role in their organizations to lead the safeguarding efforts—chief information security officers (CISOs). The role of these officers is still under development. Do they safeguard best by using law enforcement techniques and technological tools? Or are they more effective if they serve as educators and try to influence the behaviors of technology users?

Cybersecurity has been commonly associated with three aspects of information technology: "people, process, and technology." People as users and creators of information and technology systems and defined organizational processes clearly affect the ability of any technological environment to be secured. Indeed, some would argue that convincing users to utilize secure processes when handling government information is the key solution to cybersecurity issues. Others argue that technological solutions are most important because they have the ability to define border environments as well as control the behavior of users within those environments.

Increasingly, there is recognition that it may be impossible to control the movement of data and that effective processes and data management are keys to security risk management. Will Pelgrin, director and chief cybersecurity officer of New York's State Office of Cyber Security and Critical Infrastructure Coordination, recently summed up the challenge: "[A] few short years ago we had a well defined perimeter.... [I]t has now dissolved–our job is to protect data that is resident with each and every one of us."

Definition of Cybersecurity

Cybersecurity can simply be defined as security measures being applied to information technology to provide a desired level of protection. The issue of protection can be defined using the acronym CIA for Confidentiality, Integrity, and Availability:

- **Confidentiality** refers to the property that data should only be viewable by authorized parties.
- **Integrity** refers to the principle that only authorized users are allowed to change data, and that these changes will be reflected uniformly across all aspects of the data.
- **Availability** refers to the principle that data and computer resources will always be available to authorized users.

Source: Conklin, Art and Gregory B. White. e-Government and Cyber Security: The Role of Cyber Security Exercises. Proceedings of the 39th Hawaii International Conference on System Sciences. *Kauai, Hawaii. January 4–7, 2006.*

Federal Concerns about Cybersecurity

Concerns about the security of computer systems were raised in 1976 by Thomas Rona, who saw the potential threat to information technology. As the use of technology grew, concern for security of systems and data within increased. Starting with the Clinton administration in 1998, successive presidents have devoted increased attention to cybersecurity.

Clinton Administration

Federal recognition of the cybersecurity threat came in May 1998, when the Clinton administration issued Presidential Decision Directive 63, instructing federal agencies to take steps to reduce the vulnerability of computer systems and communications networks. The directive was also intended to implement measures to mitigate threats to the commercial sector.

President Clinton appointed Richard A. Clarke as the National Coordinator for Security, Infrastructure Protection and Counter-terrorism, a Cabinet-level position.

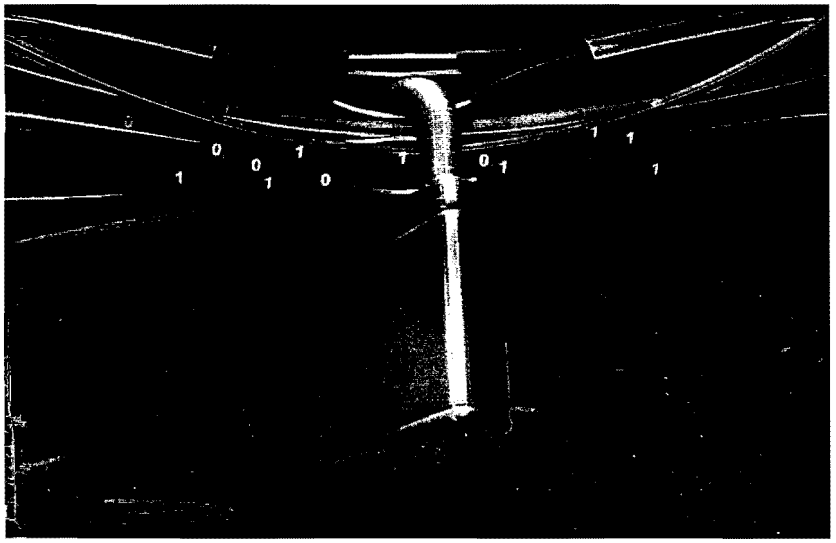
Bush Administration

The George W. Bush administration acknowledged the importance of cybersecurity and retained Clarke as a special advisor in the NSC, although his position was no longer at the Cabinet level. The Administration began reviewing cybersecurity policy in January 2001 and in October 2001 issued Executive Order 13231, which was designed to protect critical infrastructure. In February 2003, the administration released its final plan: *The National Strategy to Secure Cyberspace.*

Obama Administration

In 2009, the Obama White House released the report *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. The report signals the continued importance of cybersecurity, stating clearly. "[T]hreats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies." The report outlines seven key points:

- Cyberspace underpins almost every facet of modern society and provides critical support for the U.S. economy.
- The *status quo* is no longer acceptable.
- A national dialogue on cybersecurity must begin today and government, with industry, should explain the challenge so that the American people appreciate the need for action.
- The United States cannot succeed in securing cyberspace if it works in isolation; public-private partnerships as well as international collaboration are necessary.



- The federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well being of citizens.
- Working with the private sector, performance and security objectives must be defined for next-generation infrastructure.
- The White House must lead the way forward.

State Concerns about Cybersecurity

Pressures to elevate cybersecurity as a national priority pose challenges for cybersecurity professionals. Whereas organizing for cybersecurity at the federal level has taken shape within the Department of Homeland Security and the Department of Defense, states have had varied success in establishing links between *cyber* protection and *physical* security, as well as in integrating cybersecurity into overall state infrastructure planning. Their varied success stems from several issues:

- First, many state offices of homeland security have only recently incorporated personnel with expertise in critical infrastructure protection, even less those with expertise in cyber infrastructure.
- Second, to the extent that cyber infrastructure specialists exist, they are mostly situated within IT organizational communities, which may or may not be (in)formally coordinated with the state's homeland security apparatus. As a result, we see more CISOs advocating for structural arrangements and policies that can effectively bridge "the chasm between the worlds of critical infrastructure protection and cyber protection."
- Third, states have demonstrated both reluctance and enthusiasm to elevate cybersecurity as a major priority and to engage legislatively or administratively on issues of cybersecurity. For some, a lack of coherent guidance and intergovernmental funding from appropriate federal agencies is a serious hindrance. For others, a bottom-up approach that places state cybersecurity professionals at the forefront of decision making and dialogue is preferable. However, this approach is rife with difficulties. Challenges include overcoming authority and status barriers between federal and state experts on matters of policy (elite-actor bias), and securing two-way communication that reaches beyond symbolism to actual participatory governance (participation-deficit).

Despite these challenges, state CISOs have been on the front-end of cybersecurity dialogue, lending expertise to identifying gaps in policies, testing strategies for remediation, and acting as laboratories of innovation for how best to organize to address threats in an evolving cybersecurity environment.

2

Dr. Goodyear is the Chair of the Department of Public Administration at the University of Kansas. Dr. Goodyear teaches information policy and technology, organizational analysis, and organizational change.

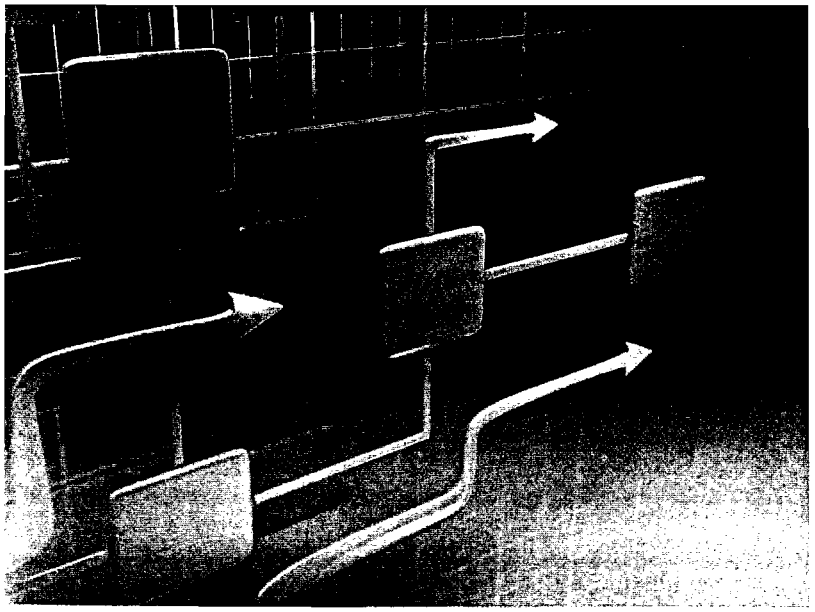
Dr. Goerdel is Assistant Professor of Public Administration at the University of Kansas. Her research focuses on the contribution of public management to organizational performance and the value of collaboration to problem solving.

Five Strategies Used by State Cybersecurity Officers

Data from the survey and case studies indicate there are five broad strategies utilized by state-level CISOs to advance their security programs. States are engaging in a common set of activities in relation to cybersecurity, but vary in the emphasis placed on each strategy. The strategies are:

- **Strategy One:** Development of policy and legal frameworks
- **Strategy Two:** Increased education of users
- **Strategy Three:** Use of technology and control mechanisms
- **Strategy Four:** Centralization of networks and IT services
- **Strategy Five:** Building collaborations across agencies, levels of government, and between sectors

Strategy One: Development of policy and legal frameworks. One of the most common strategies is the development of cybersecurity policies and assessment tools. All the states that responded to the survey have implemented IT governance structures that include a variety of stakeholders. As CISOs have worked within their governance structure to develop policy they have often gained the buy-in of stakeholders as well as developed robust policy.



Many states have implemented standards or procedures which provide more specific guidance for the implementation of the cybersecurity policies that are in place. Many states require regular assessments or audits to document compliance (or non-compliance) with cybersecurity policies, procedures, and standards.

Strategy Two: Increased education of users. All the states that participated in the study have active cybersecurity user education programs. These programs make full use of content shared nationally through CISO networks but also utilize content developed locally.

Strategy Three: Use of technology and control mechanisms. The application of technical controls to assist in cybersecurity is common among the states. Virtualization is providing a technical means of controlling data and access. Identity management systems are providing a means of implementing identification, authentication, and authorization schemas. Strong partnerships and outsourcing with private sector companies are assisting the states in improving their technical cybersecurity profiles.

Strategy Four: Centralization of networks and IT services. Centralization and consolidation of information technology services are also strategies utilized by the states. Centralization of networks and data centers is particularly helpful with cybersecurity efforts aimed at the protection of hardware, systems, and data.

Strategy Five: Building collaborations across agencies, levels of government, and between sectors. In order to successfully approach tangled problems, organizations need to create, lead, and participate in public sector knowledge networks (PSKNs) that are characterized not by a "need to know"

3

Dr. Portillo is an Assistant Professor in the Criminology, Law & Society Department and Deputy Director of the Center for Justice, Law & Society at George Mason University.

Ms. Williams is a doctoral student in Public Administration at the University of Kansas. Her scholarly research focuses on administrative law, environmental policy, and immigration policy.

information sharing environment but instead a "need to share" environment. Such networks treat the sharing of information and best practices as a primary purpose for existing and focus on sharing processes, practices, software, and other information technologies. Participating networks benefit from more timely, better quality, and more complete information by drawing on collective knowledge.

Recommendations

This review of the cybersecurity landscape at the state level provides a broad picture of both strategies used to build successful programs and the activities of the CISO. From our research, we draw the following five key recommendations:

Recommendation One: State cybersecurity officials should increase the use of collaboration and networks. CISOs should manage cybersecurity, in part, by identifying, mobilizing, participating in, and helping maintain public sector knowledge networks relevant to cybersecurity issues. CISOs and CIOs should recognize that the base of these networks is the development and preservation of interpersonal relationships, not a command and control perspective.

Recommendation Two: State cybersecurity officials should evaluate their formal and informal relationships with federal cybersecurity officials. In an effort to build on networks as discussed in Recommendation One, CISOs and CIOs should identify authority or status barriers between themselves and federal cybersecurity officials. Managerial efforts should then be directed towards removing, or mitigating, barriers most likely to impair bottom-up participatory governance by states regarding national cybersecurity programs.

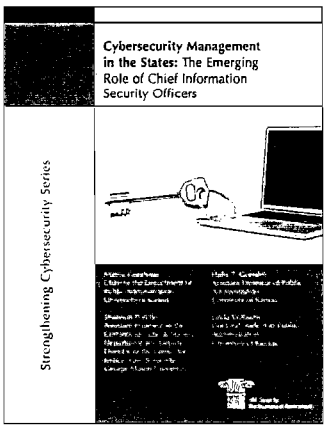
Recommendation Three: State cybersecurity officials should devote increased attention to and receive training in multidisciplinary problem solving. Cybersecurity management requires a practical philosophy of multidisciplinary problem-solving. The development of networks across security disciplines (cybersecurity, emergency management, critical infrastructure, information fusion centers, etc.) is critical for the continued success of cybersecurity efforts. Broadening CISO networks should be a priority for CISOs and CIOs.

Recommendation Four: State cybersecurity officials should receive training in collaboration competencies and those competencies should be recognized and rewarded. Education programs for the CISO community should be focused on collaboration skill sets, beyond those technical in nature. Collaboration competencies among CISOs should be incentivized, recognized, and rewarded by CIOs.

Recommendation Five: State cybersecurity officials should devote increased attention to data management. CISOs and CIOs should build collaborations with data owners, records managers, and archivists in the development of more robust data management within the states. ◘

TO LEARN MORE

Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers
by Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams



The report can be obtained:

- **In .pdf (Acrobat) format at the Center website, www.businessofgovernment.org**
- **By e-mailing the Center at businessofgovernment@us.ibm.com**
- **By calling the Center at (202) 551-9342**

4

Montgomery County Maryland

Enterprise Cyber Security and Information Risk Management Briefing

GO Committee Meeting - July 9, 2012

Presented By

Department of Technology Services

5

Contents

1. Introduction & Scope
2. Existing Security Measures & Initiatives Underway
3. Security Threats and Challenges
4. Strategies
5. Emerging Technologies
6. Initiatives under consideration
7. Cost considerations

Introduction & Scope

- Enterprise Security and Information Risk Management are interdependent
- Security is a part of all County Information Technology planning and operations
  - Enterprise Architecture
  - Enterprise Technology Strategic Plan
  - Enterprise Technology Service Offerings
  - Administrative Procedures
  - Enterprise Technology Policies
- A stand alone Cyber Security Plan will incorporate the above and enunciate strategies
- Scope of this presentation encompases DTS and Departmental Information Technology Assets

4

Existing Security Measures & Services

- Risk Assessment / Management
- Compliance
- Disaster Recovery / COOP
- Log Correlation and Management
- Incident Reporting and Response
- Computer Forensics and eDiscovery
- Remote access
- CIO and IT Review Processes
- Desktop Replacement and Patching
- Network redundancy enhancement
- Mobile policies and security
- Identity Management
- System & Service security audits
- Collaboration with other entities
  - ITPCC, COG
  - NIST, Securing Our eCity
  - Fortune 100 CISOs/CIOs

8

Existing Security Measures
Enterprise Architecture Support

- Active Directory and Single Sign On centralized directory service
- Common Enterprise Server configurations and patch management services
- Centralized desktop management with common configurations, patch management services, lockdown policy, centralized anti-virus services
- Centralized Email service including anti-virus, anti-spyware and spam removal services
- Enterprise Hosting Infrastructure hosting services
- Centralized help desk supporting Incident Response
- Enterprise network that includes protected single point of access, internal and external firewalls, wireless security, and network segmentation services
- Enterprise Service Bus for centralized secure information transfers
- Centralized Data Center that includes redundant systems for high availability, centralized backup and physical security measures
- Enterprise Server Management 24x7 server monitoring

(5)

Security Threats and Challenges

- Business and technical threats
- Consumer technologies
- Technologies evolving faster than enterprise solutions
- Targeted attacks against VIPs and government services
- More complex and new compliance regulations and laws
  - HIPAA, PA, PCI, ACH
- "Hacktivism" – targeted hacking to promote an agenda
- Increased public visibility

(6)

Strategies

1. Training - employees, contractors, and partners
2. Assess project requirements and recommend reasonable risk solutions
3. Continue and enhance the use of secure and stable cloud technologies
4. Cloud Considerations
5. Secure County information accessed from mobile devices (smartphones, tablets, etc.)
   - County Provided & Employee owned
6. Manage users of all County services
7. Streamline and automate security

6

Strategies - Training

- Security Awareness training deployed in 2008; 96% of all County employees completed training in FY09
- New technologies and threats warrant updated training content
- Ongoing training and Security Information dissemination through security reminders and notifications
- Training expansion to contractors and partners

Strategies - Requirements and Solutions

- Continue to work with departments and system owners to minimize new threats or audit/assessment findings in existing IT systems.
- Continue IT CIO and IT Review Processes that include review platform and security options
- For new major IT projects, include customer needs and risk tolerances into project functional requirement.
- Follow emerging cyber security solutions and standards

Strategies - Cloud Technologies

- DTS already uses a number of Cloud offerings in its services
- County Enterprise Architecture supports the use of Cloud Services
- Increased availability in the market of secure cloud services opens more opportunities for improved security
- Process support has been added in the project review process to help guide departments to cloud services where appropriate

Strategies - Cloud Considerations

- Legal and Contractual
  - New process for contracts
  - Standard County terms and conditions applicability
  - Data ownership

- Risk Assessment
  - Vendor certifications to known security standards
  - Service Availability and Disaster Recovery
  - Data Integrity

- Operational
  - Identity Management Accessibility
  - Data Migration
  - Integration

15

Strategies - Mobile Devices

- Engage Departments to identify business needs and use cases, security and cost consolidation
- Develop Bring Your Own Device (BYOD) policies and procedures
- Monitor BYOD management software market
- Establish Enterprise supported mobile accessible data solutions

Strategies - Manage Users

- Citizen interaction can require user management technology
- Identity Management project is building the foundation for management of both employees and non-employees
  - Initial focus is ERP access for retirees and volunteers
- Further user management focus on management of "unknown" IT service users, like citizens and other business partners
- "Multiple personality" population is a challenge for governments

5

Strategies - Automation

- Security and Operations Automation is ongoing to address resources constraints
  - Security operations automated between security cloud vendors
  - Automated system alerting notifications
  - Automated application heartbeat notifications

- Additional service automation planned for incident response, vulnerability reporting, and breach detection

- Identity Management will have automation options
  - Automatic user provisioning and deprovsioning
  - Automatic role provisioning and deprovsioning

Emerging Technologies

- Mobile Apps
  - Developing a Mobile Apps framework
  - Review process to include legal and security review and input
  - Enable sustainability and manageability
- Open Data
  - Governance and data publishing process defined
  - Data security and privacy review and approvals
  - Designed for sustainability and manageability
- Social Media, Collaboration & Cloud Data Storage
  - Use governed by Administrative Procedures
  - Enterprise solutions needed
  - Legal and contractual considerations

(19)

Initiatives under Consideration

- Expanded and new security awareness training
- Online and periodic security tips and FAQs
- Focus on compliance with legal and contractual mandates
  - Accelerated patching and vulnerability remediation
  - Expanded auditing of departmental systems
- Two factor authentication
- Expanded / accelerated Identity Management
- Enterprise Collaboration and Cloud based data storage
- Mobile Device Management solutions
- Creation of Chief Information Security Officer role/position
- Formalization of departmental security roles

(2)

Cost Considerations

- Staffing resources
  - Training development
  - Breach detection and incident response expansion
  - Patching and vulnerability remediation expansion
  - Identity Management expansion / acceleration

- Operating costs
  - Two factor authentication
  - Enterprise Collaboration and Cloud based data storage
  - Mobile Device Management solutions
  - Consulting Support

(2)