Senate Resolution 360 – Senate Study Committee on Data Security and Privacy

Presentation Summary, Findings and Recommendations

OVERVIEW

The Senate Study Committee on Data Security and Privacy was created by SR 360 in the 2016 legislative session and met four times between August and November to receive public testimony.

Below is a summary of topics covered in presentations from public and private sector representatives over four meetings:

- The **cyber threat landscape** was covered in multiple presentations to the committee, including a review of threats to critical infrastructure and the general public. Some of the themes included:
    - Nation-state actors as the main threat to critical infrastructure, such as our electrical grid,
    - The inevitability of data breaches in public and private systems,
    - An increase in threats to payments systems, with e-commerce seen as a huge threat vector, and increasing credit card fraud and losses,
    - IT systems are becoming more distributed – no real borders to defend. Defense in depth doesn't work anymore,
    - Georgia's state agencies have varying capabilities to address cybersecurity threats,
    - The level of threats is growing faster than we are growing our capabilities to respond,
    - End users of government systems and the public are not fully aware of the threats they face and how to protect themselves, and
    - In-depth discussion of specific threats, including: Advanced Persistent Threats (APT) and ransomware.
- The need for **cybersecurity skills training and workforce development** to address current and future workforce shortages.

- **Training and awareness programs** to improve public knowledge and participation in fighting cyber threats/crimes.
- **Tools and technologies** to identify and mitigate the growing number of increasingly sophisticated cyber threats and increases situational awareness.
- The need for **public-private partnerships** to address the magnitude of the threat.
- **Privacy** as an expectation of customers and constituents.
- **Public policy** around cybersecurity and cybersecurity-related legislation.
    - A presentation at Meeting 4 by Yejin Cooke, representing the National Association of State Chief Information Officers (NASCIO), included the 2016 NASCIO report entitled *State Governments at Risk: Turning Strategy and Awareness into Progress*.
    - The NASCIO report cites the top three cybersecurity initiatives in 2016 as: training and awareness, monitoring/security operations centers (SOC), and strategy.
    - Table 1 is an excerpt from the NASCIO report as a review of cybersecurity legislation in the fifty states, and will be referenced in the findings.

Table 1 – NASCIO Summary of States' Cybersecurity Legislation[1]/Statutes

	Established and funded	Established and not funded	In progress	Not in place
Cybersecurity incident/data breach reporting and handling	43%	21%	4%	32%
Data breach notification	41%	35%	2%	23%
Role and authority of the enterprise CISO or equivalent	40%	4%	2%	54%
Continuity of government/continuity of operations	35%	13%	4%	48%
Cybersecurity awareness	31%	4%	2%	63%
Data privacy provisions: authority and purpose; collection, storage, use, and sharing limitations	27%	21%	2%	50%
State-level cybersecurity program and framework for enterprise risk management	27%	17%	8%	48%
Cybersecurity budget allocation and review	26%	0%	4%	70%
Cyber threat information-sharing program between state agencies, law enforcement, and private entities	21%	10%	6%	63%
Public-private partnerships or council to support the state's cybersecurity programs	13%	2%	4%	81%
Cybersecurity workforce development and training	11%	4%	4%	81%
Cybersecurity legislative council or equivalent to do a periodic review, steer the state's cybersecurity posture, and allocate funding	11%	10%	6%	73%
Role and authority of the enterprise chief privacy officer (CPO) or equivalent	6%	2%	2%	90%

Source: 2016 Deloitte-NASCIO Cybersecurity Study. Graphic: Deloitte University Press | DUPress.com

[1] NASCIO 2016 Cybersecurity Study, State Governments at Risk: Turning Strategy and Awareness into Progress, Figure 29, page 20

FINDINGS AND RECOMMENDATIONS

Addressing the increase in threats and the frequency and sophistication of attacks will require a comprehensive approach structured around the domains of people, process and technology.

Section I.

Talent – A People Perspective

Finding #1: An acute shortage in the U.S. cybersecurity workforce and in training exists now and into the near future.

- Cyber workforce is not keeping pace with need – currently 0% unemployment rate.
- The cyber workforce is projected to face at least a 1.5 million resource shortage by 2020.
- A survey of state Chief Information Security Officers (CISOs) included in the 2016 NASCIO report[2] shows that the top three human resources challenges are:
    - State government salary rates and pay grade structures (96%),
    - Lack of qualified candidates due to demand from federal agencies and private sector (59%), and
    - Workforce leaving for private sector (47%).
- There is a critical need to increase the number of skilled cybersecurity resources, which will require:
    - Introduction of cyber training curricula and programs at educational levels from K-12 and post-secondary,
    - Programs to include private industry and academia to develop and implement effective cyber training programs, and
    - Partnerships with public-private companies and higher education institutions to introduce and promote careers in cybersecurity and create a pipeline of skilled resources.
- There is a need to increase cybersecurity awareness training for state government employees.

[2] NASCIO 2016 Cybersecurity Study, *State Governments at Risk: Turning Strategy and Awareness into Progress*, Figure 18, page 15

- All states have a least some capability of delivering cybersecurity/security awareness training to their employees. (See Table 2)[3]
- Sixteen states have some kind of mandatory requirement for security awareness training.[3]
- Of the sixteen states with mandatory security awareness training for employees, two states required it through statute (Florida and North Carolina), one state used an executive order (New Hampshire), and the other thirteen states used some kind of delegated authority to their central IT agency to pass a rule, policy, or standard requiring the awareness training.[3]

- Internships can be an effective way to find and develop talent.

Recommendations:

R1.1 Provide support for a State Cybersecurity Training Academy. (Short-term)

R1.2 Require all executive branch state employees to go through annual security awareness training and fund the licensing required to conduct the training. (Short-term)

- There are a number of vendors that sell security awareness training as a service, usually delivered as computer-based training (CBT) via a cloud-hosted learning management system (LMS).

R1.3 Require state vendors and contractors with access to state systems to complete cybersecurity awareness training.

R1.4 Explore options for building a cyber range or leveraging an existing cyber range for training. (Medium-term)

R1.5 Explore options for, and encourage, the introduction of cyber training curricula in schools. This could be any combination of K-12, technical colleges, and higher education. (Long-term)

R1.6 Provide support for a coordinated internship program (with central clearinghouse) focused on bringing students in cybersecurity education programs into state government. (Long-term)

R1.7 Explore the creation of programs to implement work requirements in exchange for training and educational opportunities. (Long-term)

[3] Table 2 produced using information from the National Conference of State Legislatures' website: http://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx

Table 2 – National Conference of State Legislatures (NCSL) Summary of Sample States' Cybersecurity Awareness Training

State	Summary	Mechanism
Colorado	Colorado's cybersecurity training is mandatory for state employees and statutorily required under the Colorado Information Security Act. Website	Rulemaking from the Office of Information Security
Delaware	Delaware offers annual statewide cybersecurity training for state and local government employees. Mandatory cybersecurity training for all executive branch agency employees, which was developed by the Delaware Department of Technology and Information pursuant to authority granted to it by Delaware Code Title 29, Chapter 90C, is part of the state's strategic plan. Website	Requirement issued by Department of Technology and Information; statute doesn't explicitly address security awareness training.
Florida	Florida has mandatory cybersecurity training for state employees as required by Florida Statutes Chapter 282. Website	Training is in the statute - 282.318 Enterprise security of data and information technology.- https://www.flsenate.gov/Laws/Statutes/2012/Chapter282/All
Louisiana	Louisiana has mandatory cybersecurity training for new employees and annual training for all employees pursuant to the Louisiana Division of Administration, Office of Technology Servicesp.52.	Policy issued by Division of Administration, Office of Technology Services. http://www.doa.la.gov/OTS/InformationSecurity/InformationSecurityPolicy-LA-v.1.0.pdf
Maryland	Maryland requires state employee cybersecurity training through the Department of Homeland Security. State agency personnel have to take a cybersecurity class each month to gain access to state networks. Website	Policy issued by the Department of Information Technology (DoIT). DoIT's authority stems Maryland Code § 3A-303 and § 3A-305.
Montana	Montana has mandatory executive branch state employee cybersecurity training upon hiring and then annually. Cybersecurity Training and Awareness Program. Legislative branch employees are not required to take cybersecurity training, but are encouraged to do so.	Training is coordinated through the State Information Services Division.
Nebraska	Nebraska has mandatory annual cybersecurity training and a refresher course for all state employees as outlined in department regulation. Website	Policy issued by the Nevada Department of Administration, Enterprise IT Services. State Information Security Consolidated Policy (State PSP 100, Section 3.5 Security Awareness) requires all Nevada State employees to complete information security awareness refresher training at least annually.

New Hampshire	New Hampshire requires mandatory cybersecurity training for state employees annually through executive order.	Executive order – press release here http://governor.nh.gov/media/news/2015/pr-2015-10-08-data-secure.htm
North Carolina	North Carolina's Statewide Information Security Manual requires each agency to provide training and annual assessments of cybersecurity issues on an agency-by-agency basis.	Statewide information security standards required by N.C.G.S. §147-33.110, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security.
Ohio	Ohio requires annual cybersecurity awareness training.	State IT Policy IT-15 (Security Awareness and Training) mandates that agencies put system users, be they employees, contractors, temporary personnel or other agents of the state, through annual security awareness training. Issued by the Office of Information Security and Privacy.
Oregon	Oregon requires each state agency to have a cybersecurity plan under which all employees, volunteers and third-party users receive appropriate cybersecurity awareness training and regular updates on policies and procedures	The boilerplate cybersecurity plan includes a section for awareness training.
Pennsylvania	Pennsylvania has mandatory online cybersecurity awareness training for all state government employees.	Appears to be required by policy - ITP-SEC000 at http://www.oa.pa.gov/Policies/Pages/itp.aspx
Utah	Utah has mandatory cybersecurity training.	State Employees are required by the Department of Technology Services to take the Security Awareness Training provided to all employees.
Vermont	Vermont has mandatory cybersecurity awareness training for all new state employees.	
Virginia	Virginia has required agency-by-agency state employee cybersecurity training.	The Virginia Information Technology Agency requires security awareness training via a formal policy.
West Virginia	West Virginia has mandatory annual training on cybersecurity and privacy.	Training is administered by the West Virginia Office of Technology.
This information is reproduced from the National Conference of State Legislatures' website: http://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx		

Section II.

Strategy and Governance - A Process Perspective

Finding #2: A lack of consistency and clarity on mandated roles and responsibilities are two of the top problems in state government cybersecurity efforts.

- Documented cybersecurity standards, policies and guidelines exist but are not consistently applied or implemented across state agencies.
- There is no single authority to mandate the implementation of cybersecurity best practices across the diverse branches of government.
- Stronger governance for cybersecurity is needed to:
    - establish best practices and requirements for security patching,
    - define encryption requirements,
    - define privacy and open records requirements and policy,
    - define incident reporting/notification requirements of agencies, and
    - define a consistent incident response model across state government that allows for faster and more effective response.
- Having in place documented and consistent cybersecurity practices across state agencies is critical in acquiring cyber insurance.
- Georgia has created the Cybersecurity Review Board for state government; members include the state CIO, the director of GEMHSA, the state adjutant general and the director of DOAS.
- Collaboration will be needed for an effective state government cyber strategy.

Recommendations:

R2.1 All executive branch state agencies should designate a cybersecurity point of contact and/or chief information security officer and file their contact information with the Georgia Technology Authority. (Short-term)

- Current GTA standards require state agencies to implement a formal information security program and to designate an Information Security Officer to run the program (GTA standard SS-08-006 Information Security Management

Organization). There is no requirement that contact information be filed with GTA.

R2.2 Designated executive branch agency cybersecurity points of contact should complete basic cybersecurity training at the State Cybersecurity Training Academy or be certified, or pursuing certification, in cybersecurity. (Medium-term)

R2.3 Enact requirements for cyber incident notification and response by state agencies. (Short-term)

- Georgia does have a notification law in statute (O.C.G.A. § 10-1-912) which specifically covers notification to *affected individuals* in the case of a breach of personally identifiable information. There is no requirement to notify any official or agency within state government.
- Current GTA standards regarding incident notification (SS-08-004 Incident Response and Reporting) requires each agency to have an incident response plan and for the plan to be approved by the State CISO and the GBI. The standard does not require agencies to notify GTA when an incident occurs.

Section III.

Operations - A Technology Perspective

Finding #3: The current environment requires an increasing investment in technology to detect and respond to increasingly sophisticated cybersecurity threats.

- Addressing this problem will require implementing security and monitoring tools to:
    - Gain greater real time visibility and context of a cyber attack – understand the who, what, when, where, and how of an attack;
    - Continue to shift from perimeter defense to active monitoring, mitigation, and event management; and
    - Aggregate monitoring of security events across agencies, vendor services, and solutions.
- Technologies and services from private sector partners should be leveraged to:
    - Prevent unauthorized access to systems and data, and
    - Limit exposure and reduce the propagation of threats (Zero Trust, micro-segmentation).

- There are specific IT tools that the state of Georgia should consider to improve cybersecurity:
    - Security Information and Event Management (SIEM),
    - Data Loss Prevention (DLP),
    - Managed Security Operations Center (SOC),
    - Identity and Access Management (IAM) web service - including multi-factor authentication,
    - Cloud Access Security Brokers (CASB), and
    - Zero day malware detection with sandboxing.
- State agency assessments which are already underway will help identify areas for improvement and in need of remediation.
    - The legislature provided funding in AFY16 to begin these assessments, and there is a need for continued funding.

Recommendations:

R3.1 Continue funding for third-party cybersecurity assessments of state agencies. (Short- to Medium-term)

R3.2 Fund the remediation efforts for gaps that are found by the current, ongoing cybersecurity assessments.

R3.3 The state should contract with a Managed Security Services Provider (MSSP) to create a managed Security Operations Center (SOC) for continuous monitoring of critical systems and continuous environmental and vulnerability scanning. (Medium-term)

Section IV.

Legislation and Policy

Finding #4: Legislators regularly hear concerns from constituents about data breaches, stolen identities and cybersecurity, but don't know what the state is doing to protect citizen data and government systems.

- There is a need to increase awareness within the General Assembly about the state's role in cybersecurity and to help legislators understand the speed of the changing cybersecurity dynamic.
- With the exception of the issue of how and when data breaches are reported, there is little current cybersecurity legislation across the fifty states, as issues around cybersecurity are being mostly handled without legislation.[4]
- Cybersecurity awareness training is needed to improve knowledge level and skills of state employees and the general public.

Recommendations:

R4.1 Explore ways to encourage and/or partner with the private sector to create public awareness campaigns to promote cybersecurity. (Medium-term)

R4.2 Create a Georgia Cybersecurity Collaborative Initiative, bringing together state, local and federal entities, the private sector, and academia. (Medium-term)

R4.3 Work with the Georgia Bureau of Investigation to explore legislation to protect citizens against cyber crimes.

Finding #5: Customers and constituents have an expectation of privacy but there is no common definition of privacy nor common standards or laws for regulation of privacy.

- Privacy requires a different set of processes from security.
- *Security* is about locking up the data so that only the "right" people can see it. *Privacy* is determining how data can be used and who those "right" people are.
- Four key components of a privacy program include governance, compliance requirements, data governance, and fair information practices.
- The varying laws and regulations in the fifty states create a "fabric" of privacy protection that is strong.
- State governments are not very far along in developing privacy programs. Currently, 8% of states report that they have a defined Chief Privacy Officer role and 13% of states report they are doing an annual privacy impact assessment.[5]

[4] See Table 1; excerpted from NASCIO 2016 Cybersecurity Study, State Governments at Risk: Turning Strategy and Awareness into Progress, Figure 29, page 20

[5] See Table 1; excerpted from NASCIO 2016 Cybersecurity Study, State Governments at Risk: Turning Strategy and Awareness into Progress, Figure 29, page 20

- European privacy laws are very strong and comprehensive, but not currently popular in the U.S.
- Privacy is a broad, complicated topic. This is especially true in state governments, where there are potential conflicts with sunshine laws, such as the Georgia Open Records Act.

Recommendations:

R5.1 Continue to monitor the issue of privacy and solicit feedback and input from citizens and industry. (Medium-term)

Finding #6: The State of Georgia is currently considering purchasing cyber insurance.

- Cyber insurance has become a useful tool to mitigate financial risks from large data breaches.
- First Party Insurance covers direct loss and out of pocket expense incurred by insured.
- Third Party Insurance covers defense and liability incurred due to damage caused to others by the insured.
- State government is a new market for underwriters handling cyber insurance. There is some caution in the industry and not all underwriters are willing to write a policy for government agencies.
- The State of Georgia is currently investigating opportunities to provide cyber insurance for all agencies, though some agencies may not be insurable due to a lack of cybersecurity processes.

Recommendations:

R6.1 The General Assembly should encourage and support the Department of Administrative Services (DOAS) in purchasing cyber insurance. (Short-term)

R6.2 DOAS and GTA should work with those agencies which underwriters are not willing to insure to improve their insurability. (Long-term)