GEORGIA CYBERSECURITY WORKFORCE ACADEMY

NASCIO 2018 State IT Recognition Awards

Title:	Georgia Cybersecurity Workforce Academy
Category:	Cybersecurity
State:	Georgia
Contact:	Stanton Gatewood Stan.Gatewood@gta.ga.gov 404.463.1003
Project Initiation Date:	January 1, 2017
Project Completion Date:	November 30, 2017

EXECUTIVE SUMMARY

The growing threats from cyber criminals and the need to ensure an enterprise-wide, coordinated approach to cybersecurity led the Georgia Technology Authority (GTA) to launch the Georgia Cybersecurity Workforce Academy in January 2017. Under the direction of State Chief Information Security Officer (ISO) Stanton Gatewood, the academy provides cybersecurity awareness, training and education to information security officers in the public sector. It's an integral component of the state's overall cybersecurity strategy.

The academy graduated 48 ISOs in November 2017 after they successfully completed a series of rigorous courses over 11 months. The courses were designed and taught by Mr. Gatewood and his team as online, instructor-led training. Feedback from graduates validates both the need for the academy and its effectiveness in advancing their cybersecurity skills.

The academy's success exceeded GTA's expectations. The academy is expanding in 2018 in response to demand from state and local government agencies, and will include participants from local government and feature guest lecturers from state universities, technical colleges and leading cybersecurity firms.

For 2018, classes are taught both online and in the classroom, and the academy will relocate from GTA's office in Atlanta to the Hull McKnight Georgia Cyber Center for Innovation and Training in Augusta when it opens in July. The Cyber Center is the single largest investment in a cybersecurity facility by a state government to date.

Architect's rendering of the main entrance to the Cyber Center.

PROJECT NARRATIVE: CONCEPT

Large-scale security breaches and cybercrimes seem alarmingly routine in today's world. They're often the focus of national and local news reports, and consumers are constantly urged to take steps to protect their computing devices and their private information – from downloading anti-malware software to upgrading operating systems and even to subscribing to credit and identity-theft monitoring services. Consumers now find that they have a significant role to play in fighting cybercrimes along with information security specialists in government and private-sector organizations.

Georgia's information systems, just like those of other state and local governments, are under constant bombardment from cyber criminals. Gartner described "relentless and ever-increasing security attacks," and Stanton Gatewood, chief information security officer (ISO) for the state of Georgia, said, "The threats are growing, they are evolving and they are persistent."

Security and risk management – encompassing security frameworks, data protection and training and awareness – are the top priority for state CIOs in 2018, according to a survey by the National Association of State Chief Information Officers (NASCIO).

The growing threats from cyber criminals and the need to ensure an enterprise-wide, coordinated approach to cybersecurity led the Georgia Technology Authority (GTA) to launch the Georgia Cybersecurity Workforce Academy in January 2017. Under the direction of Mr. Gatewood, the academy provides cybersecurity awareness, training and education to information security officers in Georgia state agencies.

It's also an integral component of the state's overall cybersecurity strategy, which includes:

- Extensive enterprise-wide policies, standards and guidelines, which are continually reviewed and updated as needed.
- The Governor's Cybersecurity Review Board, which assesses the state's overall cybersecurity preparedness each year and recommends appropriate responses.
- The Cybersecurity Risk Register, which provides a framework for categorizing and responding to cybersecurity risks across the state's IT enterprise.
- Contracts with four private-sector companies to conduct independent assessments of individual agencies using the National Institute of Standards and Technology's Cyber Security Framework.
- One hundred million dollars in cyber insurance.

The Hull McKnight Georgia Cyber Center for Innovation and Training, a $100 million facility that GTA is building in Augusta, Georgia.

The academy was one of several recommendations from the state's Senate Study Committee on Data Security and Privacy in 2016.

In addition, the first goal in Georgia's Enterprise IT Strategic Plan, which sets the technology direction for the state's IT enterprise through 2025, is to "build a culture of information security awareness, preparedness and resilience, and mature the state of Georgia's information security program."

The academy is at the center of efforts to achieve this goal.

PROJECT NARRATIVE: SIGNIFICANCE

The Georgia Cybersecurity Workforce Academy is helping equip state agencies to respond to threats from cyber criminals. In November 2017, the academy graduated 48 information security officers after they successfully completed 11 rigorous courses begun in January. The courses were designed and taught by Mr. Gatewood and his team as online instructor-led training through GTA's Learning Center.

Mr. Gatewood has more than 33 years of experience in cybersecurity programs for the U.S. military, state and federal governments, higher education and global corporations. Prior to joining GTA, Mr. Gatewood served as Director of Cyber Workforce Development for Dell™ SecureWorks®. He was also Chief Information Security Officer for the University of Georgia, Interim Vice President for Information Technology and Chief Information Officer for Albany State University and Chief Information Security Officer for the Board of Regents of the University System of Georgia. Mr. Gatewood is a distinguished fellow at the Ponemon Institute, the widely known research center dedicated to privacy, data protection and information security policy. He has also received numerous honors for his work in the field of information security, served as an active member of several professional associations and published articles on information security.

The courses were as follows:

Introduction and Basic Cybersecurity (January 2017, one day)

The course was a primer to convey an abstract of cybersecurity in a networking environment. It set out security basics, examined where major threats are coming from today and in the future and looked at new solutions to managing security.

Information Security Officer in the Public Sector (February 2017, two days)

The course introduced the role and responsibilities of an information security officer in state government. It provided ISOs with general guidance in understanding their role and developing and maintaining an effective information security program in the public sector.

Building an Information Security Program in the Public Sector (March 2017, two days)

The course explored eight key components to developing, implementing, reviewing and improving the effectiveness of a public-sector information security program:

- Security governance
- Strategic information security planning
- Policy and compliance management
- IT/IS risk management
- Cybersecurity incident management
- Security awareness and training
- Continuity of Operations planning
- Annual information security program

Cybersecurity Strategic Planning (April 2017, two days)

The course focused on the process of creating an information technology or information security strategic and implementation plan.

Cybersecurity Policy Management (May 2017, one day)

The course focused on establishing appropriate administrative, operational and technical policies, standards and procedures to ensure compliance with business requirements and laws and to support information security program goals and objectives.

Cybersecurity Incident Management (June 2017, one day)

The course reviewed agency, enterprise and state incident management processes. It focused on processes associated with the National Incident Management System and its relationship to Georgia’s cyber incident management process.

IT and Information Security Risk Management (July 2017, two days)

The course provided a foundational knowledge of the Risk Management Framework developed in accordance with the Federal Information Security Management Act and the National Institutes of Standards and Technology.

Security Awareness, Training, Education and Professional Development (August 2017, one day)

The course focused on training agency workers on information security policies, standards, procedures and techniques. It also examined the various management, operational and technical controls necessary to protect information resources and assets and the skills needed to effectively manage those controls.

Cybersecurity Maturity (September 2017, two days)

The course examined ways to measure the following components of an information security program in order to determine an organization’s cybersecurity maturity level:

- Culture
- Philosophy
- Processes
- Technology
- Awareness

It looked at how to align information security with business needs and to develop an organization-wide “security aware” culture.

Continuity of Operations Planning/Cyber Resilience (September 2017, two days)

The course focused on preparing state agencies to maintain mission-critical operations after an emergency or disaster, including critical activities such as backups and recovery, cyber incident response, disaster recovery and business continuity.

IT and Cybersecurity Leadership (October 2017, two days)

The course explored the following topics:

- Characteristics of leaders and how they think
- Leading managers and other higher-ups
- One-on-one leadership and influencing and engaging others
- Team building

Capstone Projects

Academy participants spent November 2017 researching a cybersecurity topic they selected themselves and preparing a presentation to demonstrate their mastery of the subject.

The following are representative examples of capstone projects.

Cyber Situational Awareness – The project examined the three key elements of a comprehensive approach to cyber situational awareness: computing and network components, threat information and mission dependencies.

Cyber Risk Register – A risk register documents the potential adverse events to which an organization is subject. The project examined what content should be included in an effective risk register, including descriptions of adverse events.

Cyber Kill Chain – The project took an in-depth look at the various stages in a cyber attack and how ISOs can use the Cyber Kill Chain framework to defend networks.

PROJECT NARRATIVE: IMPACT

Feedback from graduates attests to the academy's effectiveness in strengthening their awareness of cybersecurity threats and advancing their skill levels.

"After attending the Georgia Cybersecurity Workforce Academy, I had a better understanding of the direction in which the state is heading in cybersecurity, and my knowledge of information security was enhanced. The classes provided a roadmap for agency ISOs to use in building strong cybersecurity programs for their agencies." − Felicia Hedgebeth, Georgia Department of Banking and Finance

"My participation in the Georgia Cybersecurity Workforce Academy was a gateway to better understanding cybersecurity. The additional knowledge and skills will foster growth in my current role as an information security officer. The course content provided a comprehensive overview of the essential concepts and methodologies in building an information security program. I recommend that all state agency ISOs and other security specialists register for the academy." − Raquel A. Sulal, Georgia Department of Behavioral Health and Developmental Disabilities

The positive response from state agencies coupled with growing interest from local governments led Mr. Stanton to expand the academy by adding participants from county and municipal governments along with those from state agencies to the 2018 class. The academy is now offering classroom instruction in addition to online instruction.

Classes will be conducted at the Hull McKnight Georgia Cyber Center for Innovation and Training when the $100 million facility opens in July 2018. The Cyber Center is the single largest investment in a cybersecurity facility by a state government to date. Currently under construction in Augusta, Georgia, the center is a unique public/private partnership among academia, state and federal government, law enforcement, the U.S. Army and the private sector. With the U.S. cybersecurity labor shortage predicted to hit a half-million or more unfilled jobs by 2021, the Georgia Cyber Center will train the next generation of professionals through education and real-world practice and support innovative companies focused on technology to strengthen online defenses. The center includes two adjacent buildings totaling 332,000 square feet and features a cutting-edge cyber range, a 340-seat auditorium, a secure briefing space, an incubator/accelerator to foster innovation and entrepreneurship, classrooms and access to the popular Augusta Riverwalk.

The academy is also adding new certifications and courses with guest lecturers from Cyber Center partners, including Augusta University, Augusta Technical College, the University System of Georgia, the Technical College System of Georgia, the Georgia Department of Defense and private-sector firms.