



**Georgia Department
of Human Services**

Office of Information Technology

DHS Cybersecurity Challenges / Opportunities

November 14th, 2018, DHS Board Meeting

Venkat R. Krishnan, Chief Information Officer (CIO)



stronger families

FOR A STRONGER GEORGIA



Agenda

- Data - A Highly Valuable Commodity
- Evolving Threat Landscape
- Common Security Challenges at DHS
- Progress Toward Closing the gaps



Data – A highly valuable commodity

- Data is highly useful and for value for decision makers
 - Evidence-based practices
 - Optimizing outcomes
 - Performance objectives
- DHS systems contain data for 1 in 5 Georgians (est. population = 10.43 million)
 - Data is sensitive in nature (PII, PHI) due to the social services component
 - Data is regulated and audited for compliance (CMS, IRS, SSA, FBI, DOAA)
- DHS is now offering services via the traditional brick & mortar locations, online web applications and via mobile applications.



Evolving Threat Landscape

- Increased security attacks across private and public sector systems
- Recent, successful, targeted attacks by nation-states on governments and critical infrastructure
 - Ransomware (e.g., Atlanta and multiple cities in Georgia)
 - Industrial Control Systems (Foreign Governments activity documented by Homeland Security)
 - K-12 community
- While software requires constant updates to defend against new and evolving security threats, so do employees through training.



Security Data Breaches

- **Equifax (2017)**

- Personal information (SSNs, DOBs, addresses, drivers' license numbers) of 143 million consumers
- Credit card data exposed for 209,000 consumers
- Cause: application vulnerability

- **Uber (2016)**

- Personal information of 57 million Uber users and 600,000 drivers exposed
- Cause: credentials for Cloud account exposed

- **Target Stores (2013)**

- 120 million people impacted; 40 million credit and debit card numbers exposed
- Cause: access gained through a third-party HVAC vendor to its point-of-sale (POS) payment card readers



2018 Security Data Breaches

- **Pennsylvania Dept of Education**

- An error made by an employee in the governor's Office of Administration caused a database breach that lasted for 30 mins and exposed 360,000 records containing SSNs of current and former teachers.

- **Florida Virtual School**

- A breach exposed PII of more than 368,000 students
- Another breach exposed PII of 1,800 Leon County teachers.

- **California Dept of Developmental Services**

- A physical break-in may have exposed PII of 582,000 clients as well as 15,000 employees.

- **GovPayNow.com**

- Exposed 14 million customer records of 2,300 government agencies in 35 states containing PII and credit card numbers.



Cyber and Technology Liability Insurance

- Worked with DOAS and GTA to obtain Cybersecurity insurance
- Addresses losses (data breaches) from cybersecurity incidents
- Advocates preventative measures to reduce risk
- Promotes the use of security industry standards to protect systems



Common Security Challenges at DHS

- Increasing the cybersecurity awareness of staff to reduce email phishing and other social engineering attacks
- Encouraging greater physical security of DHS equipment (laptops, smart phones, tablets)
- Promoting established security practices for facility security
- Incorporating additional strategies to minimize social engineering attacks against staff and constituents



Social Engineering – Successful Attacks

Successful social engineering attacks give hackers:

- Access to physically restricted areas and locked IT systems, allowing them to install malware and viruses.
- Confidential information such as: client data, employee records, contracts.
- Ability to control devices and files within the organization's network
- Loss of productivity due to downtime

The average cost of a data breach in 2018 is **\$3.86M**

The average cost of a single stolen record containing sensitive and confidential information is **\$148**

<https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses>



Progress Toward Closing the Gaps

- Encrypting Disk Storage
- Rolling out technology to eliminate visibility to regulated data
- Increased Regulatory Compliance
- Current campaign to improve security of all DHS-operated web sites
- Monitoring Security Alerts from US-CERT, Homeland Security, FBI



Cybersecurity Awareness Fair

- National Cyber Security Awareness Month is observed in October
- Cyber Security Awareness Fair was held on Oct 17, 2018
- The theme for 2018 is “Let’s Tackle Security”
- DHS participated in conjunction with the Dept. of Public Health
- Informational stations and security professionals provided interactive presentations to attendees



Cybersecurity Awareness Fair



Dashlane Password Tester

The screenshot shows a web browser window with the following elements:

- Browser menu: File, Edit, View, History, Bookmarks, Tools, Help
- Tab: How Secure Is My Password?
- Address bar: <https://howsecureismypassword.net>
- Page title: HOW SECURE IS MY PASSWORD?
- Progress indicator: A horizontal bar with 15 black dots.
- Text: It would take a computer about **7 QUADRILLION YEARS** to crack your password
- Text: Dashlane can help you remember all of your secure passwords - and it's free!
- Button: Tweet Your Result



Security Self-Assessment Quiz



The screenshot shows a web browser window displaying the NIST website. The address bar shows the URL <https://www.nist.gov/quiz/are-you-safe-online>. The page features the NIST logo at the top left and a search bar at the top right. The main heading is "Are You Safe Online?". Below this is a large graphic with a green circular icon containing a filmstrip-like pattern, the text "National Cyber Security Awareness Month", and the date "October 2017". To the right of the graphic is the CyberAware logo. The page contains several paragraphs of text explaining the importance of cybersecurity and inviting users to take a quiz. A blue "Start Quiz" button is prominently displayed. At the bottom, there is a footer with the NIST logo, contact information for the headquarters, social media icons, and a "Feedback" button.

File Edit View History Bookmarks Tools Help

NIST Are You Safe Online? | NIST

https://www.nist.gov/quiz/are-you-safe-online

80%


Search

NIST

Search NIST

NIST MENU

Are You Safe Online?



National Cyber Security Awareness Month

October 2017

Cybersecurity is everyone's business! As personal computing devices become even more pervasive, the chances of falling victim to a cyber-attack rise higher and higher. With continuous use of email, social media, banking apps, etc., the list of vulnerabilities to which we have opened ourselves is ever-growing. Hackers often use an unsuspecting individual's error, like a weak password or clicking a suspicious link, to gain access to larger institutions or to organize large-scale denial-of-service attacks.

It is more important now than ever to be responsible with our cybersecurity practices, not just at work but also at home. Do you know how to keep your accounts secure or how to spot a suspicious email?

Take our cyber quiz to find out how cyber-savvy you really are.

[Start Quiz](#)

NIST National Institute of Standards and Technology
U.S. Department of Commerce

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
301-975-2000

How are we doing? [Feedback](#)



Georgia Cyber Center

- Located on Nathan Deal Campus for Innovation in Augusta, GA
- Hull-McKnight Building dedicated on July 10th 2018
- Shaffer MacCartney Building under construction set to open Dec 2018
- \$100M investment by SOG to promote cybersecurity growth in Georgia
- Augusta, GA is also home to U.S. Army Cyber Command, Cyber School of Excellence at Ft. Gordon, NSA at Ft. Gordon



Georgia Cyber Center

- Provides certificate, undergraduate & graduate education programs
- Georgia Cyber Range hands-on training facility
- Other tenants at the facility include
 - Georgia Bureau of Investigation
 - Incubation and accelerator programs
 - Demonstration space
- Benefits to DHS
 - Advanced cybersecurity training and certification
 - Use of the Cyber Test Range to better understand threat scenarios and improve defenses
 - Utilize cyber forensics capability at GBI and Augusta Univ labs located onsite



The Path to Stronger Security

- **Promote additional Security Awareness messaging to all staff**
- **Promote adherence to established procedures**
- **Promote a stronger security culture throughout DHS**



Resources

- Password Strength Test

<https://howsecureismypassword.net/>

- Online Password Generator

<https://www.dashlane.com/features/password-generator>

- NIST Online Quiz

<https://www.nist.gov/quiz/are-you-safe-online>



Appendix - Types of Phishing

- **Deceptive**

- Hackers send emails to users that appear to be from a trustworthy source such as a legitimate company, the government, a bank, or IT department.
- Email is designed to manipulate the end user into providing sensitive information such as account logins, and other personal information

- **Spear Phishing**

- Similar to deceptive phishing, except rather than sending out emails to many users, specific users are targeted.
- Hackers craft targeted emails by researching the users through social media, and other research methods.

- **Whaling**

- Similar to spear phishing but instead hackers target senior executives. These emails are highly customized and usually take the form of customer complaints, legal subpoena, or executive issues.





Georgia Department of Human Services
Office of Information Technology

Thank You !

**Venkat R. Krishnan, Randy
Coleburn & Shirlan Johnson**

Venkat.Krishnan@dhs.ga.gov
Randy.Coleburn@dhs.ga.gov
Shirlan.Johnson@dhs.ga.gov