



ISACA GEEK WEEK 2016
Workforce Development – Cyber
Workforce
August 2016

Introduction and Overview

Stanton Gatewood

State of Georgia - CISO

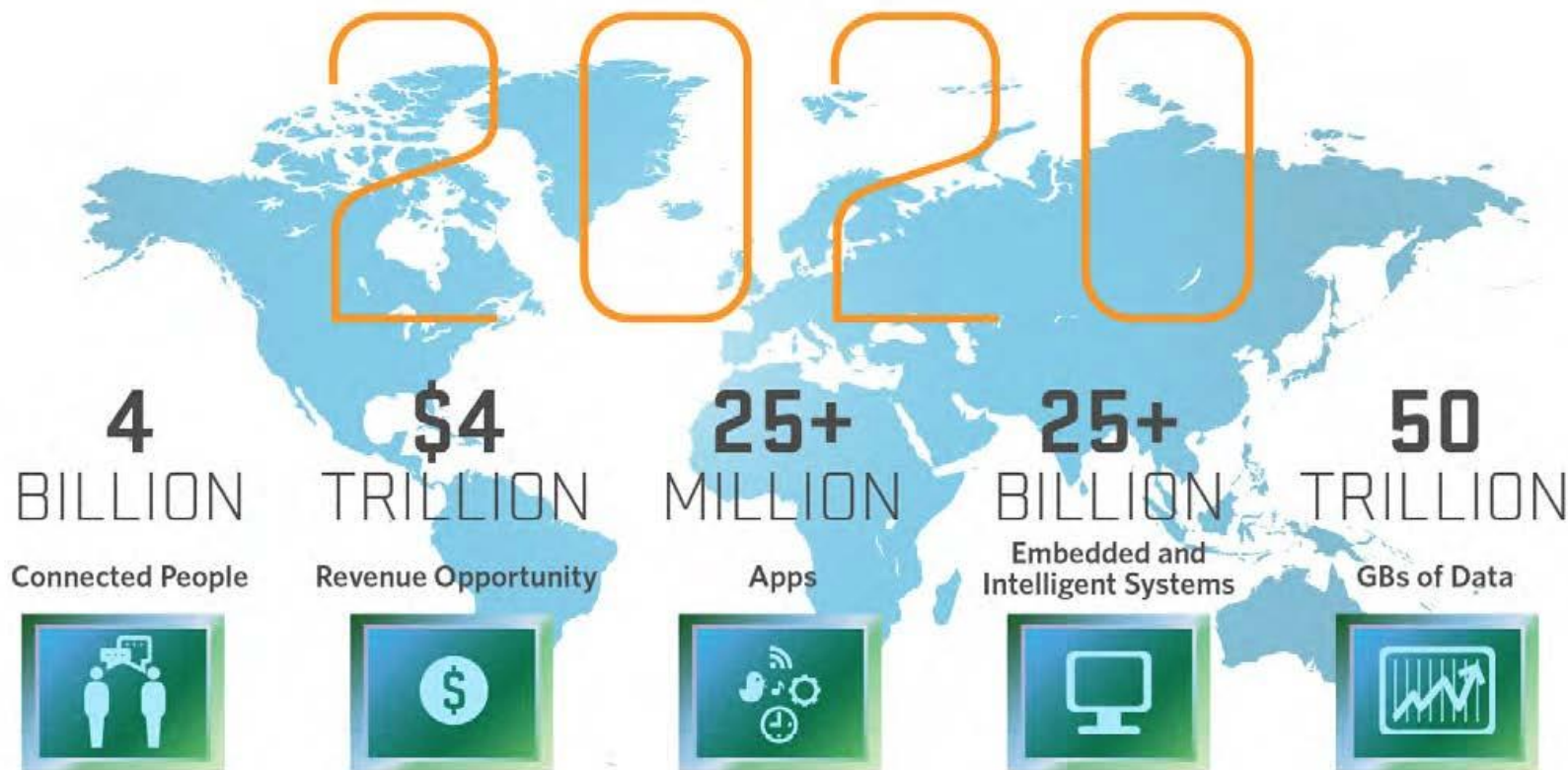
- Teacher, researcher, cryptographer, CISO and USAF flight engineer & Crypto-Officer
- 30+ years in cybersecurity – physical security, logical security and human-element security
- Trained and Educated in Teaching, Cyber Security, e-Privacy and a
- TEDx speaker

Internet Stats

- Internet
 - Around 40% of the world population has an internet connection today.
 - In 1995, it was less than 1%.
 - The number of internet users has increased tenfold from 1999 to 2013.
 - The **first billion** was reached in 2005. The **second billion** in 2010. The **third billion** in 2014.

* 7.4 billion (what's this?)

Unstoppable Growth...



Source: Mario Morales, IDC.

Cybercrime

- Stats & Trends
 - The estimated annual cost over global cybercrime is 100 BILLION
 - Yearly cyber crime victim count estimate:
 - Victims per year – 556 million
 - Victims per day – Over 1.5 million
 - Victims per second – 18
 - Identities exposed – More than 232.4 million

By the numbers...

EDU, GOV and MED

Year: 2016

2,735,649 Records

73 Breaches made public

- Jan-Jun ONLY

Since 2005

899,299,646 RECORDS BREACHED
from 4,881 DATA BREACHES made public since
2005

The Situation

- The US workforce lacks cybersecurity experts.
- Many cybersecurity training programs exist but lack consistency among programs.
- Potential employees lack knowledge, skills and abilities.
- Resources exist for teachers and students about cybersecurity but are difficult to find.
- Cybersecurity career development and scholarships are available but uncoordinated.
- Lack of communication between government, private industry, and academia.

There is a shortage of qualified cyber-workers, now and in the foreseeable future...

“The shortage stems from a variety of factors, such as high: experience requirements, “flash-to-Bang” period too long, an aging security workforce and a lack of interest from high school or college-level students...”

Gatewood, State CISO

“The Known; Unknown...”

In the last five to seven years there's been a dramatic surge in advanced threats and malware; much of it is more sophisticated than reasonable security practices and procedures driven by today's best practices.

There is an unprecedented demand for highly-skilled practitioners capable of building security into new and existing networks, assessing security on a real time basis as new vulnerabilities are identified and disclosed, and acting as front-line cyber defenders across various industries and government agencies.

Meanwhile, the number of entrants into the IT workforce has not kept up with this demand , leaving a significant gap in capacity to adequately protect these networks from attack.

At the same time, the lack of clarity and consistency in job profiles, competency models, skills assessment and workforce management contribute to a sub-optimal deployment of these scarce resources.

Specifically, we need...

High-value skills are in critically short supply, the most scarce being intrusion detection, secure software development, advanced analytics experience or analytical-thinkers and attack mitigation.

Workforce Development:

“Cyber Workforce Development”

NEW Cyber Workforce

- Clearly defined cybersecurity roles
- Clear, specific, & realistic job requirements
- Standardized skills & training
- Redefine minimum credentials for entry-level cybersecurity jobs: accept non-traditional sources of education
- Diversify the cybersecurity field
- Provide more opportunities for external training
- Identify technology that can provide intelligent security automation
- Collect attack data and develop better metrics to quickly identify threats
- Qualified cyber defenders to fill 2.5 million new cybersecurity positions

Vision: Cyber Workforce



Educators Align programs to specific jobs



Students Graduate with marketable knowledge & skills



Employers Recruit from more qualified candidates



Employees Have defined career paths & opportunities



Policy makers Set standards to promote the workforce

We Need...

- Systems Operations Professional
- Data Administrator
- Computer Network Defense (CND) Specialist
- Digital Forensics and Incident Response Analyst
- Information Security Auditor
- Information Systems Security Officer
- Information Systems Security Manager
- Information Security Architect
- Risk and Vulnerability Analyst
- Software Developer
- Information Systems Security Engineer
- Strategic Planning and Policy Development Professional
- Chief Information Security Officer (CISO)
- Advanced Analytics:
 - Predictive Analysis
 - Behavioral Analyst
 - Threat Analyst

The State of Georgia

Cyber Academy

Oct 2016

Focus

- First 18 months
 - Standardize job descriptions
 - Standardize duties, roles and responsibilities
 - Build KSAs (knowledge, skills and abilities)
- First 24 months – focus on ISOs and CISOs in the public sector
 - ISO and CISO in the Public Sector
 - Building an Cybersecurity Program in the Public Sector
 - Security Governance in the Public Sector
 - Policy and Compliance in the Public Sector
 - IT/IS Risk Management
 - Cyber Incident Management
 - Security Awareness, Training, Education and Professional Development
 - Continuity of Operations Planning
 - Cyber Protection Team – CPT
 - Security Analyst Training
- Instructor-Led and vILT
- Partner with: University System, Technical Colleges, Georgia Guard and Certification Organizations
- Collaborate with: Local, state and federal law enforcement

Summary...

- A lot more of the basics should be taught in high schools as a path for those who are interested in the field, and A+ & Security+ certifications could certainly be completed via online courses.
- More advanced training—anything requiring students to use and interact with IT equipment—would still need to take place in labs, and I don't think America's high schools are outfitted for that kind of work at this time.
- Focus on advanced IT skill development.
- Look toward the “military”.



National Cyber Security
Awareness Month

Closing Remarks

Awareness and Preparedness are the
Keys...