2017
Iowa Cyber Alliance Symposium

MG Tim Orr
Adjutant General, Iowa National Guard
"Information security is a major priority at this company. We’ve done a lot of stupid things we’d like to keep secret."
Answering the President’s Call to Defend and Protect Our Nation’s Information Networks.

“President Obama recently pledged to make securing the country’s most vital computer networks a top economic and national security priority. In doing so, he called for greater leadership and collaboration to improve the safety of information networks that power the government and the U.S. economy. Iowa – with its vast resources of federal & state facilities, academic institutions, industry strengths and intellectual capital– is answering the President’s call to action.”
“So, Why Are We Here Today?”

- Network, Communicate and Collaborate among a variety of public and private sectors face to face.
- Advance the July 2016 Iowa Cyber Security Strategy forward
- Establish a group of professionals to advance Iowa in information security literacy, education, exercises, competitions and research
- Identify stakeholders to develop a plan for cybersecurity education
- Create a collaborative with Iowa’s community colleges and universities
- Develop one or more career pathways for cybersecurity careers in Iowa
- Secure instructional resources for a world-class cybersecurity initiative
- BLUF – Safe guard our citizens which includes protection from cyber threats.
Lieutenant Governor
Kim Reynolds

Opening Comments
MG Tim Orr
Opening Comments

“I’m no expert, but I think it’s some kind of cyber attack!”

“Possible security breach, sir. It’s the smart bombs. They know too much.”
Problems/Trends

• Data breach on Anthem, Inc. Health Insurance that exposed the personal information of 80 million subscribers

• Attack on Home Depot that revealed 56 million customer’s credit card information

• A malware infection that yielded customer information for 395 Dairy Queen restaurants

• An IRS attack that resulted in $50 million in fraudulent tax returns

• In 2014, 60 percent of targeted attacks struck small-and medium sized organizations

• Proposed Russian involvement in 2016 national elections
Background

• Coalition of State, Federal, Military and Private organizations came together for one day to conduct “First Cyber Security Summit.”

• Goal of symposium was to identify the Cyber Security stakeholders in the State of Iowa and find a path forward to protect the State of Iowa.

• Path-forward for the State of Iowa
  - Governor’s Executive Order
  - Cyber Security Strategy
Steps Taken

• Conducted Cyber Security Symposium #1 – January 2015

• Governor signed Executive Order #87
  - Establish a Governor’s Cyber Advisory Council (GCAC)
  - Draft and submit a State Cyber Security Strategy
  - Draft and submit a State of Iowa Cyber Incident Response Plan
  - Establish a long-range schedule of cyber related exercises that test the State's Cyber Incident Response Plan

• Participated/Conducted local/state/federal exercises/competitions

• Educational Initiatives
  - Iowa Cyber
  - Statewide ISERink
  - Cyber Defense Competitions
  - IT Olympics
  - Security Literacy Project

• Establishment of Army/Air National Guard Cyber Forces/Training

• Organize and conduct Iowa Cyber Alliance Symposium #2 – January 2017
What is the Future?

• Focus on Iowa State Cyber Strategy Sections/Action Plans
  • Awareness Training
  • Public Education and Communications
  • Collaboration
  • STEM

• Establish the Iowa Cyber Alliance Group to address information security literacy, education/research pathways, exercises & competitions, cyber security training, cyber security workforce, and cyber security collaboration opportunities.

• Taking Immediate Action Steps – Coalition Approach
Immediate Action Steps – Coalition Approach

1. Increase Knowledge—Develop a working knowledge of what cybersecurity is and the careers and jobs that are associated with cybersecurity/IT.

2. Review Current Practices—Identify the most relevant cyber education initiatives occurring in or around Iowa that may contribute in some way to the pathway development.

3. Secure Talent—Name a variety of education, corporate, business, government, and military representatives to share information associated with developing the pathway.

4. Identify Resources—Develop a manageable list of resources that can inform the development of the pathway.
Questions