Cybersecurity Awareness and Planning

Presented by the Agency of Digital Services

Information gathered from NASCIO

Who’s Responsible for Protecting State Data?

- Chief Information Officers
- Information Security Officers
- Agency Leaders
- Data Owners
- Employees
- Human Resources
- Legal Departments
- Third Party Contractors
- Elected Officials

Top Ten: State CIO Priorities for 2017

1. Security
2. Consolidation/Optimization
3. Cloud Services
4. Budget and Cost Control
5. Legacy Modernization
6. Enterprise IT Governance
7. Data Management and Analytics
8. Enterprise Vision and Roadmap for IT
9. Agile and Incremental Software Delivery

10.Broadband/Wireless Connectivity

Source: NASCIO State CIO ranking, November 2016

State Governments at Risk!

- States are attractive targets – data!
- More aggressive threats –
  - organized crime
  - ransomware
  - hacktivism
- Nation state attacks
  Critical infrastructure protection: disruption Insider threats – employees, contractors
- Data and services on the move: cloud and mobile Need for continuous training, awareness

What are these types of attacks?

- **Malware** is sometimes used broadly against government or corporate websites to gather guarded information,or to disrupt their operation in general. However, malware can be used against individuals to gain information such as personal identification numbers or details, bank or credit card numbers, and passwords
-
- **Brute force** is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using **brute force**) rather than employing intellectual strategies.
-
- A **phishing** website (sometimes called a "spoofed" site) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate website.

- https://en.wikipedia.org/wiki/Malware
- http://searchsecurity.techtarget.com/definition/brute-force-cracking
- https://safety.yahoo.com/Security/PHISHING-SITE.html

Malicious Attempts

During the preceding 12 months (Jan-Dec 2017) the State saw over 4 million malicious attempts to gain unauthorized access across a variety of attack vectors. The top 3 were:

Phishing URL's (1,577,284)

Brute Force Attacks (1,391,206)

Malware (366,587)