Public Sector IT Leaders’ Priorities

State & County CIOs

1. Cybersecurity
2. Cloud Services
3. Consolidation
4. Wireless Connectivity
5. Cost Control Items
6. Talent Management
7. Strategic Planning

Local Gov’t CIOs

1. Financial Transparency
2. Mobility Apps
3. Cybersecurity
4. IT Staffing
5. BCDR
6. Broadband
7. Cloud Computing
Mandated Cybersecurity Training Each Year

½ Hour In Addition To Ethics Requirements
WHO ARE THE BAD GUYS?

Professional Mercenary (Cyber Criminals)
Cyber Warrior (Nation States)
Principled Idealist
Malicious Insiders
Nationalist (Script Kiddies)

WHAT ARE THEIR TACTICS?

SQL Injection Exfiltration of data
BotNet DoS, Spam, Sniffers
Phishing Malware, steal passwords
Infected Websites Malware, ransomware
Copying Data
4 To 10 Million Attacks Per Month
Identify
Protect
Detect
Respond
Recover
SOCIAL ENGINEERING
IRS HACK SHOWS GOVERNMENT SAFEGUARDS NOT UP TO DATE!

APPLE IPHONES AND IPADS VULNERABLE TO FAKE APP ATTACK!

WireLurker
ransomware

Don’t open attachments or follow links in e-mails from people or organizations you don’t recognize.
Beware of strange e-mails even from people you do know.

Only visit websites you have a business reason to access.

Install the latest anti-virus and/or anti-malware applications and verify they are pulling updates.
Scan your devices at least weekly.

Participate in “Tues-stay Safe” at work.

Don’t ignore the browser’s or anti-virus software’s warning about a potentially harmful site.