



STATEWIDE INTERNET




PORTAL AUTHORITY

Cyber Threats:
Considerations from the Data Center to the Boardroom



Mike Whatley
Chief Technology Officer
(720) 409-4632
mike@csipa.gov



Telling the Cybersecurity Story

- What is Cyber Security?
- Who are the “bad guys”?
- What are the fastest growing threats?
- What should municipal leadership consider?

STATEWIDE INTERNET PORTAL AUTHORITY



Who are the bad guys?




STATEWIDE INTERNET PORTAL AUTHORITY



Where are they?




STATEWIDE INTERNET PORTAL AUTHORITY



Ransomware

- Malware that inhibits endpoint operation of systems.
- Ransomware was a billion dollar industry in 2016.
- Growth of attacks from 2015 to 2016:
 - 3.2 M → 638 M (167x) (SonicWall Global Response Int. Grid)
- Ransom is requested to be paid in bitcoin – a digital currency.
- How do I protect against ransomware?

STATEWIDE INTERNET PORTAL AUTHORITY



Protection Strategies

- Prevention Efforts
 - Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
 - Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
 - Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
 - Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
 - Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
 - Disable macro scripts from office files transmitted over e-mail.
 - Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular internet browsers, compression/decompression programs).
- Business Continuity Efforts
 - Back up data regularly and verify the integrity of those backups regularly.
 - Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

STATEWIDE INTERNET PORTAL AUTHORITY



Leadership Considerations

- What is your risk appetite?
- There is a difference between security and compliance.
 - Compliance does not equal security, it's a snapshot of security meets requirements in a given moment of time.
- Cybersecurity is not an IT issue alone.
 - Board members have a fiduciary responsibility.
 - Recent study by Eisner Amper indicates that board directors are most worried about cyber security risk (70%) and reputational risk (65%).
 - Costs are increasing → EU's Data Protection Directorate stipulates fines of up to 5% of a companies global revenue.
 - Cyber security insurance helps but it may not be enough.

STATEWIDE INTERNET PORTAL AUTHORITY



Summary

- Cybersecurity continues to evolve.
- Cybersecurity is a business reality.
- Anticipate and confront security incidents.
- Identify, Protect, Detect, Respond, Recover

STATEWIDE INTERNET PORTAL AUTHORITY



720-409-5634



sipa@cosipa.gov



@ColoradoSIPA



facebook.com/ColoradoSipa



Statewide Internet Portal Authority

www.colorado.gov/sipa

STATEWIDE INTERNET PORTAL AUTHORITY
