National Conference & Public Power Expo

June 15-20, 2018 • New Orleans, Louisiana

Explore Together

Assess and Act: Build Your Cybersecurity Program

APPA National Conference
June 18, 2018, New Orleans, LA

Kevin Gertig
Executive Director
City of Fort Collins Utilities
kgertig@fcgov.com
(970)416-2232

Karen St.Clair
IT Manager
Columbia Power and Water Systems
karen.stclair@cpws.com
(931)375-7604

A little about us…
City of Fort Collins Utilities

•Fort Collins Utilities is committed to a cleaner environment, affordable electric bills, and a highly reliable energy system.

- Over 99% of the Fort Collins System is underground.
- Deployed Advanced Metering Infrastructure 5 years ago.
- Second Largest municipal electric utility in Colorado
- Strong energy conservation program.
- 70,500 metered accounts
- Serve a population of ~172,000
- Power Provider is Platte River Power Authority which is jointly owned by the Cities of Fort Collins, Loveland, Longmont, and Estes Park CO.
- Received a 100% score on APPA RP3 in 2014

A little about us…
Columbia Power and Water Systems

- Deployed Advanced Metering Infrastructure 9 years ago.
- 50,300 metered accounts
- Serve a population of ~ 88,000
- Power Provider is Tennessee Valley Authority
- Received Diamond designation level - APPA RP3 in 2016

The Importance of Addressing Cyber Risk

A Utility's primary objectives are to keep critical services running, safety, and possibly expand services.

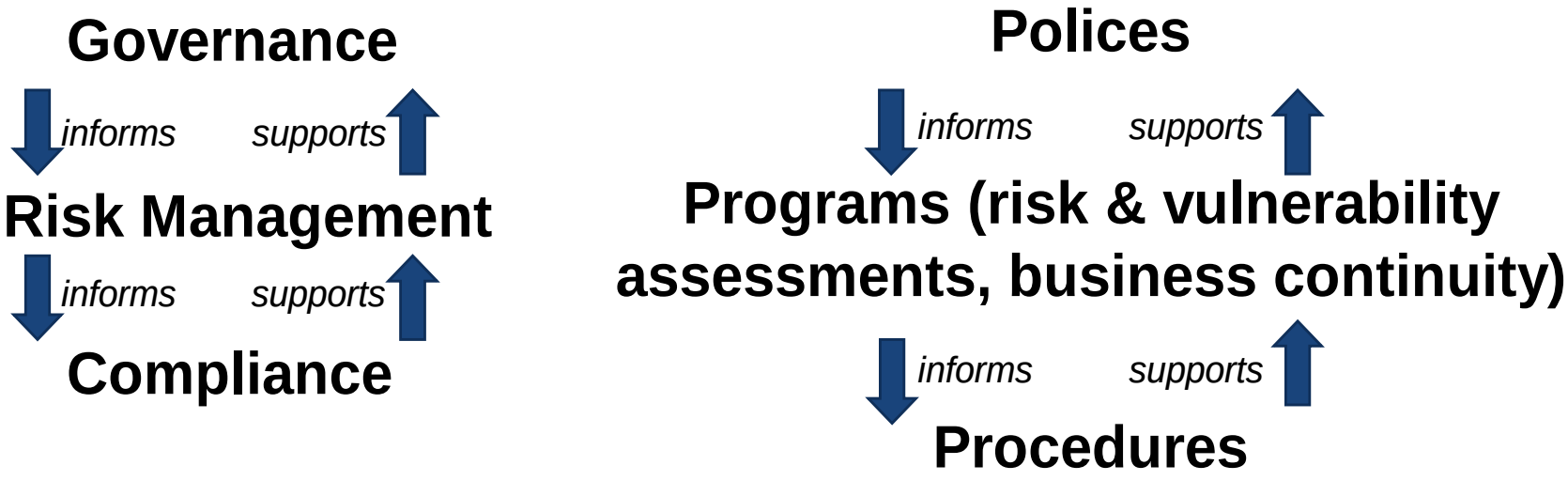
Addressing cyber risk is one method of mitigating potential barriers to reaching your goals, and can potentially aid in achieving them.

Cybersecurity & Privacy Program Design & Deployment

NIST Framework for Improving Critical Infrastructure Cybersecurity

Risk Assessment + Gap Analysis → Roadmap

GRC



Developing a Comprehensive and Sustainable Program

1. Know what you have
2. Know what is most important
3. Perform an initial risk assessment
4. Establish governance
5. Use the NIST Cybersecurity Framework to determine current state and desired future state → roadmap
6. Schedule & allocate resources for vulnerability assessments & remediation work
7. Don’t get overwhelmed! Focus on making progress.
8. Communicate!!

Training Governance & Staff

Organizational Change Management !!!

- Tie cybersecurity/privacy directly to strategic objectives
- Ensure policies and supporting documentation are easily available to staff and that they are regularly reviewed
- Build it into standing meeting agendas
- Build it into job descriptions and tie it to performance reviews
- Enlist your public communications department
- Phishing, Privacy, and Awareness training programs

Threats

Cybersecurity (including privacy) must be an ongoing effort due to our increasing reliance on data networks combined with the evolving sophistication of attacks.

- Most common threats
  - Natural - severe weather knocking out network & communication infrastructure
  - Outsiders - nation-states executing cyber/physical attacks, organized crime seeking financial gain
  - Insiders - especially accidental incidents are a constant threat
- Most common threat vectors
  - In general, email is #1 by far
  - For ICS worldwide, the internet leads (22%), followed by removable media (9%) and email (3.9)
- Most common attacks
  - Worldwide, the vast majority are Trojans and Trojan Downloaders (32%). Worms are next (4.4%)

Threats (cont.)

- Most damaging attacks
  - Those that cause physical damage or disrupt community safety
  - Those that disrupt mission critical operations
  - Those that impose severe financial hardship. Example: A breach of personal customer information costs an average of $228 per compromised record in the US energy industry.
- New and emerging attack techniques
  - Repositories & cloud storage data leakage *e.g., advanced metering data, customer data*
  - Ransomware *e.g., CryptoLocker, WannaCry*
  - Big data de-anonymization and correlation *e.g., advanced metering data*
  - Attacks on industrial control systems to disrupt critical infrastructure
  - Cryptocurrency mining or cryptojacking *resource consumption disrupts monitoring tools and system performance.*
  - Hardware flaws *very difficult to patch without entire system replacement or major performance hits*

Identifying Cyber and Privacy Risks

The risk assessment provides the information necessary to prioritize security efforts.

1. Determine a schedule
   - o Recommended frequency: annually
   - o Practical frequency: balance resources among risk assessments, vulnerability assessments, mitigation/remediation efforts, operations, and the pace of change in your environment.
2. Determine a methodology
   - o What can go wrong?
   - o What is the likelihood that it would go wrong?
   - o What are the consequences?
   - o NIST SP 800-30 r1 Guide for Conducting Risk Assessments

Identifying Cyber and Privacy Risks (cont.)

Keep on eye on ISACs, annual security reports, security organizations, and standards.

Examples

ISACs	Annual Reports	Security Organizations	Standard Updates
ICS-ISAC	Verizon Data Breach Investigations Report	SANS	NIST 800 series
MS-ISAC	Cisco Annual Cybersecurity Report	CIS	CIC CSC
E-ISAC	Ponemon/IBM Cost of Data Breach Study	ICS-CERT	NERC CIP

Vulnerability Assessments

Vulnerability assessment - A vulnerability assessment is a search for these weaknesses/exposures in order to apply a patch or fix to prevent a compromise. (SANS)

1. Determine the data and systems most critical to operations
   a. Know your systems' tolerance of vulnerability assessments
2. Rotate those systems through vulnerability assessments
3. Once the critical systems have been assessed and vulnerabilities mitigated/remediated, perform an overall vulnerability assessment to catch integrated systems
4. Repeat

Intrusion Detection

As defined by SANS, intrusion detection provides:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis – including notification of abnormal activities
- Operating system audit

Reliability & Preparedness

- Continuity of Operations Plan (COOP)
- Business Continuity *Prioritize based on your most important operations*
  - Operational contingency procedures
  - Incident response
  - Disaster recovery
- Know your resources *"Who ya' gonna call?"*
- Recommendation: National Incident Management System (NIMS)

PRACTICE!

Advanced Metering Infrastructure Security & Privacy

- Concern: Big data de-anonymization and correlation
  - o a.k.a. Re-identification
  - o Once you have usage data, everyone will want it. Have a plan for how it will be used/shared prior to gathering it.
- Concern: Wireless communication interception & system security
  - o Include a robust security section in your RFPs and make this a go/no-go item
  - o Perform a vulnerability assessment and penetration test as soon as possible – from the meter to the database, perhaps further (follow the data)

The Latest

- Privacy –more focus on securing data, not just systems
  - Data classification
  - Data loss protection (DLP)
  - GDPR-like expectations from customers
- Security – more focus on securing “things”, ICS security is starting to include more traditional IT controls like test environments and patching

Resources

- https://www.sans.org/reading-room/whitepapers/basics/vulnerability-assessment-421
- https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337