NJ WATER ASSOCIATION

CYBER SECURITY FOR WATER AND WASTEWATER UTILITIES

PRESENTED BY: JAMES SCHAEFER, PE

SUBURBAN CONSULTING ENGINEERS, INC.

Cyber Security – A Hot Topic

- Recent Equifax data leak
- Russian and Chinese cyber attacks
- Data breaches at various retailers and credit card companies

Earlier Cyber Security Efforts

- Early 2000's – Risk Assessment Methodology for Water (RAM-W)
  - Required by US EPA, based on cybersecurity work by Sandia Labs
  - Threat and vulnerability assessments
  - Consequences
  - Risk assessment and emergency response plan
- 2010 AWWA Standard J100
  - Uses RAMCAP™ (Risk Analysis & Management for Critical Asset Protection)
  - Risk and resilience analysis and management
  - Identify vulnerabilities – threats, natural hazards, and dependencies
  - Methods to evaluate options for addressing weaknesses
  - Focus on significant threats

New Jersey Requirements for Utilities

- Water Quality Accountability Act (NJSA 58:31-1 *et seq*)
- 2016 BPU Utility Cyber Security Program (Docket No. AO160300196)

Water Quality Accountability Act (NJSA 58:31-1 *et seq*)

- Water purveyors with > 500 service connections and internet connected controls system(s)
- Effective date: October 19, 2017
- By January 17, 2018 develop Cyber Security Program (Based on BPU requirements)
  - Cyber risk management responsibilities & accountabilities
  - Establish plans, policies, etc. to minimize cyber risk
  - Conduct risk assessments, implement controls to mitigate risks, maintain situational awareness, create and exercise incident response and recovery plans

2016 BPU Cyber Security Program

- Provide a copy of program to NJ Cybersecurity and Communications Integration Cell (NJCCIC)
- Join NJCCIC within 60 Days of developing the cybersecurity program
- 2016 BPU Requirements
  - Applies to utilities regulated by the BPU
  - Develop Cyber Security Program
    - Cyber Risk Management
    - Situational Awareness
    - Incident Reporting
    - Response and Recovery
    - Security Awareness & Training

Implementation of BPU Regulation

- Effective Date: March 28, 2016
- Join NJCCIC, by May 27, 2016
- Submit a report on organizational oversight, capabilities and responsibilities for cyber risk management by June 1, 2016,
- Submit a progress report by December 31, 2016
- Submit written certification of compliance, by October 31, 2017

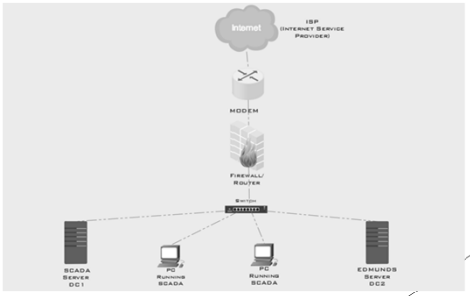
Areas of Concern

- Customer Information
- Personal Information of Your Staff
- E-mail System
- Operating Data
- Operating Control
- Cloud-Based Computing vs. On-site Hardware

Approaches for Handling Security

- Equipment – Hardware & Software
- Physical Security
- Organization
- Staff Training
  - Handling of Unsolicited Files
  - Passwords
  - Turning-off Equipment
  - Limiting Physical Access

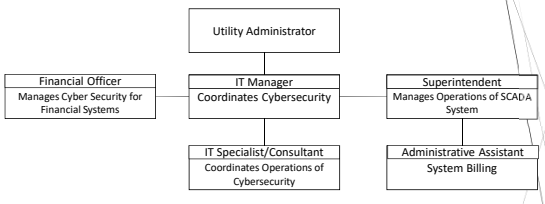
TYPICAL NETWORK INFRASTRUCTURE



Physical Security

- Lock rooms/areas that house servers and phone equipment
- Limit access to authorized personnel

TYPICAL ORGANIZATION



Staff Training

- Provide regular training for staff
  - Laws/Regulations
  - Utility company requirements
  - How to handle spam and other unwanted e-mail
  - Passwords
    - Complexity
    - Frequency of Changing

Best Practices

- Physical Security
- Access
- Passwords
- Training
- System Maintenance

Access

- Provide each employee with appropriate credentials to access systems and limit their access to subsystems
- Compartmentalize your cyber information
  - Customer vs. Staff vs. Operations
- Limit on-line access to parts of you system

Passwords

- Require very strong passwords
  - 10 digits, upper and lower-case letters, numbers and symbols
- Change them regularly

System Maintenance

- Provide regular training for staff about laws/regulations
  - Best Practices
  - New Equipment / Procedures
  - Maintain Security of Passwords
- Vet and install programming updates and patches ASAP

Other Resources for Security Ideas

- WaterISAC – Water Security Network
  - Organization of water sector professionals
  - Focuses on vulnerability and security of all types
- GMIS-NJ (Government Management Information Sciences)
  - Association to improve MIS services in government
  - Security is one area of focus

CONCLUSIONS

- Cyber security is an increasing threat to utilities
- Legislation and regulations currently require higher levels of protection for larger utilities
- Need for better protection will be extended to smaller systems, and possibly wastewater systems, over the coming years
- Effective cyber security risk management has several elements
  - Organization
  - Situational Awareness
  - Incident Reporting
  - Response and Recovery
  - Security Awareness & Training
- Start planning and developing your program ASAP

QUESTIONS?

Presenter:
James K. Schaefer, PE