CYBER SECURITY FOR WATER AND WASTEWATER UTILITIES

PRESENTED BY: DAVID A. CHANDA, PE

SUBURBAN CONSULTING ENGINEERS, INC.

Cyber Security – A Hot Topic

SUBURBAN CONSULTING ENGINEERS, INC.

- NotPetya Cyberattack
- 2018 Thales Data Threat Report
- “Tempting Cedar Spyware”

Implementation Origins

SUBURBAN CONSULTING ENGINEERS, INC.

- 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 and resilience analysis and management
  - Identify vulnerabilities – threats, natural hazards
  - Methods to evaluate options for addressing weaknesses
  - Focus on significant threats

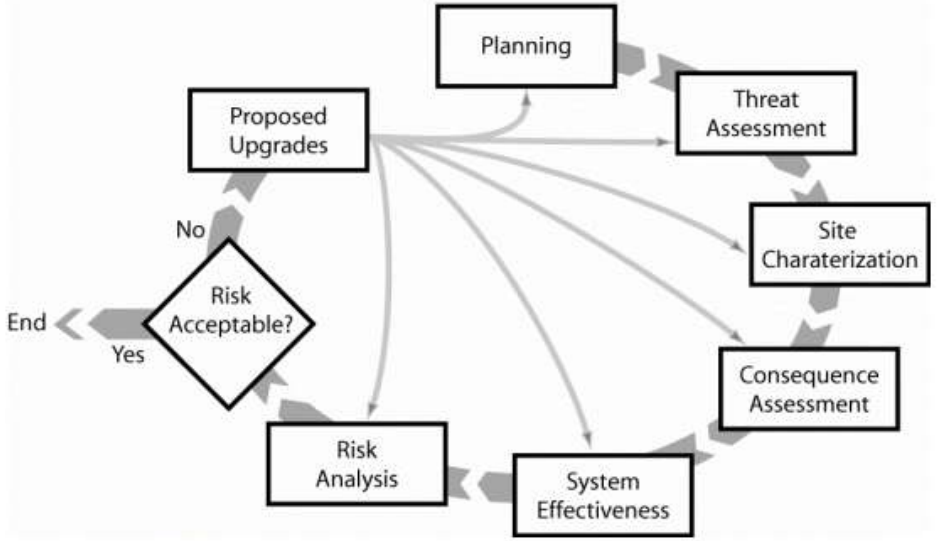


Figure 1 *RAM-W™ Process*

New Jersey Requirements for Utilities

SUBURBAN CONSULTING ENGINEERS, INC.

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

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

SUBURBAN CONSULTING ENGINEERS, INC.

- Water purveyors with > 500 service connections and “internet connected controls system(s)”
- Effective date: October 19, 2017
- By February 16, 2018 develop a Cyber Security Program (Based on BPU requirements)

2018 WQAA Cyber Security Implementation

SUBURBAN CONSULTING ENGINEERS, INC.

- Provide a copy of program to NJ Cybersecurity and Communications Integration Cell (NJCCIC)
  - Due February 16, 2018

- Join NJCCIC within 60 Days of developing the cybersecurity program

- Cyber Security Program Requirements
  - Cyber Risk Management
  - Situational Awareness
  - Incident Reporting
  - Response and Recovery
  - Security Awareness & Training

Areas of Concern

SUBURBAN CONSULTING ENGINEERS, INC.

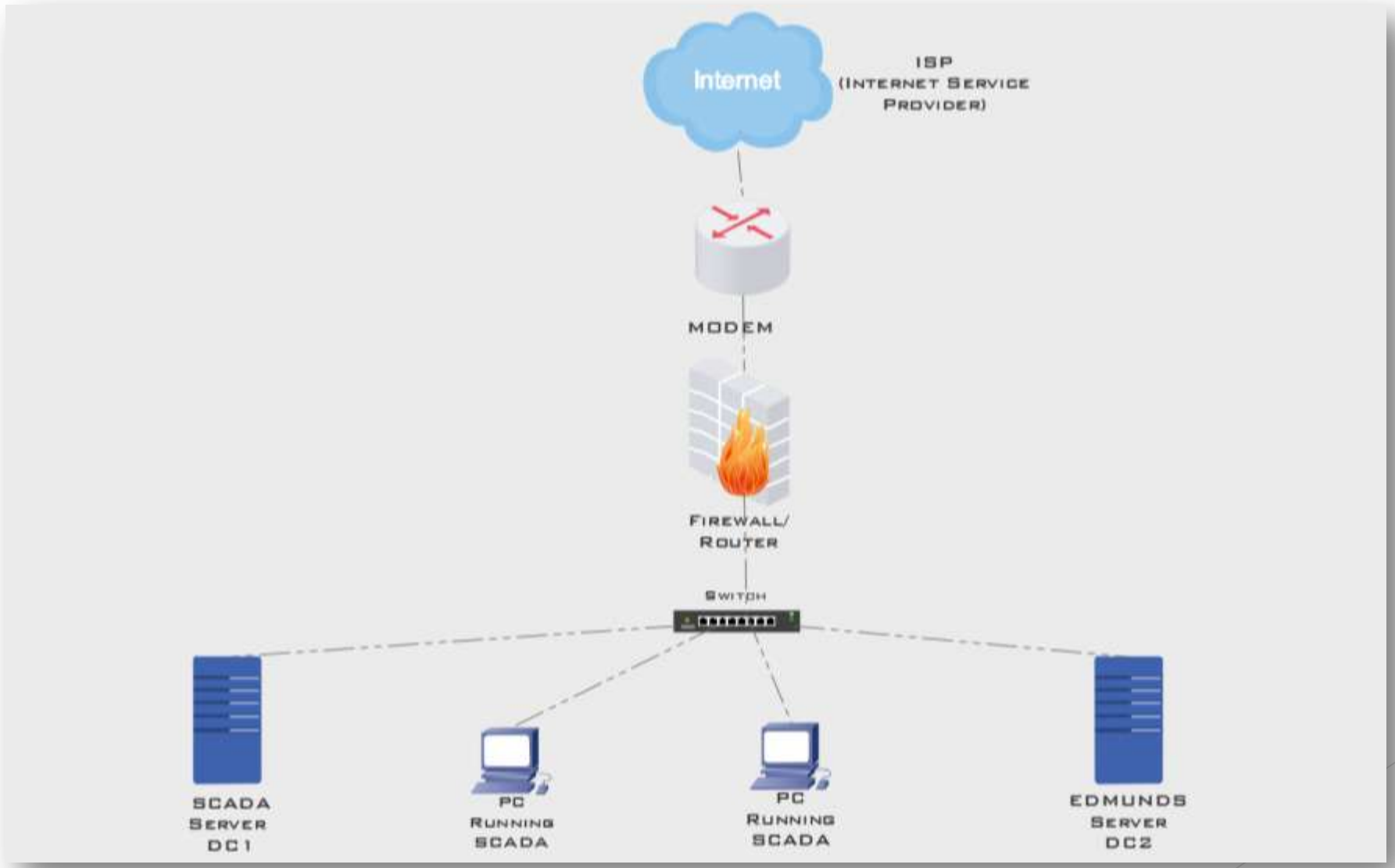
- Customer Information
- Staff Information
- E-mail System
- Operating Data
- Operating Control
- Cloud-Based Computing vs. On-site Hardware

Approaches for Handling Security

SUBURBAN CONSULTING ENGINEERS, INC.

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

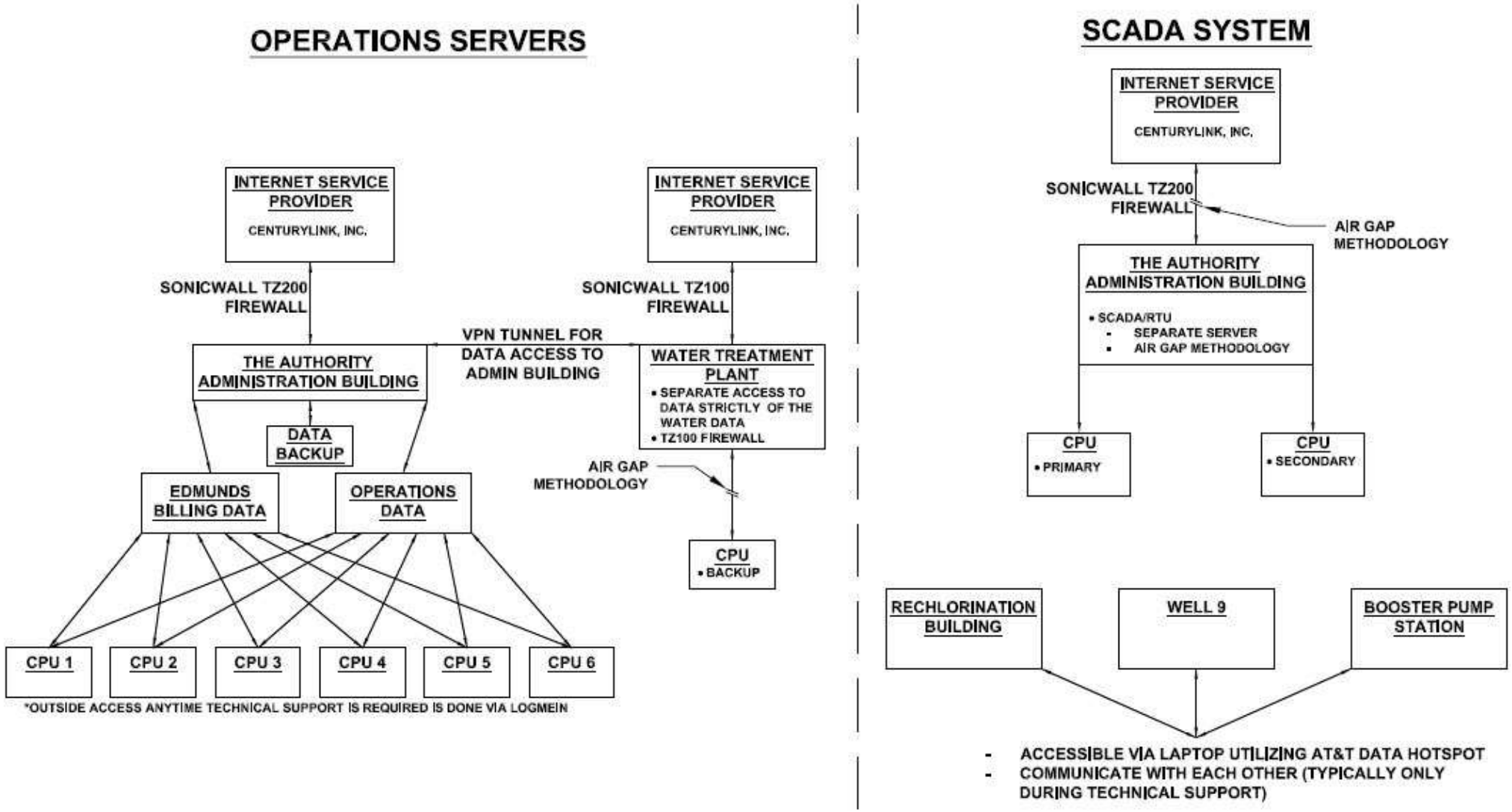
Typical Network Infrastructure



SUBURBAN CONSULTING ENGINEERS, INC.

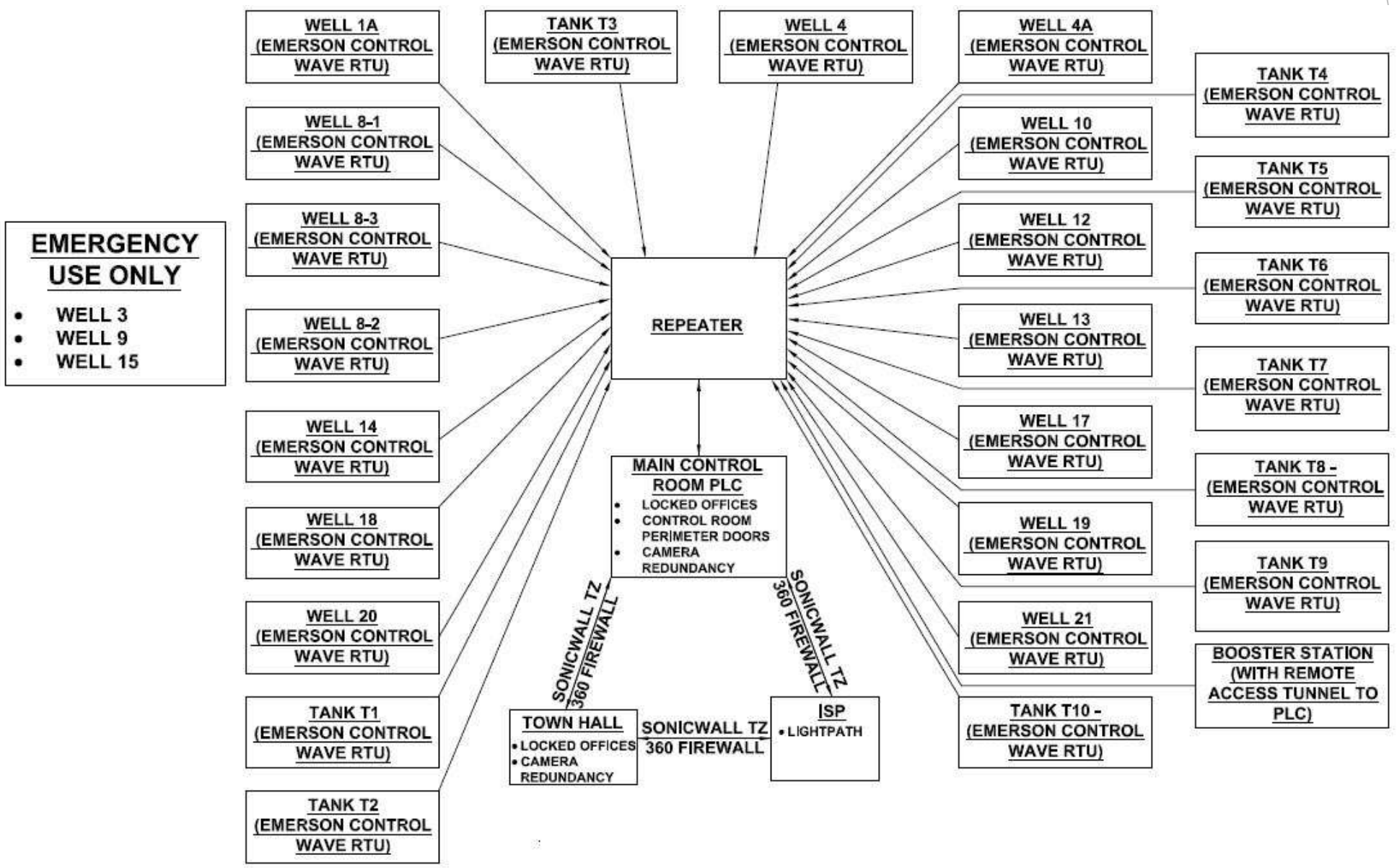
Typical Network Infrastructure – Cont.

SUBURBAN CONSULTING ENGINEERS, INC.



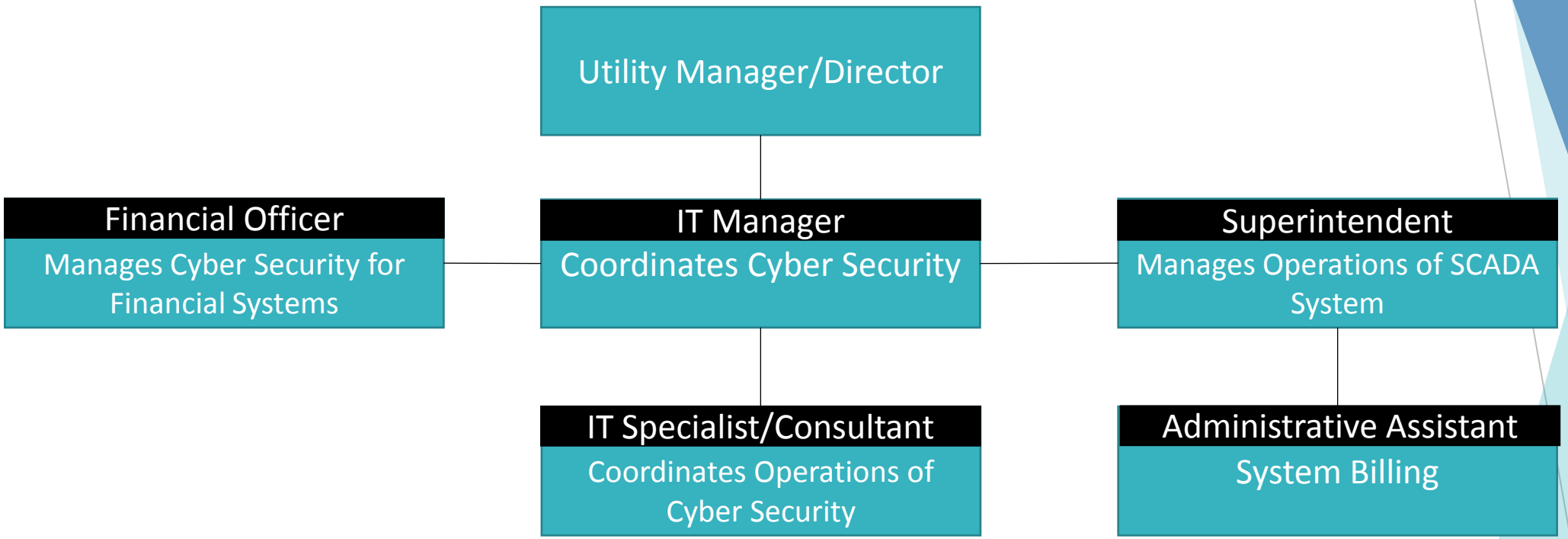
Typical Network Infrastructure – Cont.

SUBURBAN CONSULTING ENGINEERS, INC.



Typical Organization

SUBURBAN CONSULTING ENGINEERS, INC.



Monthly Requirements

SUBURBAN CONSULTING ENGINEERS, INC.

The IT specialist shall ……

- Monitor internal and external sources of threat and vulnerability
- Deliver critical alerts and notifications as they occur
- Maintain Executive Reports from Firewall including:
    - Threat Identification
    - Threat Protection
    - Intrusion Detection
    - Response Taken
    - Recovery Steps

Quarterly Requirements - Training

SUBURBAN CONSULTING ENGINEERS, INC.

The IT specialist shall train……

- Staff with access for potential pathways of threats
- New personnel

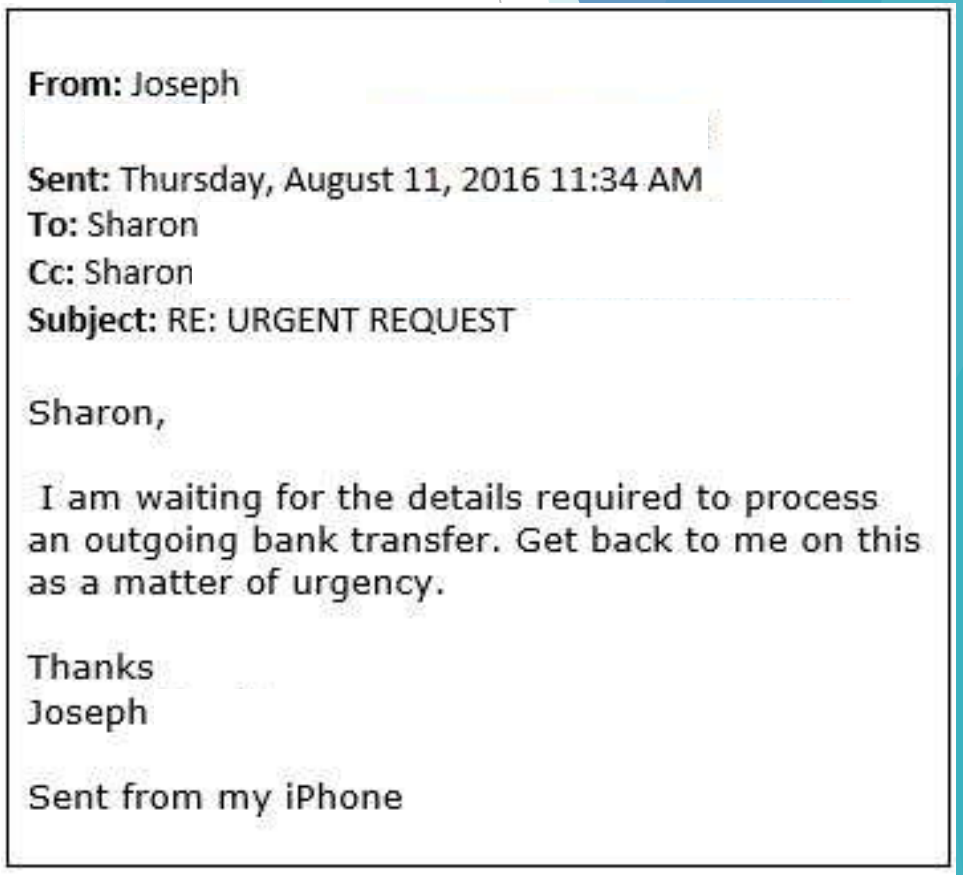
The IT specialist shall train on……

- Password management
  - Contain both upper- and lower-case letters (case sensitivity).
  - Contain one or more numerical digits.
  - Special characters, e.g. @, #, $ etc. can be included but are not required.
  - All passwords changed every 90 days
  - Recommended minimum of eight characters.

Quarterly Requirements – Training Cont.

SUBURBAN CONSULTING ENGINEERS, INC.

- Downloading unlicensed software.
- Accessing files remotely should be through a secure remote access service (VPN).
- Safe internet usage, recognize any cyberattacks and vulnerabilities, and avoid any suspicious emails.
- Trained to recognize a legitimate warning message or alert.
  - Employees should be trained to immediately report the incident so it can be investigated, and any threat reduced or removed.



From: Joseph

Sent: Thursday, August 11, 2016 11:34 AM
To: Sharon
Cc: Sharon
Subject: RE: URGENT REQUEST

Sharon,

I am waiting for the details required to process an outgoing bank transfer. Get back to me on this as a matter of urgency.

Thanks
Joseph

Sent from my iPhone

Long Term Requirements

SUBURBAN CONSULTING ENGINEERS, INC.

Annual Requirements

- Perform an annual inventory analysis of critical systems and document any changes from the system architecture as operated in the prior calendar year.
- Review risk assessment methodology as encountered in the prior calendar year.

24 Month Requirements

- Create a cyber risk assessment plan and conduct an exercise to the test the Plan every 24 months at a minimum.
- Establish a Cyber Security Incident Response Plan that follows through the life-cycle of an incident.

Other Resources for Security Ideas

- CSET – US Department of Homeland Security
  - Cyber Resilience Review (CRR)
    - Cyber Self Assessment

- WaterISAC – Water Security Network
  - Organization of water sector professionals
  - Focuses on vulnerability and security of all types

- New Jersey Office of Homeland Security and Preparedness
  - Currently Developing a checklist to determine “internet-connected control system” applicability.

SUBURBAN CONSULTING ENGINEERS, INC.

WaterISAC
Water Security Network

U.S. DEPARTMENT OF HOMELAND SECURITY

Conclusions

SUBURBAN CONSULTING ENGINEERS, INC.

- Cyber Security is an increasing threat to utilities
- Legislation and regulations currently require higher levels of protection for 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?

SUBURBAN CONSULTING ENGINEERS, INC.

Presenter:
David A. Chanda, PE