

25th ANNUAL NORTH CAROLINA PRETREATMENT CONSORTIUM CONFERENCE

Wastewater System Security Awareness

September 20, 2022

Presented by: Stephen Brown, P.E.

Acknowledgements: Robert L. Griffin, P.E. & Perry Gayle, P.E.

Introduction

Why the Need for Awareness?

What is Most Important?

Understand the Threats

Develop a Security Strategy

Operational and Physical
Security

Cybersecurity

Mitigation

Why do we need to be Aware?



The world is changing.



Why do we need to be Aware?

- Water tank intrusions
- Kids dumping mercury in a water tank
- Cyber intrusion
- Loss of intake
- Active assailant at a water plant
- Hurricanes
- Train derailment
- Other?

Past Incidents



Sewer Explosion – April 22, 1992

- 200+ dead
- 1,500+ injured
- 15,000+ homeless
- 1,000+ buildings destroyed or damaged

AP Associated Press

Bomb in Sewer Kills 30 in Algeria

*By Omar Ouali
Associated Press Writer*

ALGIERS, Algeria, July 5, 2002 — A bomb ripped through an open-air market bustling with morning shoppers Friday on Algeria's independence day, killing at least 30 people and wounding 36 others, the official APS news agency reported.

The bomb was hidden in the mouth of a sewer in a market in Larba, about 15 miles southeast of the capital, Algiers, witnesses said.

Past Incidents

Australia, 2000:
Intentional
release of
untreated sewage

- A former contract employee used insider knowledge to manipulate a SCADA system
- Caused pump station failure, resulting in overflow onto tourist resort and into storm sewers
- Sentenced to 2 years in prison and fined \$10,000 (US)

Past Incidents

2014
Elk River
chemical
spill



Freedom Industries Tank Farm

- Upstream of Charleston, WV water intake

<https://www.cfpua.org/CivicAlerts.aspx?AID=1018&ARC=2114>

<https://www.csb.gov/eq-hazardous-waste-plant-explosions-and-fire/>

https://en.wikipedia.org/wiki/2014_Elk_River_chemical_spill

What's Important To Your System?

Protect the Environment, Avoid Upsets

Maintain Public Confidence

Reduce Liability

Protect Employees

Maintain Service to all Critical Customers

Decisions Made with Utility as a Whole

Threats to Wastewater Systems

A threat is an event that may result in

- Harm to the public
- Damage or harm to a utility's physical, cyber, or human assets
- An upset or disruption to service or operations

Threats can be divided into three categories

- Natural threats
- Accidental (unintentional) threats
- Malevolent (intentional) threats

Threats to Wastewater Systems

Natural

- **Floods**
- **Windstorms**
- **Ice storms**
- **Snowstorms**
- **Fires**
- **Drought**
- **Earthquakes**



Greenville Utility Commission WTP after Hurricane Floyd, 1999

Threats to Wastewater Systems

Accidental (Unintentional)

- **Chemical spills**
- **Fires**
- **Transportation accidents**
- **Explosions**



Threats to Wastewater Systems

Malevolent (Intentional)

- **Threat actors**

- Vandals
- Criminals
- Insiders
- Terrorists

- **Threat types**

- Cyber
- Physical
- Chemical
- Biological



Wastewater Security Concerns

Wastewater security concerns include

- Physical destruction
- Illegal dumping of toxic chemicals or flammable substances in the collection system
- Release of chlorine gas or other toxics

Interruption in wastewater service can result in

- Widespread public health impacts
- Significant environmental damage

Malevolent Threats to Wastewater Systems

Spectrum of Components

- Motive
- Planning
- Knowledge
- Tools
- Weapons
- Intent to Harm

Types

- Vandal
- Criminal
- Saboteur
- Terrorist
- Insider
- Cyber

Malevolent Threats to Wastewater Systems

		Categories			
		Vandal	Criminal	Saboteur	Terrorist
Characteristics	Motivation	Thrill, dare	Financial gain	Political cause	Political cause
	Objective	Property damage	Theft	Disruption/destruction	Destruction and human casualties
	Planning	Little or none	Possible	Definite	Extensive
	Access	Stealth	Stealth	Stealth	Stealth or overt
	Weapons	None	Knife, pistol, rifle	Explosives	Assault weapons, explosives, RPGs
	Contaminants	None	Possible	Possible	Probable
	Asset damage	Minimal	Minimal	Significant	Extensive
	Injuries	None	Possible	Possible	Extensive
	Fatalities	None	Possible	Possible	Definite

Develop a Security Strategy

- Assess the threats and conduct a vulnerability assessment
- Apply the three approaches to the development of a balanced plan
 - Management of the utility
 - Operations and operational functions
 - Security design enhancements
- Build support for the strategy
 - Consider all potential drivers
 - Evaluate cost-risk reduction

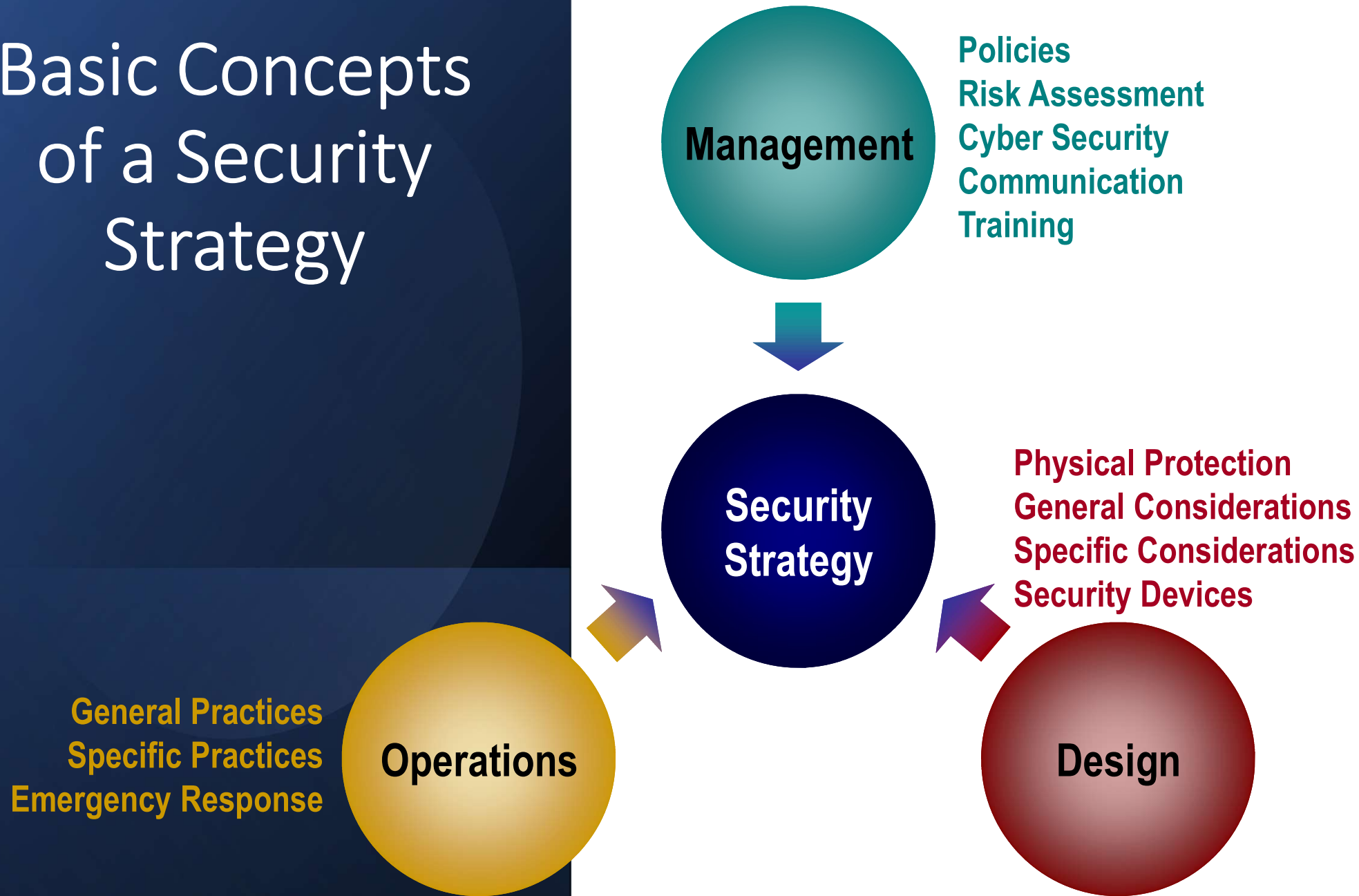
Vulnerability Assessments

Objectives of Vulnerability Assessments (VAs)

- Mission - What's Important?
- Identify threats
- Identify specific assets that may be impacted
- Determine the relative criticality of the utility's assets
- Determine the likelihood that a threat may materialize
- Evaluate existing countermeasures
- Analyze current risks

Do Not Randomly Approach Security Without a VA

Basic Concepts of a Security Strategy



Management Security

Facilitate improved security and reduce risks by:

- Informing the Governing Body and involving stakeholders
- Addressing organizational culture and engaging employees
- Updating policies and procedures
- Mitigating employee, visitor, and contractor risks
- Leveraging financial resources
- Managing sensitive records
- Planning for procurement
- Ensuring effective communication and coordination
- Securing information systems and other cyber networks

Operational Security



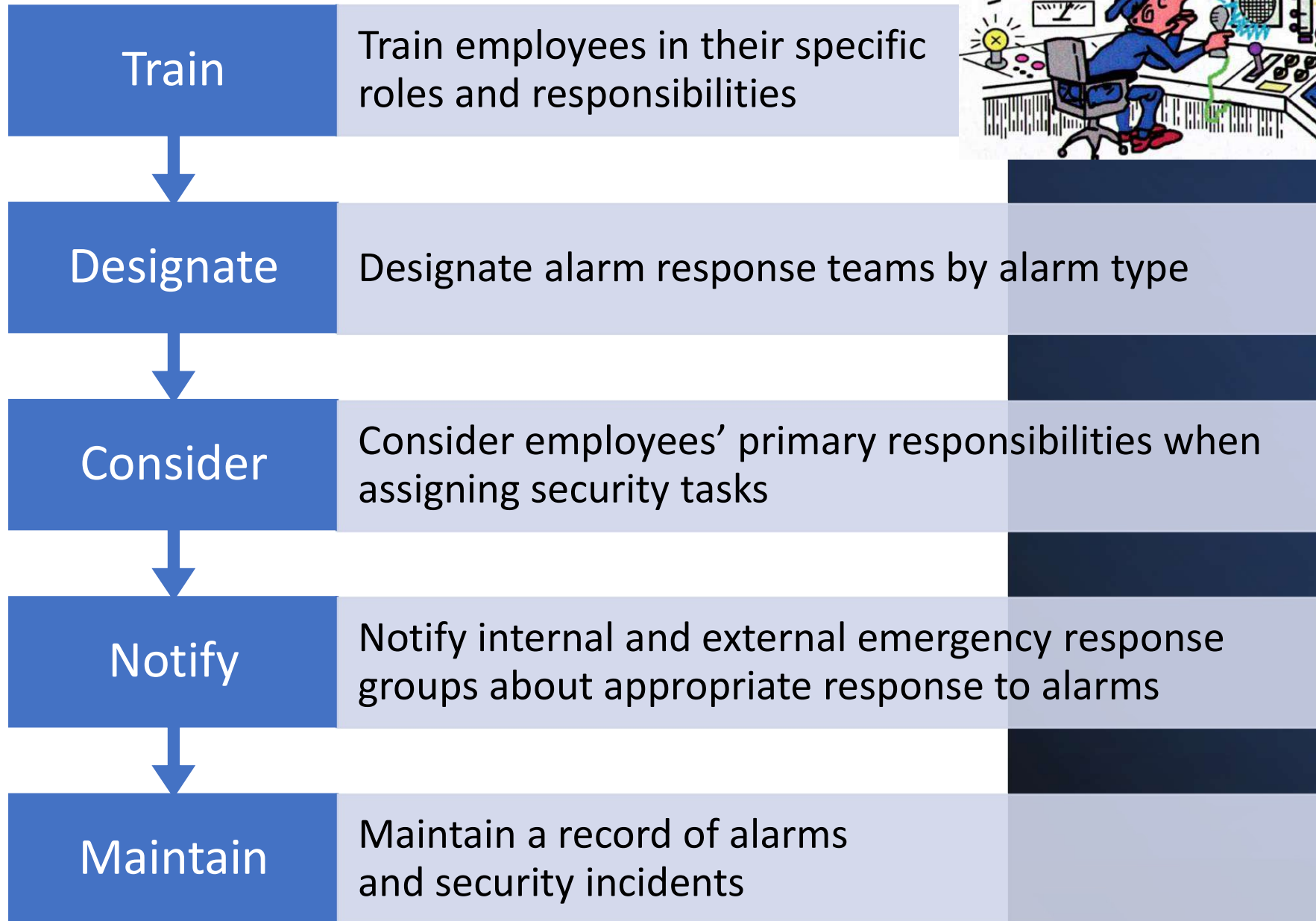
Operational changes can provide cost-effective ways to enhance security



Operational practices should always be geared to reduce risk based on the utility's Design Basis Threat and threat condition

Operational Security

Alarm Response



Operational Security

Delivery Protocols

Pre-approve drivers who regularly serve the facility and provide them with ID badges

Perform an assay on a sample of any chemical prior to accepting or while in holding vessel

Maintain detailed logs of deliveries and pick-ups

Provide a delivery hold area

Add a surveillance system at unloading areas

Have bill of lading and driver ID sent to the facility via fax or e-mail prior to truck arriving onsite

Notify chemical suppliers if deliveries are late

Security Procedures for Personnel



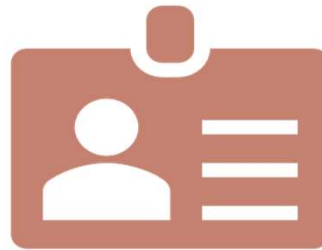
Engage ALL Staff in Security

Awareness ram

Employee awareness of anything out of the ordinary

Look for suspicious activities around all utility facilities as part of work

Provides Positive Buy-In



Employee Security Screening

Consider for Critical Positions

What to Screen For?

May not be an Indicator of the Future



Vendor/Contractor Security Screening

Can be Costly, Difficult to Enact

Physical Security

- **Elements of a Physical Protection System (PPS)**
Need a Balance of Detection, Delay and Response
- **Protection in Depth**
- **Crime Prevention Through Environmental Design (CPTED)**
- **Target Hardening**
- **Specific Countermeasures**

Elements of Physical Security

- Detection

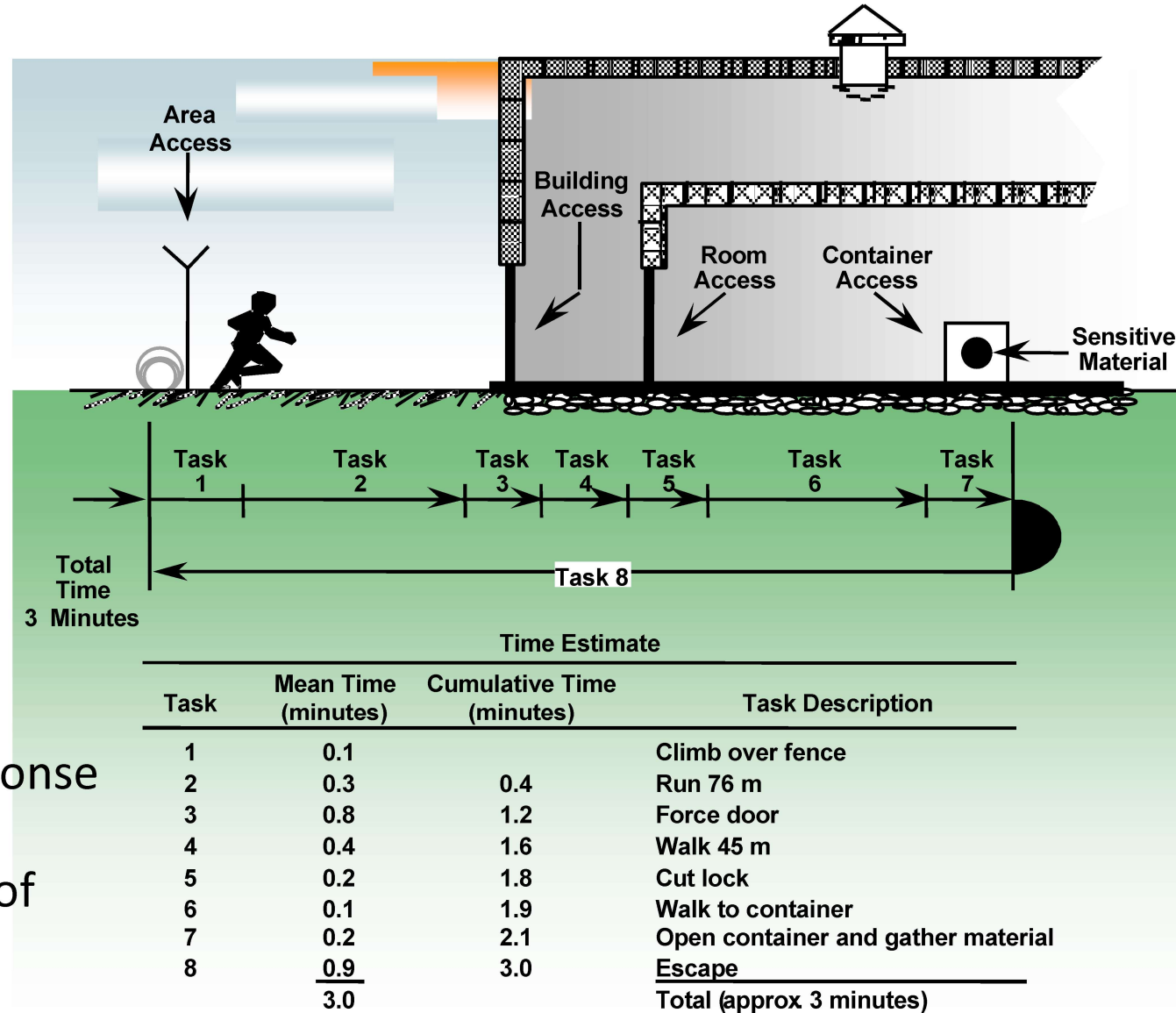
- Intrusion sensing
- Alarm communication
- Alarm assessment
- Entry control

- Delay

- Barriers
- Distance

- Response

- Communications to response force
- Deployment and arrival of response force



Physical Security

Delay

- Fences
- Vehicle/Pedestrian Gates
- Barriers
- Doors and Windows
- Walls/Buildings
- Access Control Systems
 - Locks
 - Biometrics
 - Card Reader/PIN



Physical Security

Detection

- CCTV
 - Resolution
 - Illumination
 - Digital Motion Capture
 - Hardwired Surveillance vs. Wireless Systems
- Access Control
 - Door/Window Contact Alarms
 - Motion Sensors
- Lighting



Physical Security

Key Control

- Don't use master keys except as necessary
- Track all keys
- Distribute only keys necessary to do the job
- Retrieve keys from employees who don't need them or have been terminated
- Periodically change codes and replace locks
- Perform random key audits



Physical Security

Target Hardening

- Physical protective measures that increase resistance threats
- Enhance delay/detection thru physical improvements
- Above and beyond CPTED* and basic design considerations
- Based on vulnerability and criticality of facility



* Crime Prevention Through Environmental Design

Protection in Depth



PROVIDES
MULTIPLE
LAYERS OF
PROTECTIVE
MEASURES



REQUIRES AN
ADVERSARY TO
DEFEAT
A SYSTEM,
TRAVEL TO THE
NEXT
PROTECTIVE
LAYER AND
DEFEAT THAT
SYSTEM



AT SITE
BOUNDARY
(PERIMETER
FENCING
SYSTEM)



AT BUILDING
ENVELOPE
(EXTERIOR
WALLS,
DOORS,
WINDOWS,
GRILLES, AND
ROOF SYSTEM)



AT TARGET
ENCLOSURE
(THE ROOM IN
WHICH THE
TARGETED
ASSET IS
HOUSED)

Physical Security

Specific Countermeasures - Response

Reliable, Alternate
and Compatible
Means of
Communication

Knowledge and
Relationship with
Local Law
Enforcement (LLE)

Facility and Alarm
Awareness for LLE



Cyber Security

- Physical disruption of SCADA
- Attacks on central control system to create simultaneous failures
- Software attacks using worms/viruses
- Network flooding, jamming
- Corrupt chlorine residual data allowing proliferation of microbes
- Ransomware (2018 ONWASA, 2020 Greenville, SC, 2020 Durham, NC)
- Take control of equipment, damage equipment (2016 Iranian attack on dam)

https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A

<https://securityboulevard.com/2020/01/north-carolina-water-supplier-targeted-in-international-cyberattack/>

<https://time.com/4270728/iran-cyber-attack-dam-fbi/>

Vulnerabilities to Computer System Infrastructure

- AMR / AMI
- Financial systems
- Human resource systems
- Laboratory information management
- Maintenance management
- SCADA
- Information Technology vs. Operation Technology (IT v. OT)

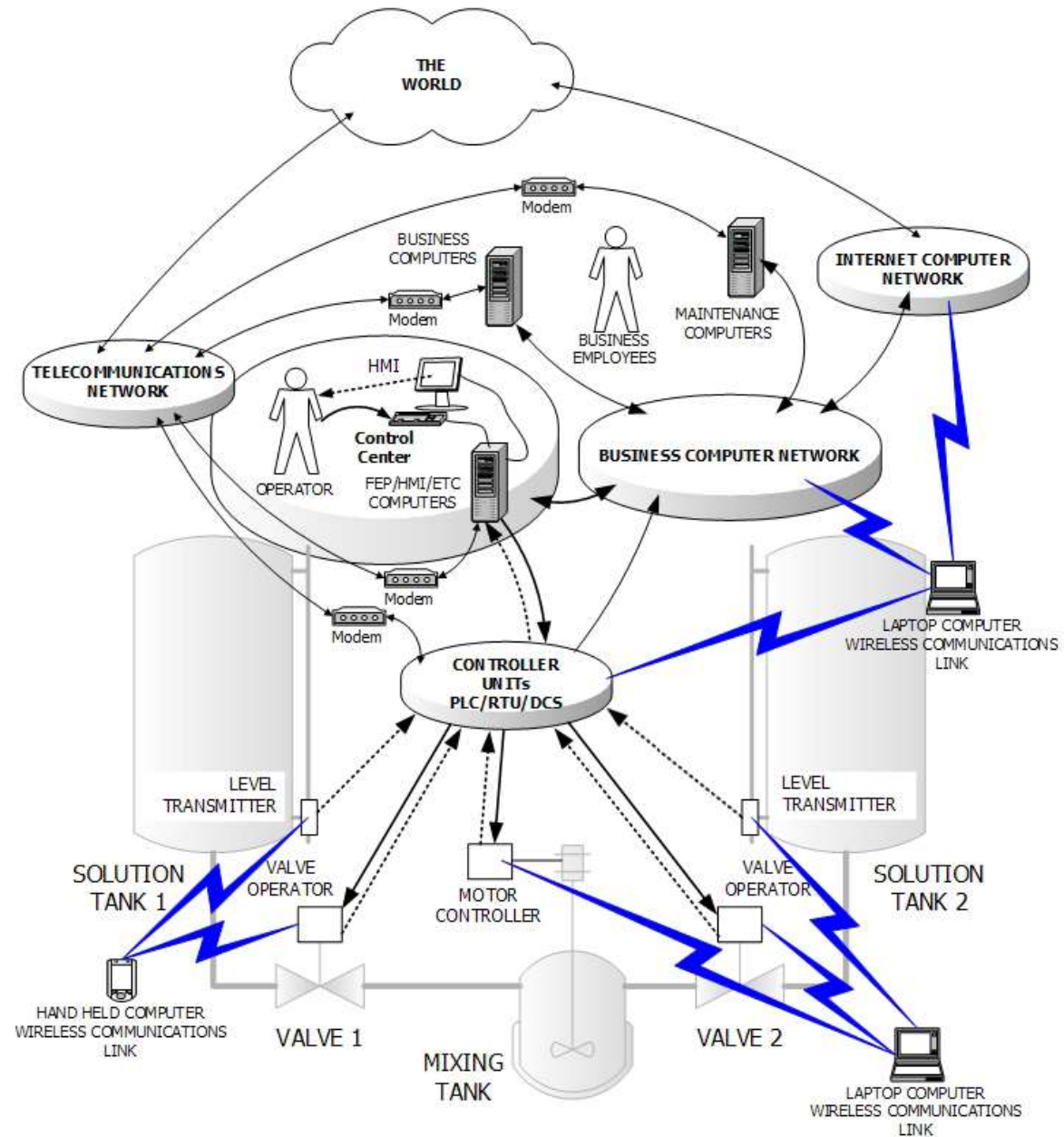


Business IT vs. SCADA (OT)

Topic	Business IT	SCADA
Availability	Reboots allowed for applying patches	Maintenance windows are few and far between
Consequences of Downtime / Outages	Data and production can typically be recovered	Data often not reconstructable, Process restarts are highly disruptive
Endpoint Protection	Common and easy to deploy	PCS components do not support endpoint protection
Technology Support Lifetime	3 to 4 year lifecycle	20+ year lifecycle
Physical Security of Assets	Offices and data centers are relatively easy to secure	Remote location of some assets make physical security more challenging
System Security Development	Security features designed into all modern hardware and software	Most PCS components designed without security features
Internet Access	Systems designed for internet access	Older systems were never intended to be internet attached

Connectivity = Exposure

- Process Control Systems
 - SCADA
 - Sensors
 - Remote asset communications
- Enterprise IT Systems
 - AMR/AMI
 - Customer Billing
 - Employee Payroll
 - Vital business records
 - Asset management
 - GIS
 - LIMS



Computer Vulnerabilities



- Operator station logged on all the time
- Physical access to the SCADA equipment easy
- Unprotected SCADA network access from remote locations
- Insecure wireless access points on the network
- Most SCADA networks directly or indirectly connected to the internet

Computer Vulnerabilities



- No firewall
- System event logs not monitored
- Intrusion detection system not used
- Operating and SCADA system software patches not routinely applied
- Network and/or router configuration insecure
- Passwords not changed from manufacturer's default

Mitigation

You cannot prevent every attack.
You can 'mitigate' to prevent, minimize, and limit injury and damage.

- Train to Repair/Replace Most Critical Facilities
- Maintain Accurate, Up To Date Plans/Maps
- Maintain Agreements with Local Contractors and Vendors for Emergency Response

Mitigation – Best Practices

Operations & Maintenance best practices for normal operations are also important for security mitigation

- Employ redundant processes
- Know your process dynamics
- Rotate standby equipment into operation
- Store spare equipment in a separate location
- Exercise backup generators

Mitigation – Emergency Response Plan (ERP)

A standardized response and recovery protocol to prevent, minimize, and mitigate injury and damage.

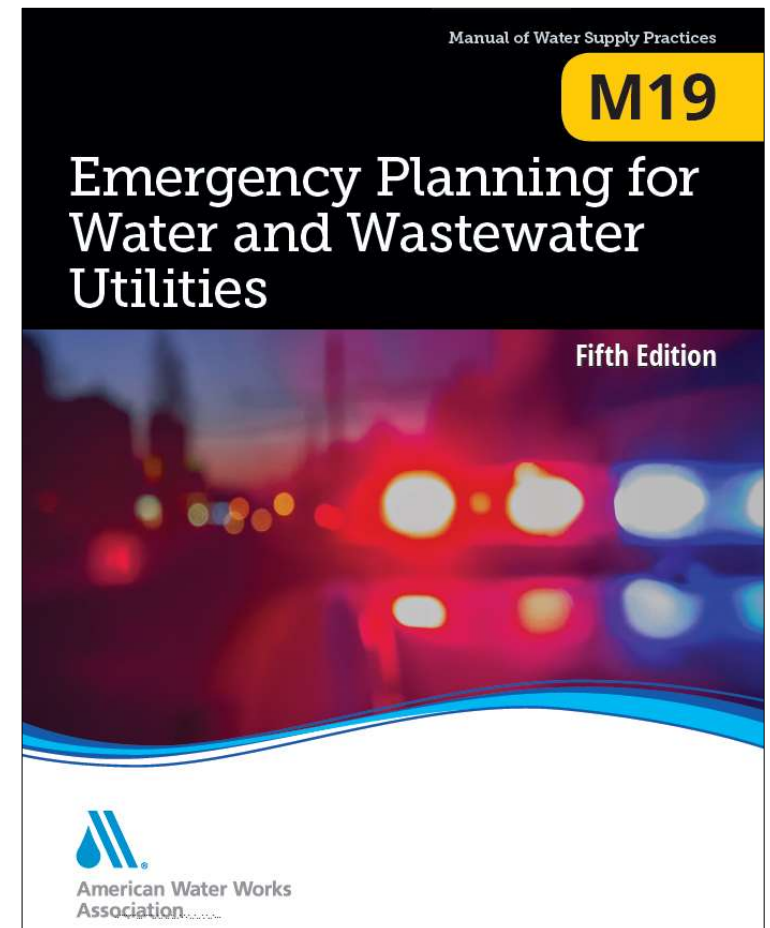
Should follow from a VA and be distributed on a “Need to Know” basis.

The ERP should:

- Outline communication and coordination between utility and emergency response personnel
- Define procedures and protocols to be followed in an emergency
- Identify equipment and resources to assist responding to and recovering from a disaster

Mitigation – Emergency Response Plan (ERP)

People Procedures Resources



Mitigation - Emergency Response Plan (ERP)



- Update ERP annually
- Update contact lists quarterly
- TRAIN AND EXERCISE the ERP

References

- ANSI/AWWA G430-14, Security Practices for Operation and Management
- ANSI/AWWA J100-10: Risk Analysis and Management for Critical Assets Protection for Risk and Resilience Management of Water and Wastewater Systems (J100) methodology
- AWWA, Water Sector Cybersecurity Risk Management Guidance and Tool
- ANSI/AWWA G440-17, Emergency Preparedness Practices
- AWWA M19, Emergency Planning for Water and Wastewater Utilities
- Cyber-Informed Engineering, Idaho National Labs, INL/EXT-16-40099
- The End of Cybersecurity, Harvard Business Review, May 2018
- EPA ERP Template
 - https://www.epa.gov/sites/production/files/2019-07/documents/190712-awia_erp_template_instructions_kab_508c_v6.pdf
- EPA Drinking Water and Wastewater Resilience
 - <https://www.epa.gov/waterresilience>

Wastewater System Security Awareness

Questions?

Stephen Brown, PE

Senior Consultant

D 919-900-1648 **M** 919-268-3001

stephen.brown@hdrinc.com