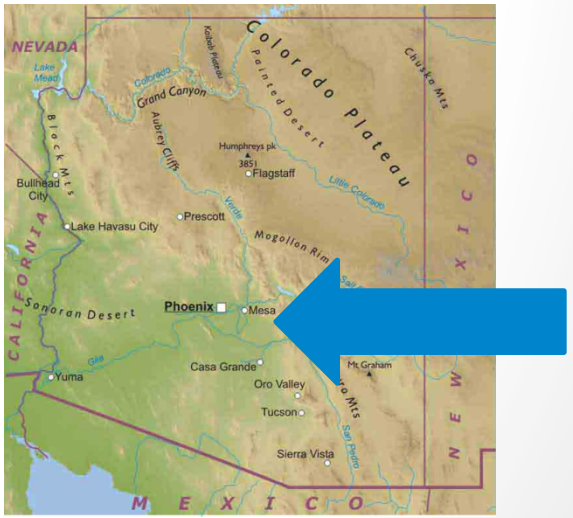
A Threat from the Inside

Incident Response and Lessons Learned

mesa water

Reliability ~ Quality ~ Value

- Serve water to around 500,000 people
- Deliver around 90,000 AFY
- Water revenues around $115 M/YR
- Wastewater revenues around $67 M/YR
- Service area 144 square miles



The Insider Threat

- Employee perceives some inequity or injustice
- Contrived solution that results in negative consequences for the organization
- Actions often the result of problems or crisis in the individual's personal life

Source: Micheal G. Gelles, Psy.D., David Brant, MS, Brian Geffert, *Building a Secure Workforce*

Greenfield Plant

- 16 mgd wastewater treatment plant
- Anaerobic digestion for residuals treatment
- Jointly owned by the City of Mesa and the Towns of Gilbert and Queen Creek
- Plant operated by City of Mesa, located in the Town of Gilbert
- Plant staffed 24/7

Incident Basics

- Buildup of methane gas
- Standoff with SWAT
- Handgun
- Lack of pay raises, increasing health care costs
- Resentment, family pressures, foreclosure
- Terrorism charges

Incident Timeline

- 11:30 pm -12:10 am: alarming and paging system turned off.
  - Other employees “blind” to problems at the plant, not receiving SCADA alarms.
- 12:12 am: Digester gas flares turned off; methane gas that would normally be burned started to build pressure in the digesters.

Incident Timeline

- 12: 19 am: Ultraviolet disinfection system turned off. Backup disinfection employed.
- 12:27 am: Influent pumps turned off. Sewage began backing up into the collection system.
- 12:39 am: Blower turned off, which supplies air for bacteria that treat the sewage.

Incident Timeline

- 12:45 am: Safety valves began venting methane from the top of the digester complex.
- 1:10 am: Effluent pumps turned off.

- 2:39 am: Employee called 911.

Incident Response

- Town of Gilbert police/SWAT responded to the 911 call
- 911 operator “talked him down”
- 4:34 am employee taken into custody
- Mesa employees helped police during the incident, and took back operation of the plant once the employee was apprehended.

Outcome

- No one was harmed during the incident
- Plant operations were restored within hours
- Plant did not suffer major damage, and raw sewage did not overflow into streets
- Safety mechanisms designed to prevent the buildup of methane gas worked as designed
- The general public was not in harm's way

Significant Factors to Success

- The following factors were the most significant contributions to the success of the response:
  - Communication among Water Resources Department staff
  - Advanced training of plant staff
  - Single individuals

Media and Community

- Conflicting goals
- Isolated nature of the plant
- Media/Public confusion

Mitigating the Insider Threat

Utility Style!

- Much focus on cybersecurity and the insider threat
- Many of the suggested best practices either do not apply or are not workable for physical rather than cyber environments
- The ***nature of remote sites*** in the utility industry presents additional challenges

Remote Site Context

- Remote sites are “bubbles”
  - Physically separate, often by many miles
  - Fewer staff, and they spend ***a lot of time together***
  - More difficult to keep tabs on
  - Experience less influence from the “mothership”—develop their own culture
- Remote sites contain our most important, most vulnerable assets

Threat Mitigation

- Know your vulnerabilities
- Address negativity in the workplace
- Ensure employees have a sense of personal mission and dignity in the job
- Be ambassadors that counter negativity towards government
- Tailor management strategies to meet the challenges presented by remote sites

Last Word

- Prepare for and practice incident response

Questions?