

A decorative graphic on the left side of the slide consisting of white lines and circles on a dark blue background, resembling a circuit board or a stylized tree structure.

# INFORMATION SECURITY

CITY OF DENTON – PUBLIC UTILITIES BOARD



# AGENDA

- Information Security Overview
- City of Denton Information Security Practices
- Electric-Specific Security Information (NERC CIP & SCADA)



# INFORMATION SECURITY OVERVIEW

***Information Security*** is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.



# INFORMATION SECURITY OVERVIEW

## Desired Goals:

- Security: Controlling access and privacy of data
- Integrity: Consistency, accuracy and trustworthiness of the data
- Availability: Insuring that data is accessible to users and business continuity measures are in place

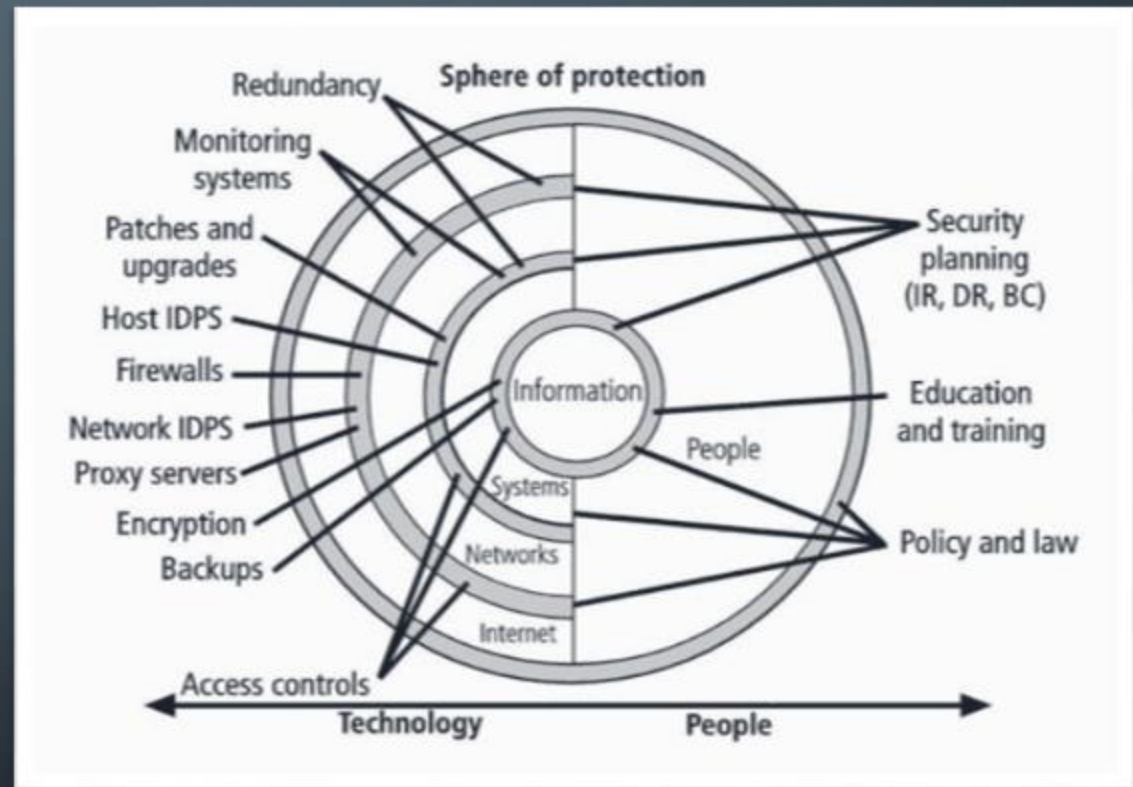
## Security Measures:

- People: Education, Training and Awareness
- Process: Policy, Standards and Procedures
- Technology: IT Solutions



# INFORMATION SECURITY OVERVIEW

Information Security is not a single technology; rather it is a multi-layered strategy comprised of the **People, Processes** and **Technology** necessary to prevent, detect, document and counter threats to digital and non-digital information.



# INFORMATION SECURITY OVERVIEW

Threat	Examples
Deviations in service from service providers	Fluctuations in power, data and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail, threat of information disclosure
Sabotage or vandalism	Damage/destruction of systems or information
Software attacks	Malware: viruses, worms, DOS attacks, Trojans, etc.
Technical hardware failures	Hardware equipment failure
Technical software failures	Bugs, code vulnerabilities, unpatched software, etc.
Technological obsolescence	Outdated technologies or practices
Theft	Illegal confiscation of equipment or information

## BY THE NUMBERS

- The City of Denton detected 55 million threats. This includes over 30 thousand instances of spyware and 5,000 viruses.
- The City of Denton has blocked over 990,000 attacks from 367 unique attack types.
- On average, we block about 50,000 thousand malicious webpages a month.
- Received over 7,042,339 million emails. Out of those, 69% percent were detected as threats and only 30% percent (2,968,927) were delivered to email recipients.

The background is a dark blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks, with lines and small circles connecting them.

A staggering 43% of companies have  
experienced a data breach in the past year

Source: USA Today



# Worst Data Breaches of 2015

- **Federal Office of Personnel Management**

- An attack exposed over 21.5 million citizen records compromised.

- **Lansing Board of Water and Light**

- Ransomware left systems offline for nearly a week.

- **Unnamed water utility**

- Hackers breached a water utility and manipulated systems responsible for water treatment and flow control

- **City of San Antonio**

- City sends \$349,000 to fraudulent account

- **Grapevine Police Department**

- Database was hacked as a group demanded dashcam video of shooting.

- **Dallas County, Texas**

- Data breach of residents information online for over 6 months

- **Damariscotta County Sheriffs Department, Maine**

- Malware outbreak caused them pay hackers to retrieve confidential records

A decorative graphic on the left side of the slide consisting of a network of thin, light green lines and small circles, resembling a circuit board or a stylized tree structure, extending from the top and bottom edges towards the center.

# CITY OF DENTON

IT SECURITY PROCESSES AND PROCEDURES

# CITY OF DENTON

## PEOPLE

- Hiring
- Security awareness training
- Education
- Assessment
- Accountability



# CITY OF DENTON

## PROCESS (PREVENTION)

- Security architecture and design
- Physical security controls
- Password policies and access controls
- Controlled use of administrative privileges
- Proactive monitoring and analysis of logs
- Vulnerability assessments, penetration testing and Tabletop Exercises

## PROCEDURE (RESPONSE)

- Site Redundancy
- Incident response plans
- Security retainers with companies specializing in information security





# CITY OF DENTON

## TECHNOLOGY

1. Perimeter Security: firewall, IDS/IPS, DMZ, e-mail scanning (anti-virus)
2. Network Security: firewall, web proxy, wireless security, enterprise remote access
3. Endpoint Security: desktop firewall, anti-virus, patch management, local security policies
4. Application Security: application testing, code review, database monitoring
5. Data Security: drive encryption, data archive, data wiping, data classification, identity access management



# CITY OF DENTON

## OPPORTUNITIES

- Provide security awareness and training to the entire organization. Training should cover security issues, policies, standards, procedures and regulations.
- Implement a comprehensive, written information security policy.
- Review our Incident Response Plan
- Use ITIL methodologies to improve information security by allowing current practices to be replaced with standardized, integrated processes based on industry best practices



## CITY OF DENTON

## OPPORTUNITIES (CONT.)

Evaluate possible security and reliability improvements gained through a centralized IT model.

- Centralization will create a more effective disaster recovery strategy, minimize labor redundancies, allow for volume discounts on technology purchases, and lower maintenance and training costs through standardization.



A decorative graphic on the left side of the slide consists of white and light blue lines forming a circuit-like pattern. These lines connect to small circles of varying sizes, creating a vertical, branching structure that resembles a stylized tree or a network diagram. The background is a gradient of blue, with faint, larger-scale circuit patterns visible in the upper half.

# DENTON MUNICIPAL ELECTRIC

IT SECURITY PROCESSES AND PROCEDURES



# DENTON MUNICIPAL ELECTRIC

- DME uses the City Tech Services policies and procedures for all staff computers.
- DME also maintains a completely independent SCADA network that controls the electric grid, communicates with ERCOT, and collects data regarding electric usage and the bulk electric system.
- DME maintains 3 full-time staff members to manage the SCADA network and ensure compliance with NERC CIP requirements
- We are required to self-report at any time that we become non-compliant
- Subject to NERC audits and potential fines for non-compliance

# DENTON MUNICIPAL ELECTRIC

The SCADA network, including the electronic and physical controls surrounding it, are regulated by NERC and their Critical Infrastructure Protection (CIP) standards.

- There are 10 CIP Cyber Standards and 1 CIP Physical Security Standard
- CIP standards are highly detailed documents ranging from 20 to 50 pages each.
- DME meets all of these standards and has been compliant since their effective date of July 1, 2016.



# DENTON MUNICIPAL ELECTRIC

CIP Standard	Subject Matter Covered by Standard
CIP-002-5.1	<a href="#">Cyber Security – BES Cyber System Categorization</a>
CIP-003-6	<a href="#">Cyber Security – Security Management Controls</a>
CIP-004-6	<a href="#">Cyber Security – Personnel &amp; Training</a>
CIP-005-5	<a href="#">Cyber Security – Electronic Security Perimeter(s)</a>
CIP-006-6	<a href="#">Cyber Security – Physical Security of BES Cyber Systems</a>
CIP-007-6	<a href="#">Cyber Security – System Security Management</a>
CIP-008-5	<a href="#">Cyber Security – Incident Reporting and Response Planning</a>
CIP-009-6	<a href="#">Cyber Security – Recovery Plans for BES Cyber Systems</a>
CIP-010-2	<a href="#">Cyber Security – Configuration Change Management and Vulnerability Assessments</a>
CIP-011-2	<a href="#">Cyber Security – Information Protection</a>
CIP-014-2	<a href="#">Physical Security</a>

# DENTON MUNICIPAL ELECTRIC

DME follows all of the requirements set forth in the CIP standards, including the following:

- IDS/IDP & anti-malware
- Change control processes
- Site and hardware redundancy
- Electronic and physical security controls
- Annual training for users & admins
- Annual vulnerability assessments
- Tabletop exercises
- Mock audits
- Scheduled patch management
- Annual document and process review



# DENTON MUNICIPAL ELECTRIC

## NEXT STEPS

- Complete build-out of redundant DMZ site
- Continue to review and enhance our internal processes and systems
- Develop plans for the new Denton Energy Center (RDP) and the related NERC CIP requirements affecting that project.



An abstract graphic on the left side of the slide, consisting of a network of white lines and small circles on a blue gradient background. The lines and circles resemble a circuit board or a neural network diagram, with some lines extending vertically and others branching out horizontally and diagonally.

QUESTIONS?