# Technology Director Meeting

EDUCATION SERVICE CENTER, REGION 20

*Serving the Educational Community*

ESC★20
Serving the Educational Community

**Mission:** ESC-20 positively impacts the learning community **through high quality, cost effective products and services.**

**Vision:** To be the **definitive choice** for **leadership, innovation,** and the **advancement of learning.**

## We believe...

in **service** first • **change is opportunity** • our employees **drive our success** • in **cultivating strengths**
**collaboration** maximizes results • **learning** is **life-long** • in **purposeful** and **effective communication**

### Strategic Drivers

**Customer Service:** Create a service culture through a focus on the total customer experience.

**Customer Focus:** Listen to our customers, anticipate their needs, and create value that exceeds their expectations.

**Employee Talent:** Attract, grow, and retain top talent.

**Continuous Improvement:** Create a culture of excellence through a mindset of continuous improvement.

### Quality Objectives

**Positive Impact on Education**

**Customer Satisfaction**

**Employee Satisfaction**

**Operational Excellence**

**Public Awareness/Relations**

### Strategies

**Build relationships** and **engage stakeholders**

Provide comprehensive **school improvement services** and **support**

Recruit and retain **high quality workforce**

Allocate resources to **develop** and sustain **quality products** and **services**

Implement a **performance excellence management system**

# Agenda

ESC★20 Serving the Educational Community

## Network Infrastructure and Security Services

- Security Awareness Training
- Security IQ
- Network Assessment
- Network Diagraming
- Network Vulnerability Scan

ESC★20 Serving the Educational Community netVISION20 EDUCATION SERVICE CENTER, REGION 20

RAPID7

SecurityIQ BY INFOSEC INSTITUTE

# Security Awareness Training

Security Awareness Training Provided by ESC-20

## Live user security awareness training - ideal for staff development sessions.

## Risk:

Employees, contractors or third party users breach security because they are not aware or trained on information security requirements.

Topics Covered:

- Passwords
- Social Engineering
- Physical Security
- Remote Access and Electronic Communications
- Incident Reporting

*Topics can be customized to suit your district

1 hour session provided to your staff

- Certification of completion
- Phishing example that points out phishing email indicators

# Security IQ

Security IQ licensing available through ESC-20

ESC-20 has partnered with computer based training and Phishing Simulation platform, SecurityIQ.

## Risk:

Phishing attacks are a very common form of social engineering.  Successful Phishing attacks may result in financial loss, data theft, and loss of productivity,

Use Security IQ **PhishSim** to create phishing simulations to test user responses.

Follow up phishing campaigns with **AwareEd**, interactive training, to stablish a program for recurring training.

- Establish an ongoing information security awareness education program for all users
- Provide role-based information security training to staff with information security responsibilities.

# Network Assessment

Network Assessments provided by ESC-20

## The network assessment provides an understanding of the architecture, infrastructure, and security posture.

## Risk:

Objective reviews of information security are not regularly performed to determine the continuing suitability, capability, and effectiveness of the organization's information security program.

The goal of a network security assessment is to identify network and system vulnerabilities by assessing management, operations, and technical aspects of an information system and provide recommendations to remediate or improve the security posture.

5 phase approach to the network security assessment:

1) Planning
2) Survey
3) Analysis
4) Reporting
5) Remediation

# Network Diagraming

Network Diagrams by ESC-20

## Understand data flow and connectivity from ISP to endpoint.

## Risk:

Lack of usable network documentation may lead to unnecessarily long troubleshooting. Network drawings show the layout of the network infrastructure - where devices are physically and logically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks could take place.

**Layer 1/2 Diagram**

Physical diagram

- Interfaces
- Trunking
- VLAN Information
- Root Bridge

**Layer 3 Diagram**

Logical map of the network

- VLAN Subnet Information
- Route Next Hop Information
- Applied Access Controls

# Network Vulnerability Scan

ESC-20 Vulnerability Scanning with Rapid 7 Nexpose

## Scan for vulnerabilities in information systems and hosted applications.

## Risk:

Technical vulnerabilities are exploited to gain inappropriate or unauthorized access to information systems due to lack of controls for those vulnerabilities.

Perform discovery and vulnerability scans of subnet scopes of 254 IP address

Annual Vulnerability Scan Included with Premier Membership

**Full Audit Report**

- Provides a detailed look at the state of security in your environment.
- Vulnerability information:
  - ○ Affected assets
  - ○ Vulnerability descriptions
  - ○ Severity levels
  - ○ References and links to important information sources, such as security advisories

Additional Reports Deliverables

- Highest Risk Vulnerabilities
- Remediation Plan
- Top 10 Assets by Vulnerability Risk
- Top Remediations with Details

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"

*Sun Tzu - The Art of War*