# Security Awareness Training for OT

## Building a Human Firewall in Industrial Environments

OT Security Learning Series

Document 895 | February 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

# Contents

# 1 Introduction

**Information**

Security awareness training in OT environments must address the unique challenges of industrial settings, where personnel interact with both cyber and physical systems. Effective training transforms employees from potential vulnerabilities into active defenders of critical infrastructure.

Human factors remain one of the most significant vulnerabilities in OT security. While technical controls are essential, they cannot prevent all attacks—especially those targeting personnel through social engineering, phishing, or manipulation. Security awareness training bridges this gap by equipping staff with the knowledge and skills to recognize and respond to threats.

## 1.1 Why OT-Specific Training Matters

OT environments differ significantly from traditional IT settings:

- **Safety implications** – Security incidents can cause physical harm
- **Different threat landscape** – USB-based attacks, physical access, and insider threats are critical vectors, especially for isolated systems
- **Diverse workforce** – Operators, engineers, and contractors have varying technical backgrounds
- **Legacy systems** – Many systems lack modern security features
- **24/7 operations** – Training must accommodate shift workers

# 2 IT vs OT Security Awareness

| Aspect | IT Focus | OT Focus |
|---|---|---|
| Primary concern | Data confidentiality | Safety and availability |
| Common threats | Email phishing, malware | Phishing, USB, physical access |
| Attack impact | Data breach, financial loss | Physical damage, safety hazards |
| User base | Office workers | Operators, engineers, technicians |
| Training delivery | Online modules, email | Hands-on, shift-based sessions |
| Compliance drivers | GDPR, PCI-DSS | IEC 62443, NERC CIP |

Table 1: Key differences between IT and OT security awareness

# 3 Key Training Topics

## 3.1 Social Engineering

**Warning**

Social engineering attacks exploit human psychology rather than technical vulnerabilities. In OT environments, attackers may pose as vendors, contractors, or support personnel to gain physical or logical access.

Training should cover:

- **Pretexting** – Attackers creating false scenarios to extract information
- **Tailgating** – Following authorized personnel into secure areas
- **Impersonation** – Posing as vendors, auditors, or IT support
- **Phone-based attacks** – Vishing (voice phishing) targeting control rooms
- **Verification procedures** – How to validate identities and requests

## 3.2 Phishing and Email Security

Phishing is the leading initial access vector for ransomware attacks (approximately 35% of incidents). While OT networks may be isolated, many personnel have access to both IT and OT systems, making phishing a primary threat:

- Recognizing suspicious emails and links
- Spear-phishing targeting specific roles (e.g., control engineers)
- Reporting procedures for suspected phishing
- Safe handling of attachments

## 3.3 Removable Media Threats

**Critical**

USB devices are a critical attack vector for targeting air-gapped OT networks. Stuxnet spread via infected USB drives, demonstrating how removable media can bypass network isolation. While USB accounts for a smaller percentage of overall ransomware attacks, it remains essential for targeted attacks on isolated systems.

Training must emphasize:

- Never using unknown or untrusted USB devices
- Following media scanning procedures before use
- Understanding the risks of “USB drop” attacks

- Proper handling of vendor-provided media
- Using only approved, encrypted devices

### 3.4 Physical Security

OT security extends beyond cyber threats:

- **Access control** – Badge usage, door security, visitor management
- **Clean desk policy** – Protecting sensitive documents and credentials
- **Device security** – Locking workstations, securing portable equipment
- **Photography restrictions** – Preventing reconnaissance
- **Reporting suspicious activity** – What to report and to whom

### 3.5 Password and Authentication

- Creating strong, unique passwords
- Never sharing credentials (even with colleagues)
- Understanding shared account risks in control rooms
- Multi-factor authentication where available
- Recognizing credential harvesting attempts

### 3.6 Incident Recognition and Reporting

Personnel should know how to:

- Recognize signs of a security incident
- Distinguish between safety and security events
- Report incidents through proper channels
- Preserve evidence without disrupting operations
- Understand their role in incident response

## 4 Role-Based Training

Different roles require tailored training content:

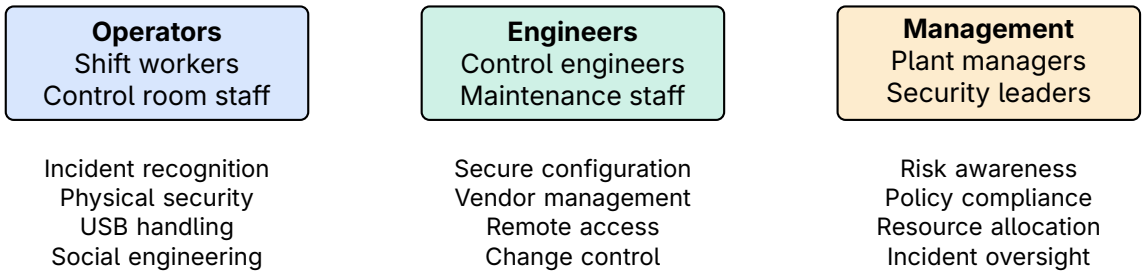


Figure 1: Role-based training focus areas

### 4.1 Operators and Technicians

- Focus on daily operational security practices
- Hands-on scenarios relevant to their work environment
- Clear, simple procedures for reporting
- Emphasis on safety-security relationship

### 4.2 Engineers and Technical Staff

- Deeper technical content on attack methods
- Secure engineering practices
- Vendor and third-party risk management
- Secure remote access procedures

### 4.3 Management and Supervisors

- Risk management and business impact
- Regulatory compliance requirements
- Resource allocation for security
- Leading by example and fostering security culture

### 4.4 Contractors and Vendors

**Key Point**

Third parties often have privileged access to OT systems. They must receive security awareness training before accessing your environment, covering your specific policies and procedures.

## 5 Training Delivery Methods

### 5.1 Classroom Training

Traditional instructor-led sessions work well for:

- Initial onboarding of new employees
- Complex topics requiring discussion
- Building team awareness and culture
- Hands-on exercises with equipment

### 5.2 Online/E-Learning

Digital training modules offer:

- Flexibility for shift workers
- Consistent content delivery
- Progress tracking and documentation
- Cost-effective refresher training

### 5.3 Hands-On Exercises

Practical exercises reinforce learning:

- Simulated phishing campaigns
- Physical security walkthroughs
- USB drop tests
- Tabletop exercises

### 5.4 Just-In-Time Training

Brief, targeted training at the point of need:

- Quick reminders before high-risk activities
- Toolbox talks during shift handovers
- Posters and visual aids in control rooms
- Security tips in regular communications

## 6 Building a Security Culture

**Tip**

A strong security culture means employees naturally consider security in their daily decisions, without needing constant reminders or enforcement.

### 6.1 Leadership Commitment

- Visible support from plant management
- Security discussed in regular meetings
- Adequate resources for training programs
- Recognition of security-conscious behavior

### 6.2 Positive Reinforcement

- Reward reporting of security concerns
- Recognize employees who identify threats
- Avoid blame culture for honest mistakes
- Celebrate security achievements

### 6.3 Continuous Communication

- Regular security updates and newsletters
- Share relevant incidents (anonymized)
- Post security reminders in visible locations
- Include security in operational briefings

## 7 Measuring Effectiveness

### 7.1 Key Metrics

| Metric | Description |
|---|---|
| Phishing click rate | Percentage clicking simulated phishing links |
| Reporting rate | Number of security concerns reported |
| Training completion | Percentage completing required training |
| Time to report | Average time to report incidents |
| Assessment scores | Pre/post training knowledge tests |
| Policy compliance | Adherence to security policies |

Table 2: Security awareness program metrics

### 7.2 Continuous Improvement

- Regular assessment of training effectiveness
- Update content based on emerging threats
- Gather feedback from participants
- Benchmark against industry standards

- Adjust frequency based on results

## 8 Compliance Considerations

Several standards require security awareness training:

- **IEC 62443-2-1** – Requires security awareness and training programs
- **NERC CIP-004** – Mandates personnel risk assessment and training
- **NIST SP 800-82** – Recommends OT-specific awareness training
- **NIS2 Directive** – Requires cybersecurity training for essential entities

## 9 Implementation Roadmap

1. **Assess current state** – Evaluate existing awareness levels and training
2. **Identify requirements** – Determine compliance and organizational needs
3. **Develop content** – Create OT-specific training materials
4. **Pilot program** – Test with a small group and gather feedback
5. **Roll out** – Deploy to all personnel with role-based tracks
6. **Measure and improve** – Track metrics and continuously enhance

## 10 Summary

**Key Takeaways**

- **OT-specific training** is essential—generic IT awareness is insufficient
- **USB and physical security** are critical topics often overlooked in IT training
- **Role-based content** ensures relevance for operators, engineers, and management
- **Multiple delivery methods** accommodate shift work and diverse learning styles
- **Security culture** requires leadership commitment and positive reinforcement
- **Measure effectiveness** through phishing tests, reporting rates, and assessments

## 11 Further Reading

### Standards and Guidelines

- **IEC 62443-2-1** – Security program requirements for IACS
  https://webstore.iec.ch/publication/7030
- **NIST SP 800-50** – Building an IT Security Awareness and Training Program
  https://csrc.nist.gov/pubs/sp/800/50/final

### Resources

- **SANS Security Awareness** – Resources and training materials
  https://www.sans.org/security-awareness-training/
- **CISA Industrial Control Systems** – Training and resources
  https://www.cisa.gov/topics/industrial-control-systems

### Books

- Hadnagy, C. – *Social Engineering: The Science of Human Hacking* (Wiley)
- Mitnick, K. – *The Art of Deception* (Wiley)

*Part of the OT Security Learning Series*