Began training Airports in 1997

Design Scalable, Flexible Web-based Training System

Train 1,000,000 Employees and Tenants Annually

Aviation Experts + ISD Professionals + Interactive Technology Developers

Today Over 50 Airports of ALL Sizes

SMEs provide consulting including ARFF review and manual creation/updates

Our Background
TOTAL TRAINING SOLUTION

OnDemand Training & Workshops
SME Led Training
25 Years Experience

Consulting
ARFF Consulting
ARFF Recurrent
Airport Regulatory Consulting

Curriculum Design
Syllabus, Scripting
Quizzes and Tests
Internal and Client SME Reviews

Computer Based Training
Audio / Graphical / Textual
Training Assignment, Records
Hosted and Integrated Services

Deployment Options
We Communicate

Training - Training - Training
Crisis can come from many directions.
Port Disaster Preparedness and Risk Management

Fractured Emergency Responsibilities
How does your Port deal with . . .

- Determining if the Port needs to shut down?
- What priority does CON OPS have in this?
- Setting up Port Operation Center to ensure EOC doesn’t impede on daily ops?
How does your Port deal with . . .

• A Family Assistance room and personnel from the port to open it 24/7?
• Is it Onsite, Pre-/Post-security, Offsite – enough back-up locations?
• Do you have supplies for children, elderly, and non-English speakers?
• How often do you bring the mutual-aid assistants/volunteers out to show them what is expected of them on site?
How does your Port deal with . . .

- Ensuring a Port representative is designated to go to each hospital and track the victims?
- How will these Team members communicate back with the EOC?
- Are you prepared to sequester the crew members from the passengers/victims/media?
Common Threats
At Home

Port Threats

2019

Hurricanes & Tornadoes
Earthquakes
Port operators have evolved to manage a complex environment of physical security challenges.

**Targets**
Ports have long been targets for those seeking to cause high-profile disruption and damage.

**Physical Assets**
Port personnel focus most of their efforts on protecting the physical assets such as security access, airfield lighting, fuel distribution, power management, and baggage handling systems.

**Security Challenges**
Port operators have evolved to manage a complex environment of physical security challenges.

**Port IT Systems**
A breach on Port IT systems, whether connected to internet or not, can cause disruption to service, theft of confidential data, or potential loss of human life.
Cyber Threat

- There are thousands of cyber attacks per month on transportation systems.
- This poses a real and current threat to Port safety, security and reputation.

Cyber security standards and best practices don’t appear to be widely adopted by US Ports.
Prime Targets
Ports are a prime target of computer hackers and other cyber criminals.

Continuous Targets
Ports continue to be targeted for attack by cybercriminals, hacktivists and nation-state actors.

Scarce Resources
Small and medium-sized Ports often struggle to adequately protect the networks used to operate and manage the Port and serve passengers.

Why Port Cybersecurity?
Quick Question

Where do you think Cyber Security Ranks in Port Security importance?
Security vulnerabilities, threats to avoid – especially when using electronic access control systems.
Examples of Phishing Emails
How might a cyberattack impact your Port?

- Phishing attacks against Port personnel resulting in information theft or network penetration
- Attempts to disrupt Port physical security systems
- Disruption of Port HVAC systems or other network accessible systems
- Attacks on Port electronic signage
- Defacement or service interruption to Port websites
More reasons to mitigate a cyberattack at your Port!

- Ransomware attacks encrypting Port files and data
- Theft of sensitive Port documents or emails
- Theft of credit and debit card information from passengers and other visitors
- Release of Port executive's personal information, such as home address, email address, family member information and phone numbers (known as “doxing”)
Where do most of the cyber risks come from?
The Error Factor

91% of all cyber breaches are caused by HUMANS.
Causes of Cyber Breaches

- Employee negligence or malfeasance: 66%
- External threat factor: 18%
- Other: 9%
- Social engineering: 3%
- Cyber extortion: 2%
- Network business interruption: 2%

Source: Willis Tower Watson claim data
HOW TO ACHIEVE CYBER RESILIENCE IN 7 STEPS

01 System Hygiene
02 Develop a Plan
03 Map Out Risk Profile
04 Assess & Measure
05 Mitigate Risk
06 Cyber Insurance
07 Get Started

What can your port do?
GET STARTED!
Engaging Strategies to Use

- Hold Regular Meetings
- Post Regular Security Alerts in a Common Location
- Create a Community of Knowledge with Awareness Training
How does your Port deal with . . .

Training and practicing with ALL STAKEHOLDERS on:
What to do when the media is asking questions?
What to expect WHEN an Emergency occurs?
Are you ready....are your co-workers?
Get Social With Us!

www.SSinstruction.com
www.ARFFRecurrent.com
@WeTrainAirports
@ARFF_Training
* SSInstruct1
Time for questions!

Emergency / Security Awareness

Lorena de Rodriguez, President, SSI, Inc.

Thank you!