

The logo for SSi, with 'SS' in red and 'i' in white with a red dot above it.

SSi

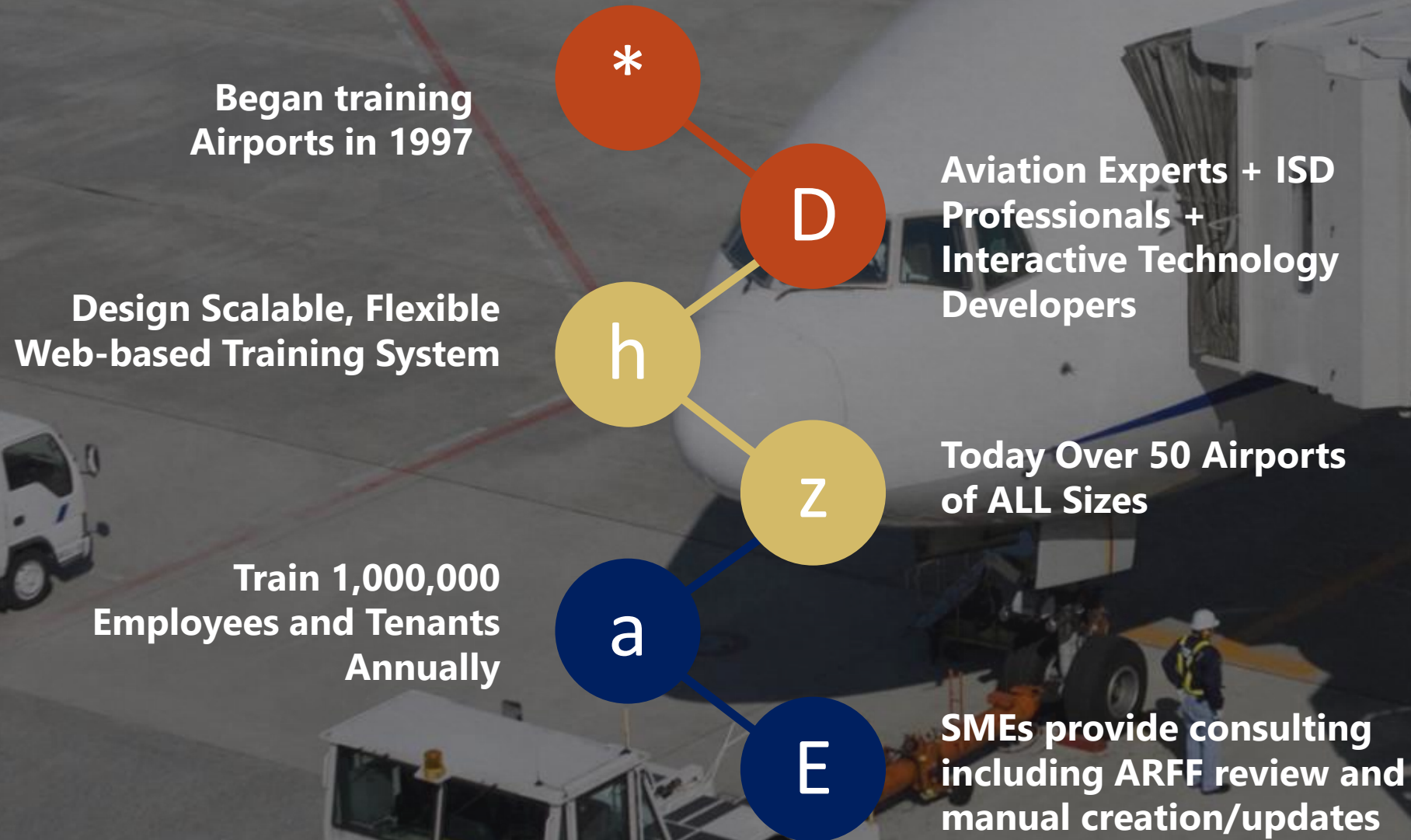
safety & security instruction

The text 'Emergency / Security Awareness' is written in a bold, red, sans-serif font. It is centered and overlaid on a blue circular graphic composed of many concentric, slightly irregular lines, resembling a stylized globe or a signal. The text has a slight glow effect.

**Emergency / Security  
Awareness**

Lorena de Rodriguez, President, SSi, Inc.

# 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

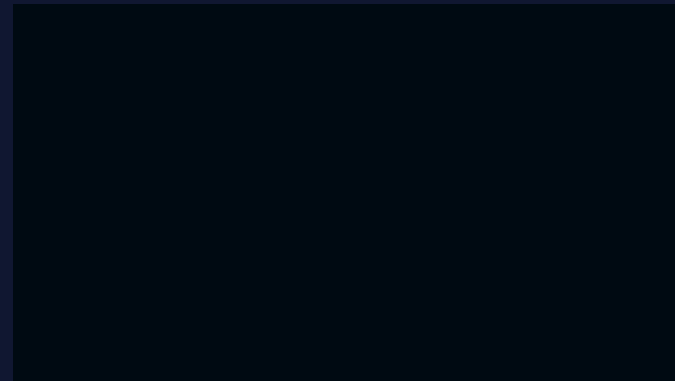
Audio /Graphical /Textual  
Training Assignment, Records  
Hosted and Integrated Services

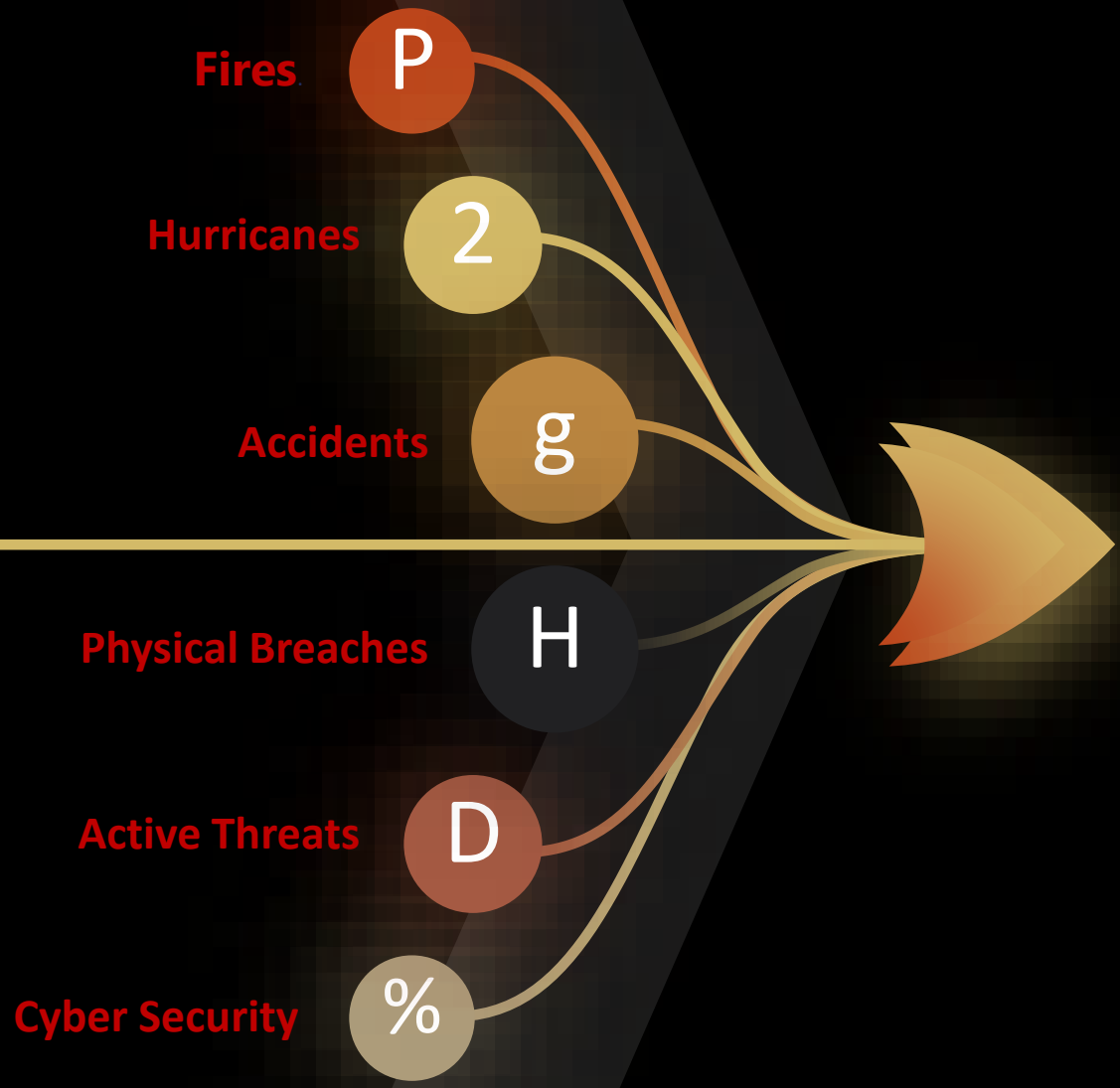
### Deployment Options



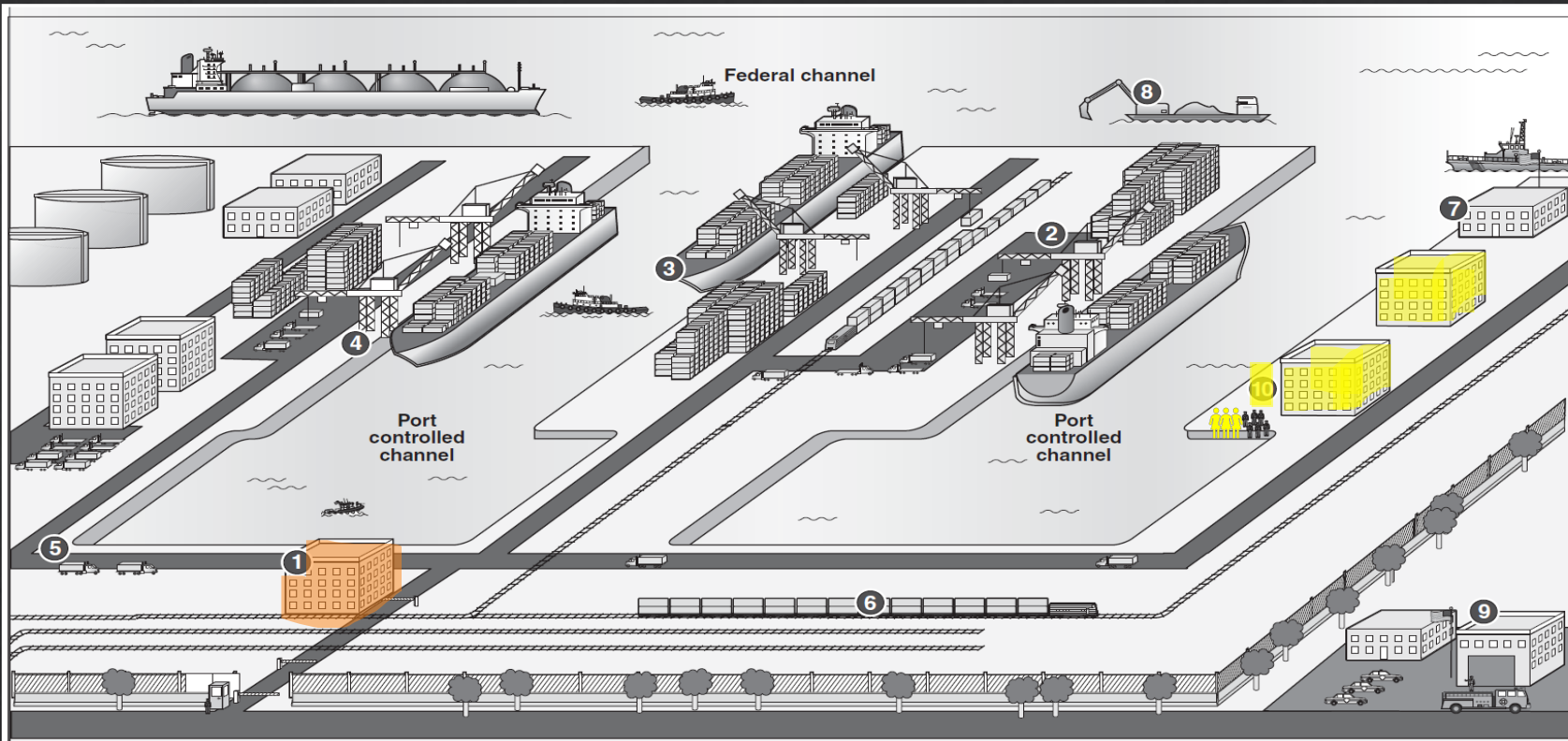
# We Communicate

Training - Training - Training















**Crisis** Can  
Come  
From Many  
Directions



# Fractured — Emergency Responsibilities

<p><b>1</b></p>  <p><b>Port authority</b> Provides limited governance structure for the port and may own port assets.</p>	<p><b>2</b></p>  <p><b>Terminal</b> The area for loading and unloading ships. It may be leased from the port authority by a private operator.</p>	<p><b>3</b></p>  <p><b>Container ship</b> Container ships bring goods to and from the port.</p>	<p><b>4</b></p>  <p><b>Gantry crane</b> A gantry crane is used to transfer containers and other types of cargo between ships and trucks or trains.</p>	<p><b>5</b></p>  <p><b>Trucking companies</b> Transport goods within the port and from the port to inland locations.</p>
<p><b>6</b></p>  <p><b>Rail carrier</b> Transport goods from the port to inland locations.</p>	<p><b>7</b></p>  <p><b>U.S. Coast Guard</b> Provides federal oversight of portwide safety and security.</p>	<p><b>8</b></p>  <p><b>U.S. Army Corps of Engineers</b> Maintains the federal channel leading to a port.</p>	<p><b>9</b></p>  <p><b>Emergency Management Agency</b> State or local agency helps coordinate disaster response services such as police, fire, and medical teams.</p>	<p><b>10</b></p>  <p><b>Information sharing forums</b> Provide a means of coordinating disaster planning among port stakeholders.</p>

# 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?



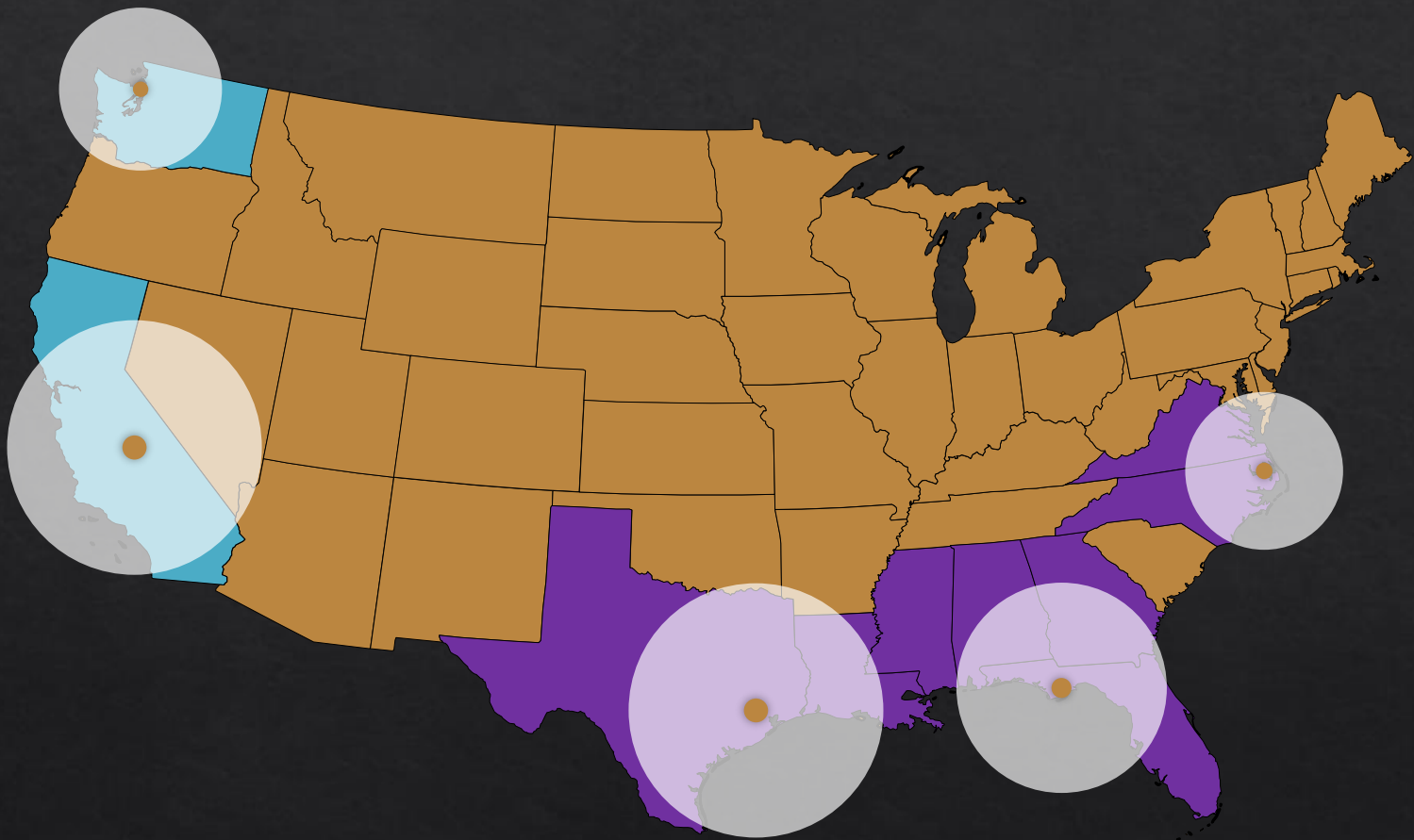


# How does your **Port** deal with . . .

- 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



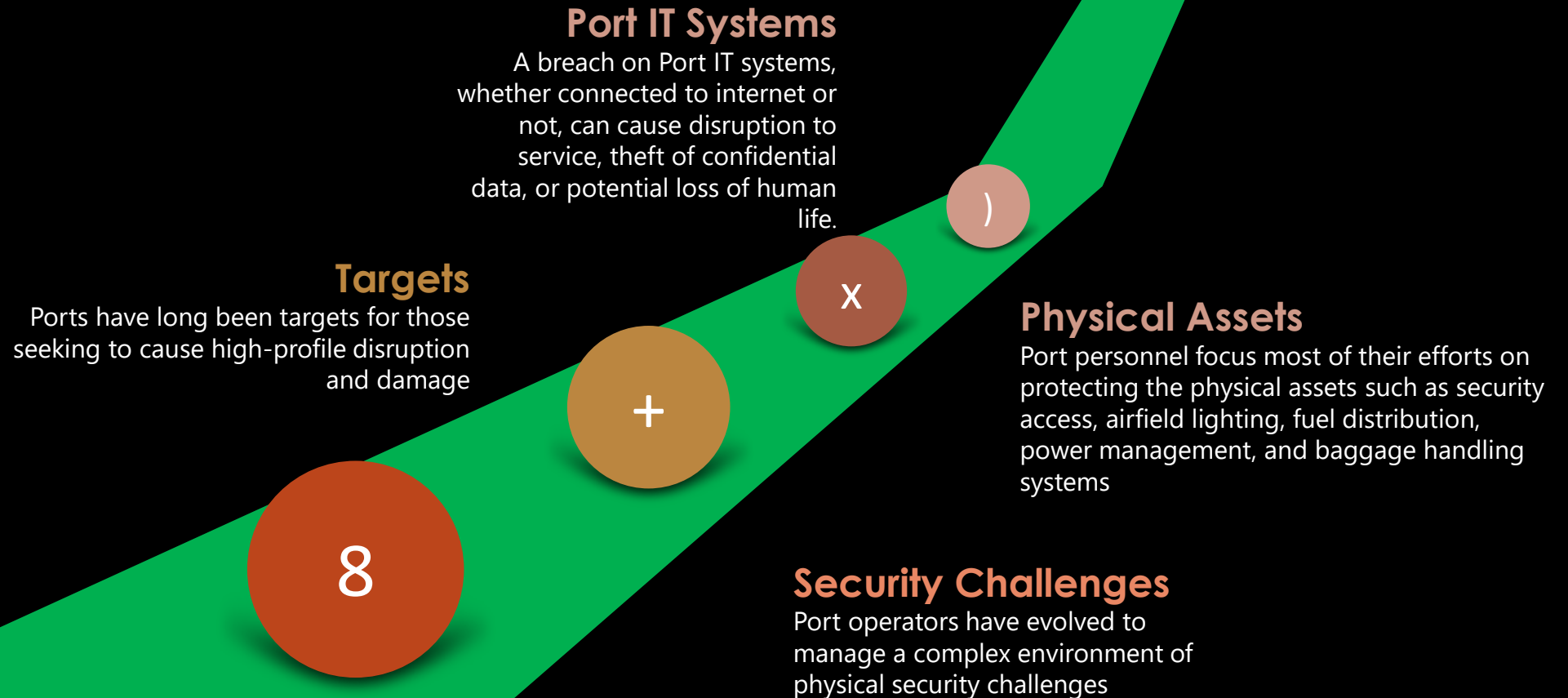
Port Threats

# 2019

Hurricanes & Tornadoes  
Earthquakes

# Evolving From Physical to Cyber Security

All these assets are controlled by Port IT systems



# Port 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.**





H

### Prime Targets

Ports are a prime target of computer hackers and other cyber criminals

A

### Continuous Targets

Ports continue to be targeted for attack by cybercriminals, hackers and nation-state actors

j

### 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

?

Market

Where do you  
think **Cyber  
Security** Ranks  
in Port Security  
importance?



1

**Security vulnerabilities, threats to avoid – especially when using electronic access control systems.**

# Attack Vectors

||  
Phishing

S Public Wi-Fi

Social Engineering C

Computer/Mobile Security

Passwords D





VoiceMAIL Service Alert Message from (714-490-9111)



WirelessV-Mail Center (+1714490911) <@WirelessVoiceNote voice@y0umail.com Wireless services intel Business>  
To

## YOU HAVE A NEW VOICEMAIL!

You have a new voicemail from 1 (714) 490-9111 (LOS ANGELES, CA)

This link will work for the Direct Recipient only.

2019-02-22 VOICENOTE

TO LISTEN, CLICK BELOW

[PLAY/LISTEN](#)

Microsoft respects your privacy. To learn more, please read our Privacy Policy.  
[Microsoft Corporation. One Microsoft Way, Redmond, WA 98073](#)



Office 365 Voice

CALLER ID: +1 (532) 122-7019\*\*\*@listenvm.rc.com <vm\_new\*\* -voicemailcenterattached-listen.sharepoint+attachedlisten\*\*\* -sharepoint\_newvoicemail <jmc  
To Lorena de Rodriguez  
New Wireless  
<https://www.taste-buds.org/ce78/?pop3=lorena@ssinstruction.com>,  
Click or tap to follow link.

[Listen WAV](#)

[Download WAV](#)

- IP Phone System Number: +1 (532) 122-\*\*\*\*
- CallerID: WAV783847
- Duration: 00:00:30secs.
- Provider: AT&T
- MessagingVOIP ID#: 93848940BEAVNVOIP093
- Date Received: Friday 29 March 2019

This is an automatically generated administrator.

Received at 02-22-2019 12:02:20 PM (33 seconds).  
Mobile Record <assistancehc7d9af8826rese96a6a6f9eb27e9d19@preswex.ie>  
To o365mc@microsoft.com



Received at 02/22/2019 12:02:20 PM (33 seconds).  
Outlook item

CALLER ID: +1 (\*\*\*) - \*\*\* - 2643  
Conference phone number: +1 (\*\*\*) - \*\*\* - 2643  
Audio Conferencing PIN: 80266

# 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

Release of Port executive's personal information, such as home address, email address, family member information and phone numbers (known as "doxing")

Theft of credit and debit card information from passengers and other visitors





## Challenge

?

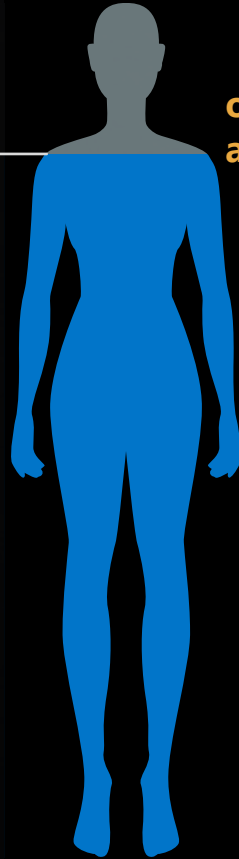
Market

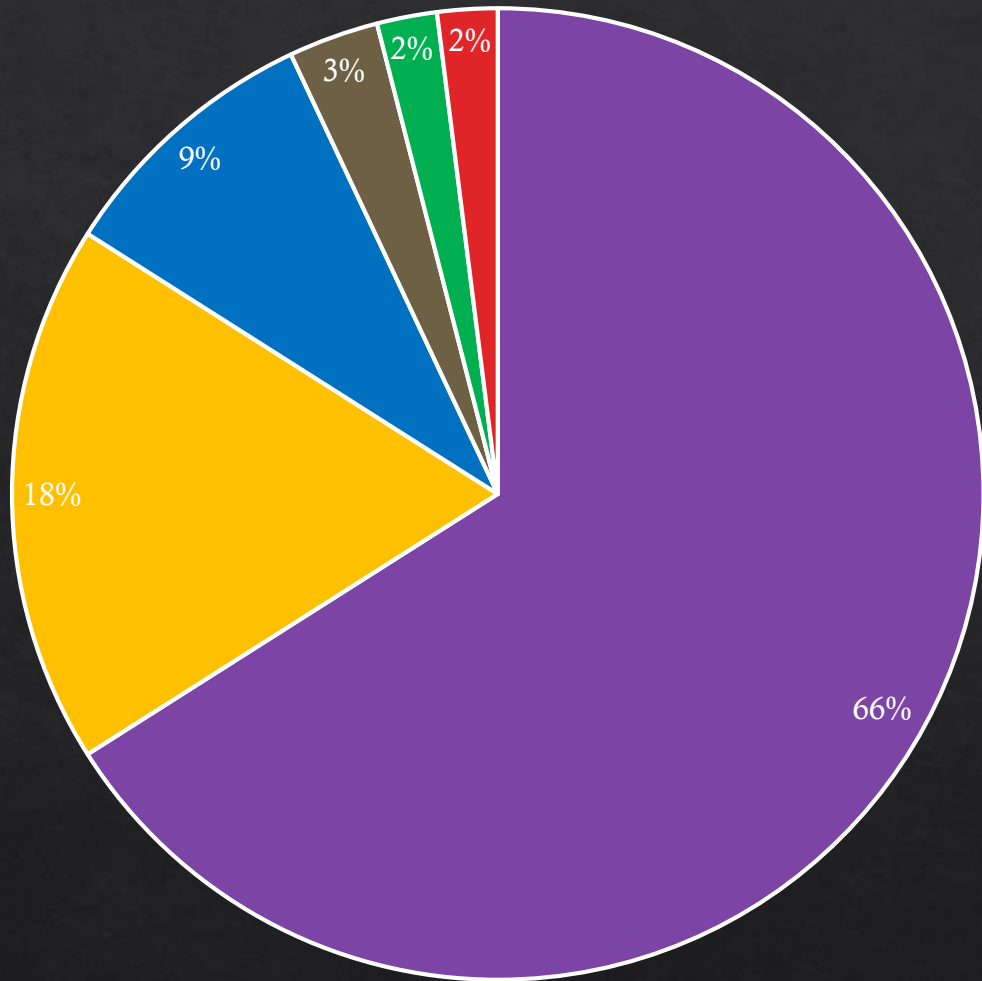
Where do most  
of the **cyber**  
**risks** come  
from?

91%

of all cyber breaches  
are caused by HUMANS

The  
**Error**  
Factor





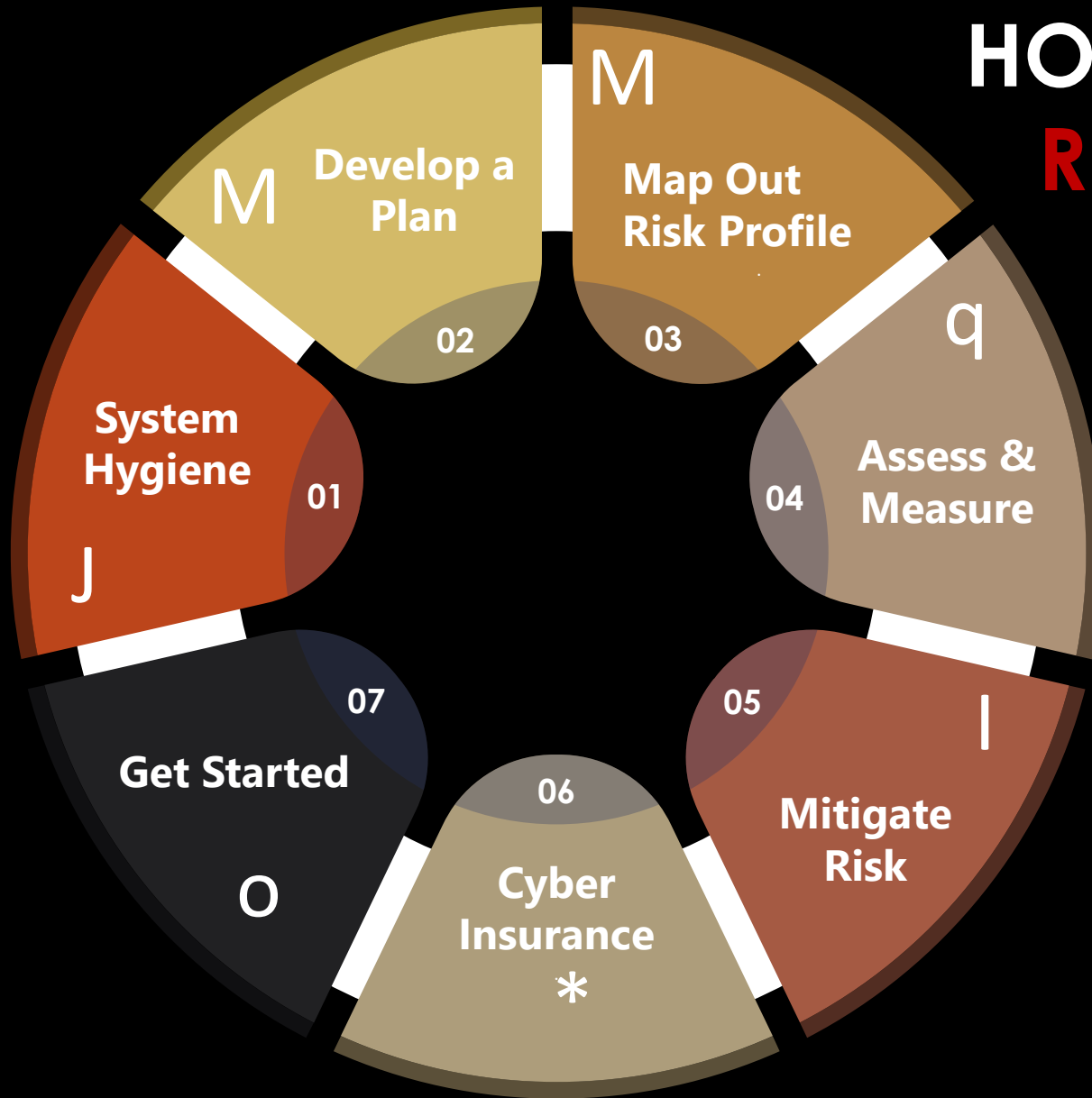
Source: Willis Tower Watson claim data

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



## Causes of Cyber Breaches

# HOW TO ACHIEVE **CYBER RESILIENCE** IN 7 STEPS



What can  
your **port** do?  
**GET STARTED!**

# Engaging **Strategies** to Use

X

Hold Regular Meetings

W

Post Regular Security Alerts in a Common Location

Y

Create a Community of Knowledge with Awareness Training

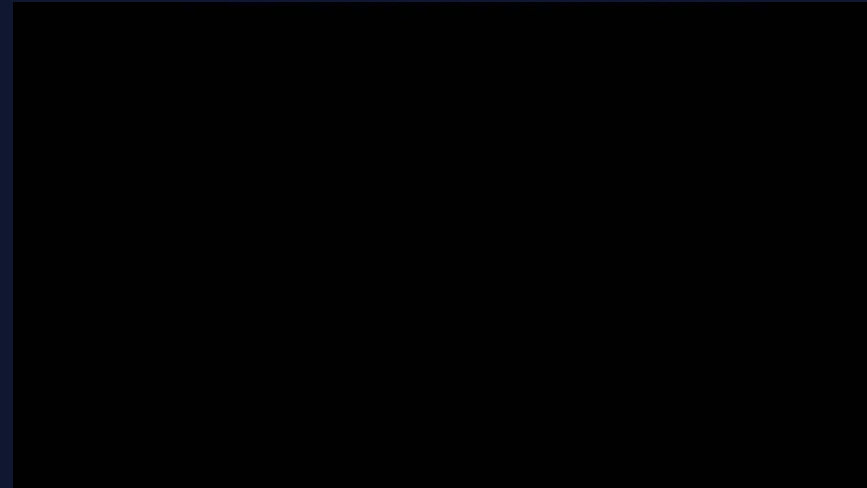


# How does your **Port** deal with . . .

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](http://www.SSinstruction.com)

[www.ARFFRecurrent.com](http://www.ARFFRecurrent.com)

1

@WeTrainAirports

@ARFF\_Training

\*

SSinstruction1

**Time** for questions!



**Thank you!**

**Emergency  
/ Security  
Awareness**

**Lorena de Rodriguez, *President, SSi, Inc.***