



Security for Critical Operations

Bryan Owen PE
OSIsoft – Security Architect



About.me

Recent activities

- 2020 SANS Michael J. Assante ICS Security Lifetime Achievement Award
- 2020 CISA Control Systems Interagency Working Group
- 2019 NERC GridSecCon Supply Chain Threat Vector
- 2019 PIWorld What you need to know about the PI System, DERS and Cybersecurity
- 2019 NSA Operational Technology and Cybersecurity
- 2019 S4 OnRamp ICS and the Cloud



About.us

Major PI System security milestones

- 2020 PI System Security Hardening
- 2017 Read only PI Connectors and Interfaces
- 2015 Transport Security using Windows Integrated Security
- 2012 PI Vision with application server design pattern
- 2009 PI Server with Windows Integrated Security
- 2006 PI Interface Node Security Hardening

Agenda

- Critical Operations
- Advice from cyber experts
- Destructive malware trends
- Customer experiences
- Evolution of OSIsoft guidance
- What to expect from OSIsoft in 2020
- Suggested PI World talks
- Call to Action



Our Mission: Make Operations Data an Asset Everyone Can Use in Real Time



Process Engineer

“Can we increase the overall yield?”



Control Room Tech

“The process is like a baby – you have to watch it.”



Production Manager

“What is the forecast of productivity?”



Data Scientist

“Can we find new savings with machine learning?”



Reporting Analyst

“I need to combine 3 data sources into 1 report.”



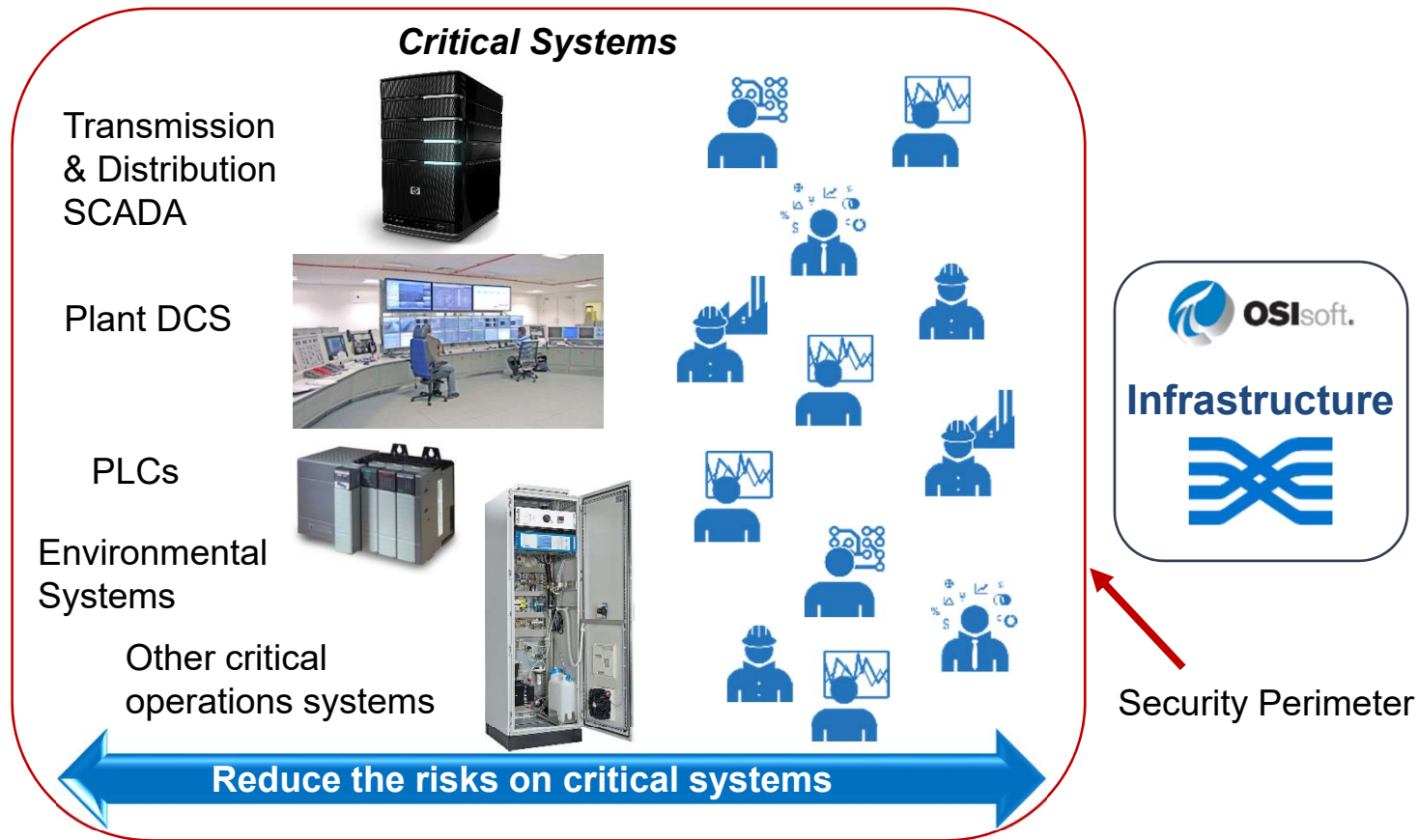
Maintenance Engineer

“I need to know the moment it goes out of tune.”

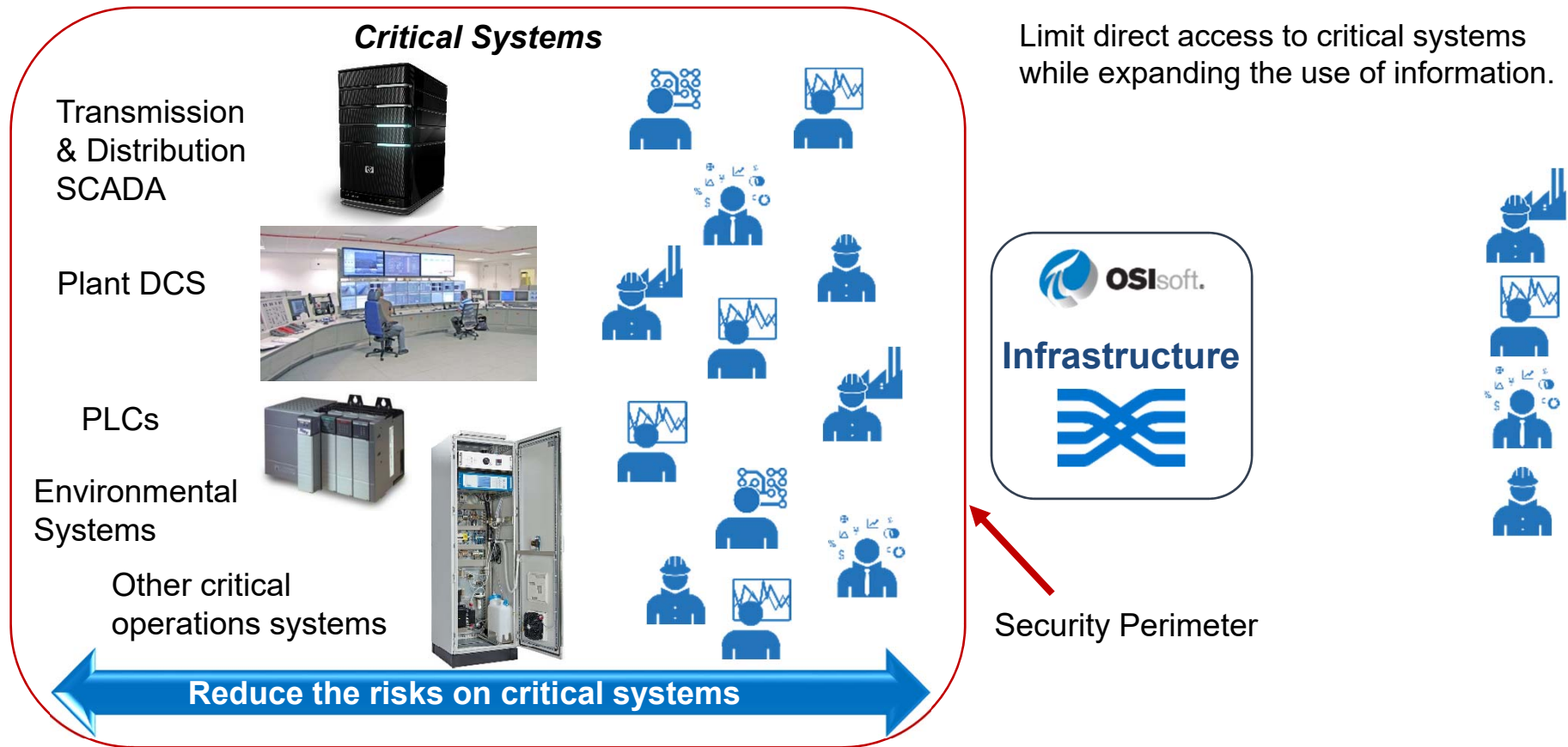
OSIsoft Leads the Market in Critical Operations



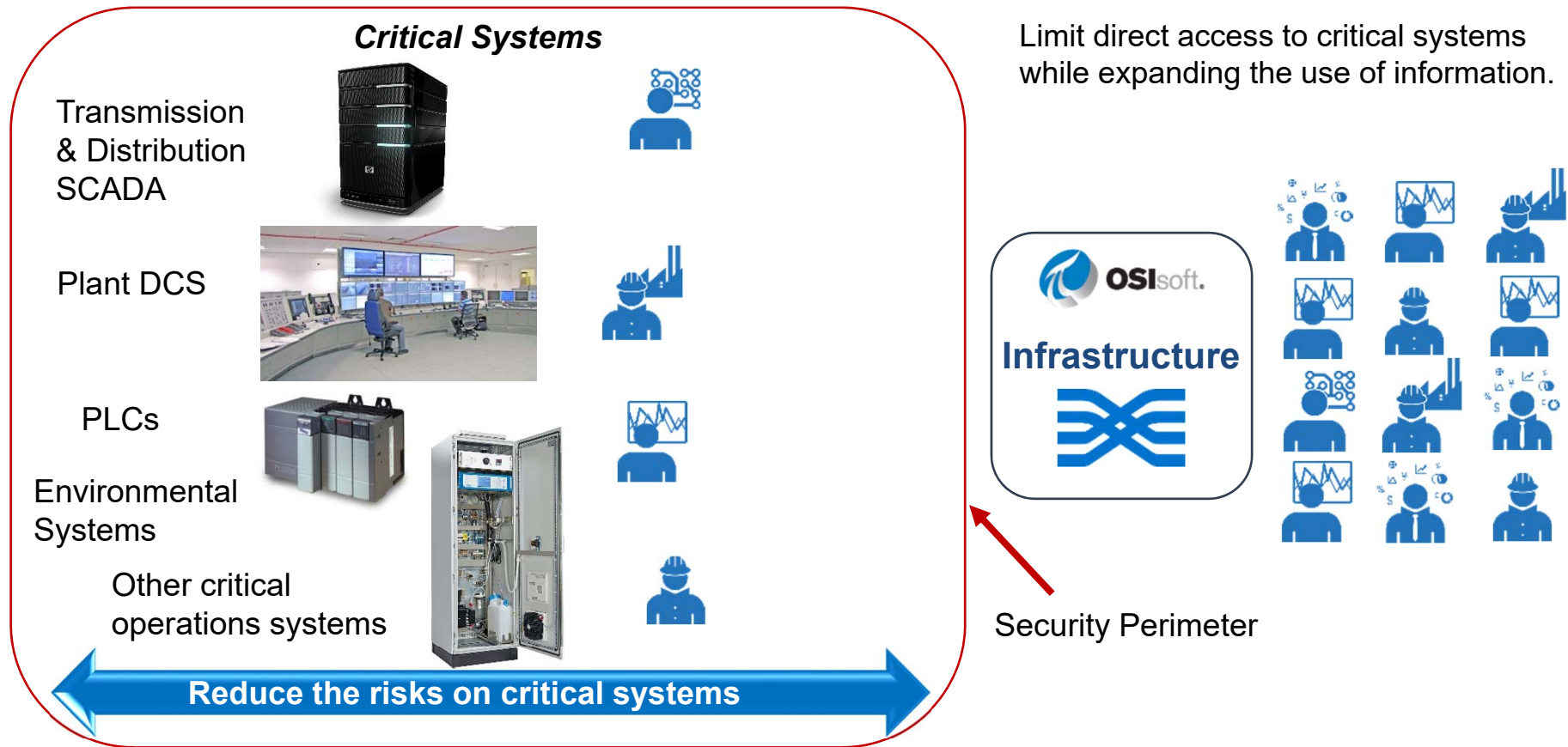
Architectural Concept: Dedicated Data Infrastructure



Architectural Concept: Dedicated Data Infrastructure



Architectural Concept: Dedicated Data Infrastructure




Critical Operations Mindset

A large offshore oil rig is illuminated at night, with its complex network of pipes, platforms, and cranes reflecting on the dark water. The sky is a deep blue with some clouds. The rig's lights create a bright, industrial scene.


Am I
collecting
all of the
data?

Critical Operations Mindset




Is the
system
always
available
?

Critical Operations Mindset

A large offshore oil rig is illuminated at night, with its complex network of pipes, platforms, and cranes reflecting on the dark water. The sky is a deep blue with some clouds. The rig's lights are bright yellow and white, creating a stark contrast with the dark surroundings.

Is it
**secure,
stable &
agile?**

Critical Operations Mindset

A large offshore oil rig is illuminated at night, with its complex structure of pipes, platforms, and cranes reflected in the dark water. The sky is a deep blue with some clouds. A large, light gray silhouette of a human head in profile is overlaid on the right side of the image, facing right. Inside the head, the text "Is it a system of record?" is written in a bold, black, sans-serif font.

Is it a
**system of
record?**

Critical Operations Mindset

Can we operate
while
compromised?

KIM ZETTER SECURITY 01.20.16 09:23 AM

NSA Hacker Chief Explains How to Keep Him Out of Your System



“If you really want to protect your network...
you have to know your network.”

October 2015

The Case for Simplicity in Energy Infrastructure

For Economic and National Security

Michael Assante, Tim Roxey, and Andy Bochman



‘we must reengineer selected last-mile and
endpoint elements of the grid’

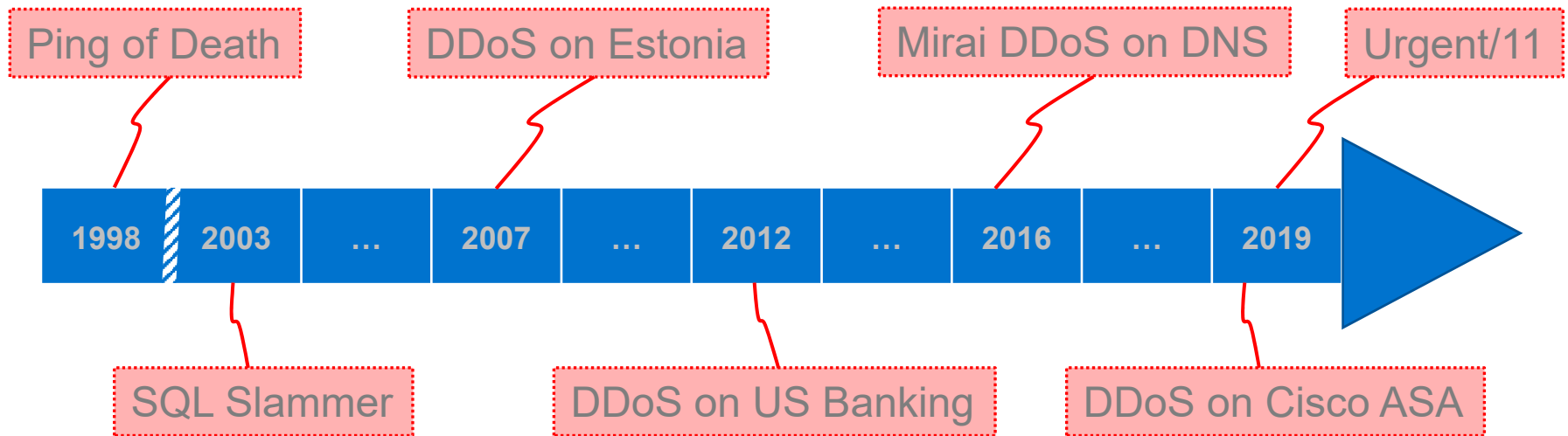


"Security is a team sport and everybody needs to be part of the solution. They should participate in their own rescue and security should be a celebrated part of organisational culture."

Ann Johnson

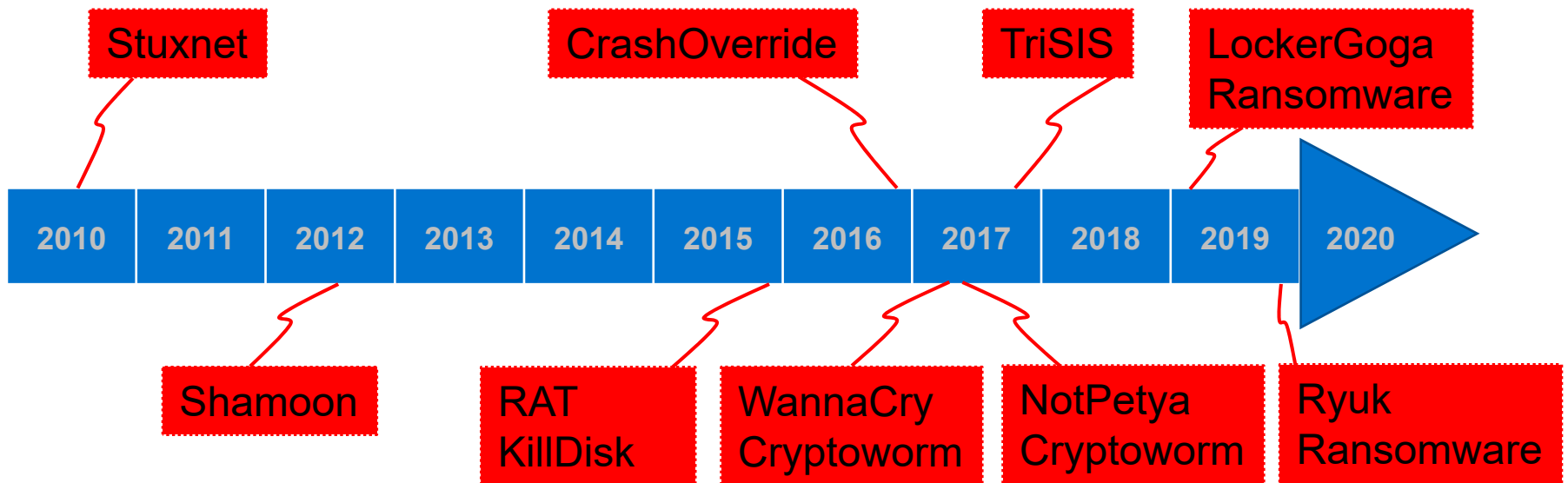
Vice President, Strategic, Enterprise & Cybersecurity, Microsoft

Trends in DoS attacks affecting critical operations



24/7 availability is a top concern for critical operations

The scope and scale of destructive malware affecting our industrial community is escalating



Stuxnet brought 'cyber war' into the open
...
Shamoon was the industry 'eye-opener'



The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

\$870,000,000	Pharmaceutical company Merck
\$400,000,000	Delivery company FedEx (through European subsidiary TNT Express)
\$384,000,000	French construction company Saint-Gobain
\$300,000,000	Danish shipping company Maersk
\$188,000,000	Snack company Mondelez (parent company of Nabisco and Cadbury)
\$129,000,000	British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)



Hurricane Maria's lessons for the drug industry

[Share](#)

Keeping Puerto Rico's pharmaceutical industry intact after the storm was a monumental task. A year later, companies consider how they can better prepare for the next natural disaster

by *Lisa M. Jarvis*

SEPTEMBER 17, 2018 | APPEARED IN **VOLUME 96, ISSUE 37**

'The makeshift solution was for a team at the company's headquarters in California, to print out the paperwork and fly it over to the island.'

Lessons Learned

No matter how much you plan,
no matter how much you train and
no matter how many contingency
plans you have,

You will be surprised.





Neil Walsh @NeilWalsh_UN · Apr 3, 2019

#Cybercrime and #cybersecurity compromises hurt #economic prosperity

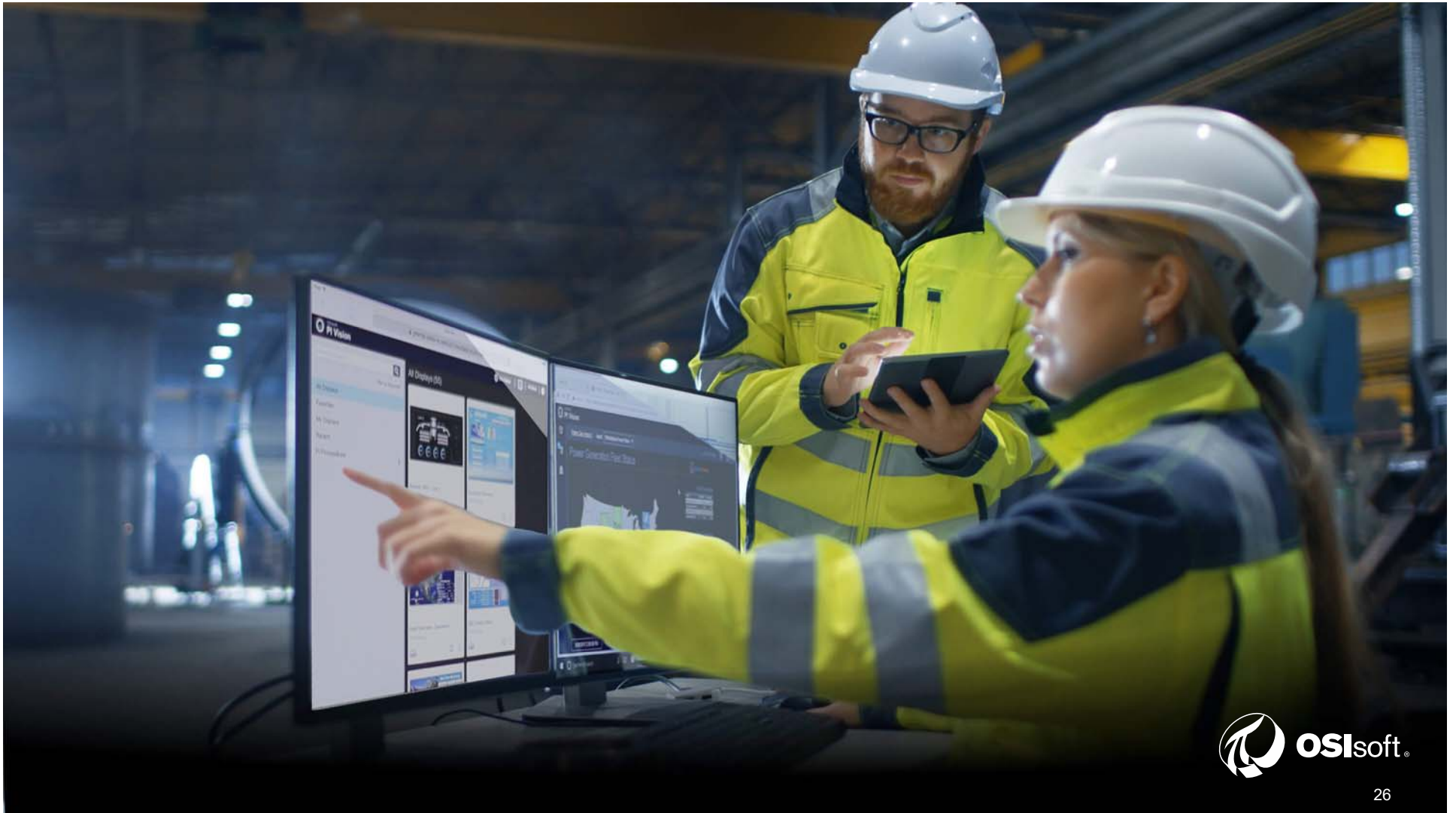
Here's how @NorskHydroASA recovered from #Lockergoga #ransomware @UN_Cyber

1. Transparency	daily webcasts and social media posts to keep business partners and the media informed – even control room visits
2. Don't pay the ransom	rebuild infrastructure to be safe and be sure that the attacker is not still part of it – don't feed the hackers
3. Cloud services	workers were still able to communicate via smartphones and tablets even without company computers
4. Empowered people	virtually all production back up to 100% normal, despite operating in manual mode – 'cyber heroes'

Microsoft Transform

<https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>

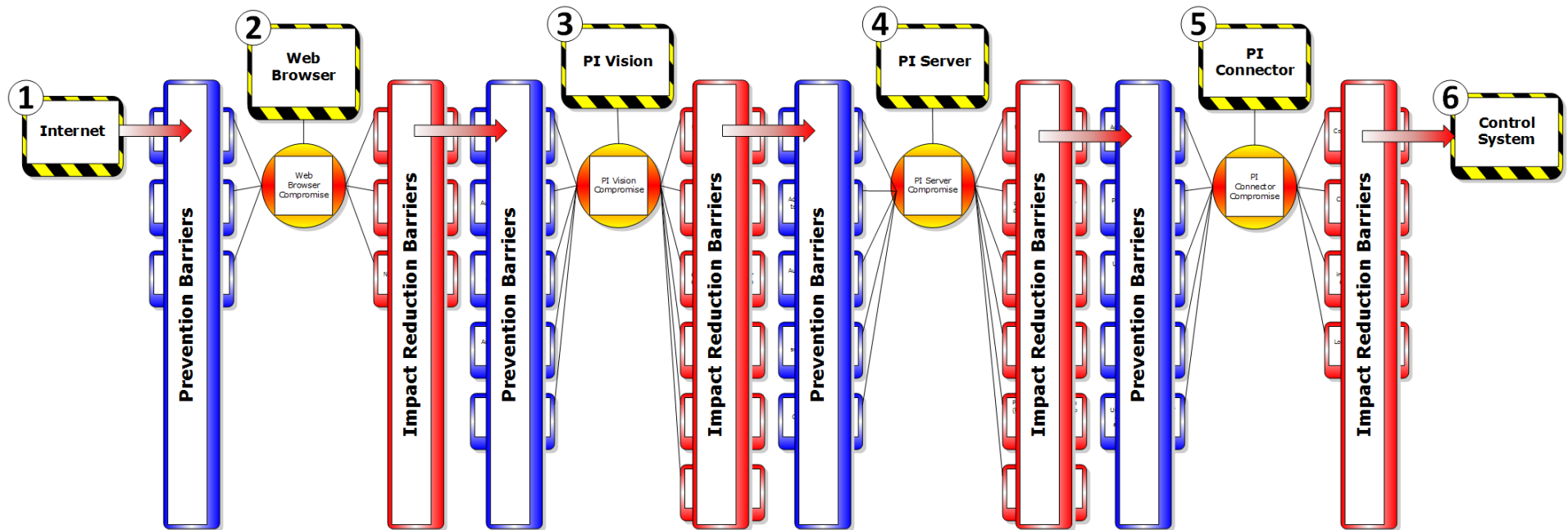
Tips so you can be a 'cyber hero' with the PI System.



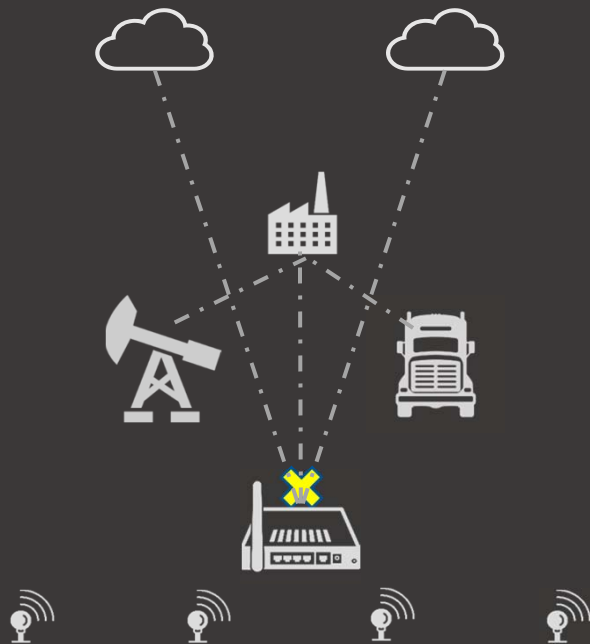
Know your PI System disconnect points



Make use of PI System security barriers



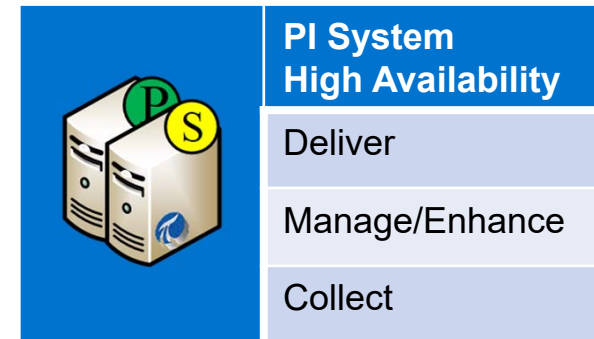
Edge Data Store is more than data collection



- Reengineered for ‘the last mile’ edge
- Data queues
- Local access with a restful API
 - e.g. display critical operations data while disconnected

Use the '3-2-1 rule' for critical operations data

- Three backups of your data
- Two different storage types
- One offsite backup – cloud!



Knowledge

PI Data Archive Backup Best Practices



Knowledge

How to Restore the PI AF Servers PIFD Database from Backup

Cloud enablement to enhance security



- Modern authentication
 - Across organizational boundaries
- Reduces third party access to corporate network
- Adds another option to access critical data streams
 - (e.g. BYOD during a crisis)

Recommended PI World talks and labs

- PI World 2020
 - Migrating from PI ProcessBook to PI Vision
 - Flexible Connectivity Strategies for OCS and the PI System
 - Making PI Data Ingress cOMFortable with PI Web API
- PI World Encores
 - [Security and Hardening Your PI System](#)
 - [OSIsoft Cloud Services Security](#)
 - [Using the System Connector to Build a Strong Security Posture](#)

Enhance your security measures to combat cyber crime

CHALLENGES

- Cyber risk reduction investment priorities
- Increase security without slowing down digital transformation
- Capability to operate while compromised

SOLUTION

- Create awareness of losses and impact to critical operations
- Enable your people and security barriers built into the PI System
- Know what systems can be trusted for response and recovery

BENEFITS

- Avoid significant losses and recovery costs (*in the hundreds of millions!*)



**We live in an industrial world.
Going after industrial security, and doing it well, is worth doing.**



Robert Lee CEO Dragos, Inc (OSIsoft security partner)

Contact



- Bryan Owen PE
- Security Architect
- OSIssoft
- bryan@osisoft.com



Questions?

Please wait for
the **microphone**

State your
name & company



Save the Date...



REGISTER YOUR INTEREST

AMSTERDAM

October 26-29, 2020



