

# Risk and Security



# Risk and Security

Risk Assessment defined:

A method to identify the risks and all probable effects that those risks will have on the person(s) and/or organization being protected, to minimize that risk to an acceptable level, and the proper implementation of or measures to deal with the remaining elements associated with that risk.

# Common Risk Terms

Risk Reduction: Identification of significant risks to the organization that can be systematically reduced or eliminated. Typically achieved through implementation of appropriate programs.

Risk Avoidance. Taking steps to remove a hazard; engaging in an alternate activity; and/or ending a specific exposure.

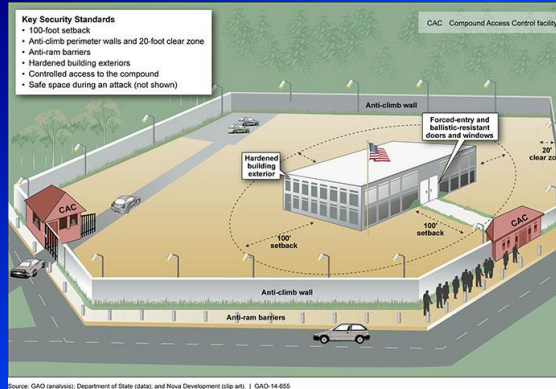
Risk Transfer. An insurable risk is transferred to another party through insurance or warranty.

Risk Elimination. If the risk is too great to accept, end the activity, sell it off, or cease operations.

# Risk and Security

Yesterday and Today

# Yesterday



# Today's Additional Stressors



# Workplace Violence



*“A spectrum of behaviors that generates a reasonable concern for safety”*

- A nexus exists between the behavior and the physical safety of employees.
- Can be anything from verbal threats all the way to workplace mass shootings.
- Dilemma: Spend the extra money to stand up required resources or risk potential litigation.

# Workplace Violence

*“Employers have a legal and ethical obligation to promote a work environment free from threats and violence and, in addition, can face economic loss as the result of violence in the form of lost work time, damaged employee morale and productivity, increased workers’ compensation payments, medical expenses, and possible lawsuits and liability costs.”*

FBI

*“Employers have an obligation to ensure that reasonable steps are taken to prevent harm to employees, customers, and visitors.”*

OSHA



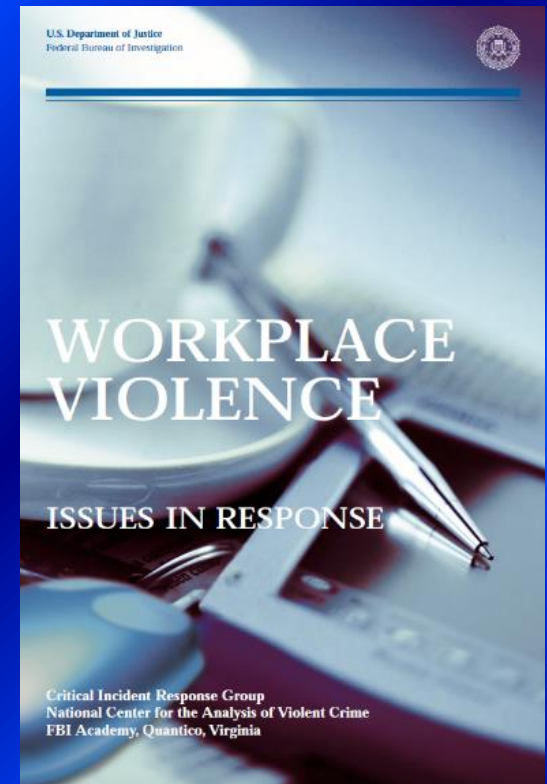
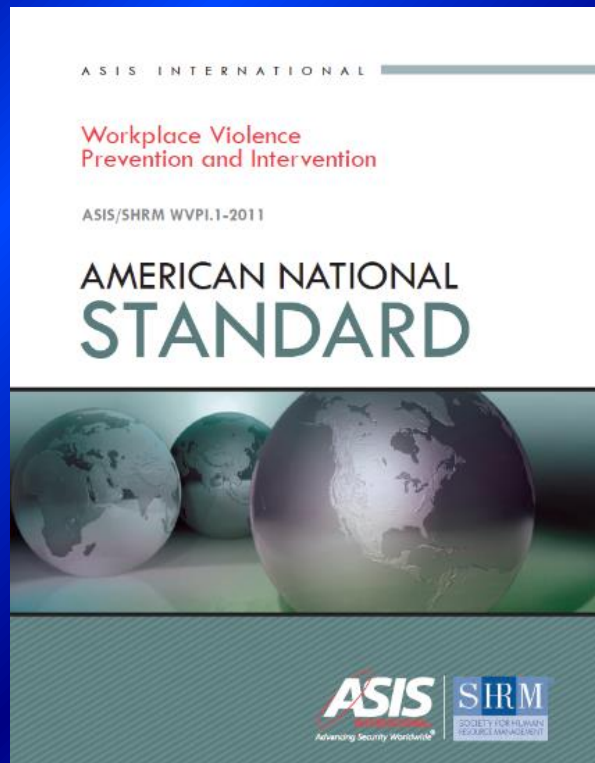
# Workplace Violence

*Will having a Workplace Violence Program somehow magically save my firm or institution from acts of violence?*

Maybe not - but it will put you in a much better position on these:

- ❖ Avoid hiring potentially problematic employees.
- ❖ Initial and follow-up response actions.
- ❖ Required internal and external relationships.
- ❖ Legal and ethical responsibilities (litigation).

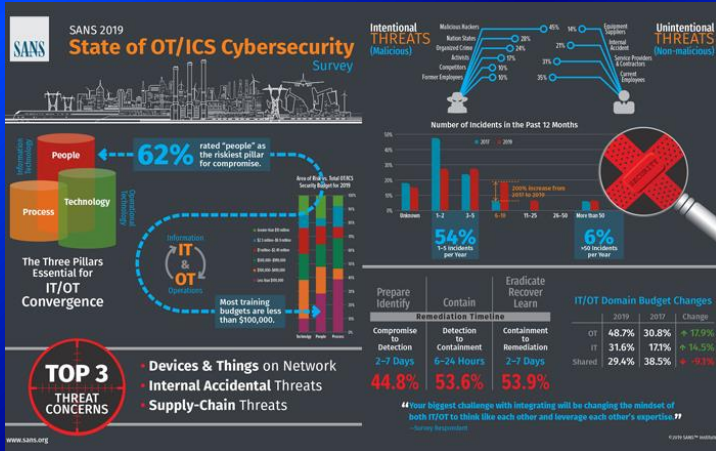
# Resources



*Workplace Violence Issues in Response, National Center for the Analysis of Violent Crime, FBI Academy, Quantico, Virginia.*

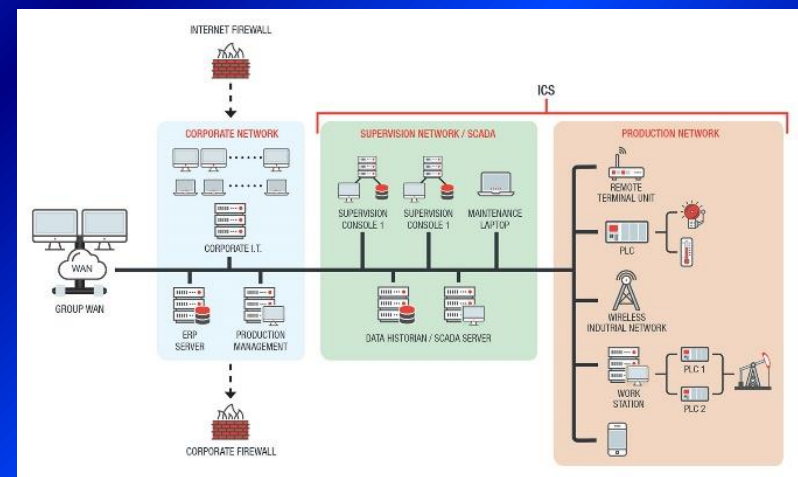
*Workplace Violence Prevention and Intervention, ASIS Standard ASIS/SHRM WVPI.1-2011, Society for Human Resource Management, ASIS International.*

# Cybersecurity



## INDUSTRIAL CONTROL SYSTEM CYBERSECURITY

WITH GREAT CONNECTIVITY COMES GREAT RISK. PROTECT CORE OPERATIONS WITH SECURITY EXPERTISE AND INDUSTRY INSIGHT.





# Information Technology

## Industrial Control Systems

- Programmable Logic Controller (PLC). Reads binary code of a logic statement (command).
- Distributed Control System (DCS). Provides instruction to machines.
- Supervisory Control and Data Acquisition (SCADA). Gathers and displays data remote to the process.
- Human Machine Interface (HMI). A 'localized' version of SCADA.

# Cyber Resources

*NIST Cybersecurity Framework.* National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>

*Industrial Control System Cyber Emergency Response Team.*  
<https://www.us-cert.gov/ics>

*United States Computer Emergency Readiness Team.* <https://www.us-cert.gov/>

*National Cybersecurity and Communications Integration Center.*  
<https://www.us-cert.gov/nccic>

*United States Coast Guard Cyber Strategy.*  
[https://www.uscg.mil/Portals/6/Documents/PDF/CG\\_Cyber\\_Strategy.pdf](https://www.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf)

# Unmanned Aerial Vehicles

- Weaponized or smuggled payloads.
- Prohibited surveillance.
- Intellectual property theft.
- Crimes and trade secret theft.
- Disruption or harassment.



# Autonomous Surface Vehicles



- Mobile Buoys/Station Keeping
- Towed Targets
- Surveys
- Monitoring
- Research & Data Collection



# Business Continuity

Defined: The ability to ensure critical processes and core business functions are not severely impacted by disaster or unplanned events and continue unimpeded.

## Risk Assessment Process:

*Identify critical functions.*

*Identify supporting functions.*

*Consider dependencies/interdependencies.*

*Consider threats and consequences.*

*Implement mitigation strategies.*

# Business Continuity

*Mission-essential Functions*: Functions that cannot be deferred in a continuity situation.

*Business-critical Functions*: Business activities that must be restored in the event of a disruption to ensure protection organizational assets, needs, and regulations.

*Essential Supporting Activities*: Critical functions that an Organization must continue during a continuity activation, but that do not meet the definition of essential.

# Business Continuity

## Mission-essential functions:

- Providing JIT deliveries of bulk Butadiene to clients in the Port of Zambi .
- Providing Benzene shipments to refineries X and Y in Port Charles.

## Supporting functions

- Shipping/Receiving
- Trucking/Rail Lines
- HR/Payroll

## Dependencies

- Plant needs water from the City of Port Charles.
- Plant needs electricity from Acme Power Plant.

## Interdependencies

- XYZ Railroad provides the plant with coal for fuel which in turn allows the plant to produce electricity for rail line signals, switches, and control center.

# Business Continuity

## Suggested focus:

- Bulk Butadiene storage
- Bulk Benzene storage
- Rail Yard
- Truck loading dock
- Water main
- Plant substation

# Weather Risk

Inland versus coastal ports

Hurricane/Typhoon conditions of readiness

USCG Port Conditions

Have a plan and be flexible

# In Summary

- Business Continuity
- Cybersecurity
- Workplace Violence
- Understand Potential Weather Impacts

# Contact

John Bray

(361) 939-0415

[John.M.Bray@uscg.mil](mailto:John.M.Bray@uscg.mil)