Risk and Awareness for 100

A documented formal security training and awareness policy and program is designed to?

(name at least 2 examples)

Training and awareness programs are designed to:

- keep staff up to date on:
  - organizational security policies and procedures
  - industry cybersecurity standards
  - recommended practices
  - vulnerabilities

Without training on specific ICS policies and procedures, staff cannot be expected to maintain a secure ICS environment.

Guidance: Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions

Risk and Awareness for 200

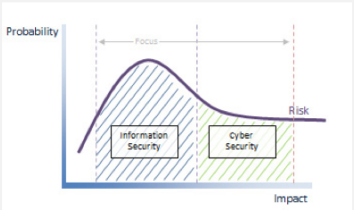
What is the ”traditional” cyber risk equation?

ABS Advanced Solutions

The “traditional” risk equation is…

Risk = <u>Threat</u> X Vulnerability X Consequence.

- The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.
- Threats:
  - specially designed malwares
  - manipulated hardware and firmware
  - the usage of stolen certifications
  - spies and informants
  - exploiting vulnerabilities in archaic hardware
  - attacking third-party service providers
  - advanced persistent threats



Source: Steven Chabinsky, Deputy Assistant Director, FBI Cyber Division, Armed Forces Communications and Electronics Association Homeland Security Conference, Washington D.C., 2010

ABS Advanced Solutions

Risk and Awareness for 300

Cybersecurity is really a balance of <<?>> versus cost?

ABS Advanced Solutions

Risk vs Cost

There is not a one-size-fits-all set of cybersecurity practices.

Cybersecurity is really a balance of RISK versus cost.

All situations will be different.

Source: ISA-62443-1-3 Security for industrial automation and control systems

ABS Advanced Solutions

Risk and Awareness for 400

Is cyber security policy strategic?

ABS Advanced Solutions

Cyber Security Policy is Strategic

- Cyber Security Policy is a strategic element of a security program and may be a strategic element of the business strategy.
- Standards, Guidelines, and Procedures are all tactical elements of a cyber security program

ABS Advanced Solutions

Risk and Awareness for 500

What is the primary goal of a cybersecurity policy?

ABS Advanced Solutions

The primary goal of a security policy is:

To influence secure behavior.

ABS Advanced Solutions

IT and OT for 100

Describe the priorities of protection for Operational Technology.

ABS Advanced Solutions

OT priorities are the inverse of IT

Operational Technology	System Priorities	Information Technology
Highest ↑	**Availability**: Ensuring timely & reliable access	Lowest ↓
	Integrity: Performing its intended functions	
Lowest	**Confidentiality**: Preserving authorized restrictions	Highest

ABS Advanced Solutions

IT and OT for 200

Why is “scanning” and “penetration testing” a potential issue for Operational Technologies?

OT systems aren’t necessarily built for IT tools and techniques

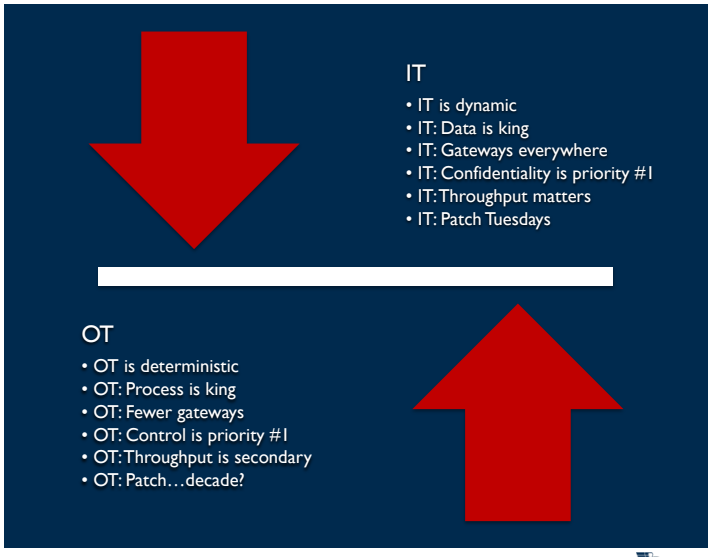
- A “ping” sweep destroyed over $50,000 in product at a semiconductor factory
- A gas distribution system was blocked for several hours after a penetration tester went slightly off-perimeter during an assessment for a gas company

IT and OT for 300

Name different characteristics of OT and IT - ”OT is x while IT is y”…

ABS Advanced Solutions

Characteristics of OT and IT



ABS Advanced Solutions

IT and OT for 400

Name 2 reasons OT systems weren't designed with cyber security in mind.

ABS Advanced Solutions

OT System Design

- Many systems are old and designed when cyber security was not the prevalent risk it is today and the known cyber risks/threats were significantly less sophisticated that those today
- Many were designed with the thought that they would be "air gapped" from other systems – i.e. not connected physically (or wirelessly) to other systems that had unknown exposure and could introduce vulnerabilities (i.e. other IT systems on the business network or the internet)

ABS Advanced Solutions

IT and OT for 500

Name at least 4 “high-value” governance activities that contribute the most to reducing operational cyber security risk?

ABS Advanced Solutions

High-Value Governance Activities:

- Cyber Awareness Training
- Software Inventory
- Updated System/Network Maps
- Controlling Physical Access to Operational Technologies
- Operational Technology Network Segmentation
- Formal Identification of Vulnerabilities
- Co-mingling IT and OT Groups/Teams
- Monitoring OT Systems and Networks
- Periodic Risk Assessments

ABS Advanced Solutions

Cyber Hygiene for 100

What is the “first line” of cyber defense”?

ABS Advanced Solutions

The First Line of Cyber Defense is:

Trained cyber security personnel.

ABS Advanced Solutions

Cyber Hygiene for 200

Who should be allowed to access a SECURED network?

A Secured Network Should Only be Accessed by:

Authorized personnel.

Cyber Hygiene for 300

What should be done to ANY external memory device before it is connected to a protected system?

ABS Advanced Solutions

External Memory Devices Should be:

- Considered as a corruption vector and other ways to connect/xfer stored data (email file vs USB xfer if corporate controls are strong) should be considered
- Scanned for malware
- Governed by a written policy
- Authorized by the system owner before connecting

ABS Advanced Solutions

Cyber Hygiene for 400

Name a simple, system administrative task to be performed before a system is made operational.

ABS Advanced Solutions

Pre-Operational System Task:

Change default or supplier provided passwords

ABS Advanced Solutions

Cyber Hygiene for 500

Name at least two ways to securely manage wireless-enabled devices operated NEAR protected systems.

ABS Advanced Solutions

To Securely Manage Wireless Devices:

- Prohibit device access
- Authorize device access
- Disable device wireless operation

ABS Advanced Solutions

Rules and Regulation for 100

Briefly describe the USCG CG-5P Policy Letter No. 08-16 14 December 2016

CG-5P Policy Letter No. 08-16 14 December 2016

- REPORTING SUSPICIOUS ACTIVITY AND BREACHES OF SECURITY
- An owner or operator of a vessel or facility that is required to maintain an approved security plan in accordance with parts 104, 105 or 106 of Reference
  - (a) shall, without delay, report activities that may result in a Transportation Security Incident (TSI) to the National Response Center (NRC), including Suspicious Activity or a Breach of Security.

Rules and Regulation for 200

What cyber related requirement can be expected by IMO in the near future?

Extra credit if you know the committee name!

IMO Maritime Safety Committee (MSC) Resolution

- Resolution MSC.428(98) affirms that an approved safety management system should take into account cyber risk management and encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021

Rules and Regulation for 300

What cyber elements are prescribed in TMSA3?

ABS Advanced Solutions

TMSA 3

Cyber risk management has been included in TMSA 3 under elements 7 and 13. KPI 7.3.3 includes cyber security as an assigned responsibility for software management in the best practice guidelines. Under element 13 security threats are to be managed.

ABS Advanced Solutions

Rules and Regulation for 400

Per TMSA3: ”The company is involved in the testing and implementation of innovative security technology and systems.”

What does this include? IT systems? OT systems? Both?

TMSA 3 13.4.5 Addresses IT Systems

			• Manning levels.
	13.4.5	The company is involved in the testing and implementation of innovative security technology and systems.	This may include: • Physical measures to improve security. • Software enhancements to IT systems.

Rules and Regulation for 500

Interpret the draft USCG Navigation and Vessel Inspection Circular NVIC 05-17, titled "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. Or for short: "Title 33 Code of Federal Regulations Parts 105 & 106 Subpart C"

ABS Advanced Solutions

USCG NVIC

- Requires facilities to conduct security assessments that identify vulnerabilities with their physical security, as well as computer systems and networks
- Based on the security assessment results, facility owners and operators are required to develop mitigation strategies and document the strategies in their facility security plans
- Provides guidance on implementing a cyber-risk management governance program

ABS Advanced Solutions

Potpourri for 100

"All communications between our site and <Company Name> will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via out-of-band shared secret, or PKI certificates."

Policy? Standard? or Guideline?

ABS Advanced Solutions

Policy? Standard? Guideline?

Standard.

A standard is typically a collection of system-specific or procedural-specific requirements that must be met by everyone.

Source: SANS Institute - www.sans.org

ABS Advanced Solutions

Potpourri for 200

Policy communication is important because…

ABS Advanced Solutions

Policy communication is important because…

- The organization's personnel can not be held responsible for their actions unless it can be demonstrated that they were aware of the policy prior to any enforcement attempts.
- Mitigation of corporate and personal liability.
- Increased effectiveness of cyber security safeguards;
  - Increased integrity of the entire infrastructure
  - Increased ROI from the organization's investment in cyber security
  - Increased ROI in the asset in general

ABS Advanced Solutions

Potpourri for 300

Name 3 of the 4 main things an “identity management” system does?

ABS Advanced Solutions

Identity Management Systems:

Identify users of controlled or protected assets

Enroll authorized users of those assets

Authenticate access privileges for using those assets

Initialize/Remove user access privileges and credentials for those assets

ABS Advanced Solutions

Potpourri for 400

Why is the traditional Risk Equation not really a mathematical equation?

Risk = Consequence x Vulnerability x Threat

ABS Advanced Solutions

The Factors Aren't Calculable:

- Consequence = Money? Lost life? Pain?
- Vulnerability = Lack of protection?
- Threat = Modes? Cleverness? Attempts?

It's a useful concept, but not an "equation." An equation has a quantitative solution.

ABS Advanced Solutions

Potpourri for 500

Of the 10 Model Domains presented in C2M2, how many specifically require a Risk Model as a reference?

ABS Advanced Solutions

Answer: Nine (9) of Ten (10)

1. **Risk Management:** Establish, operate, and maintain an enterprise cybersecurity risk management program **to identify, analyze, and mitigate cybersecurity risk**….
2. **Asset, Change, and Configuration Management:** Manage the organization's IT and OT assets, including both hardware and software, **commensurate with the risk**….
3. Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, **commensurate with the risk**….
4. **Threat and Vulnerability Management:** Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, **commensurate with the risk**….
5. **Situational Awareness:** Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information….
6. **Information Sharing and Communications:** Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, **commensurate with the risk**….
7. **Event and Incident Response, Continuity of Operations:** Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, **commensurate with the risk**….
8. **Supply Chain and External Dependencies Management:** Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, **commensurate with the risk**….
9. **Workforce Management:** Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, **commensurate with the risk**….
10. **Cybersecurity Program Management:** Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the **organization's strategic objectives and the risk to critical infrastructure**.

ABS Advanced Solutions