Identifying Control System Cybersecurity Incidents

MLM-038-A

Industry	–	All
Principal Role	–	Owner
Professional Role	–	All
Enterprise Phase	–	Master Planning

Image from PowerPoint Stock Images

Turn on your audio and click start to begin video

START

This Micro-Learning Module describes industrial cybersecurity incidents including useful definitions, causes and characteristics, and key actions when incidents are detected.

ISA 62443 Cybersecurity Definitions

Event - An occurrence of or a change to a particular set of circumstances.

Incident - An event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system.

Security Incident - A Security compromise that is of some significance to the asset owner, or a failed attempt to compromise the system whose result could have been of significance to the asset owner. This includes physical, human, and system security incidents.

Industrial Cybersecurity Incident - An unauthorized internal, external, or supply chain-initiated activity that threatens the operating Safety, Reliability, or Performance of the process run by the Automation or OT system.

2

ISA-62443 defines an "Event" as an occurrence of, or a change to, a particular set of circumstances. See ISA-62443-3-3.

An "Incident" is defined as an Event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system. See ISA-62443-4-2.

A Security Incident is defined as a security compromise that is of some significance to the asset owner, or a failed attempt to compromise the system whose result could have been of some significance to the asset owner. See ISA-62443-1-1,. This includes physical perimeter security, human security, and control and information system security.

PERA adds a definition of an "Industrial Cybersecurity Incident" as: Any unauthorized internal, external, or supply chain-initiated activity that and threatens the operating Safety, Reliability, and Performance of the process run by the Automation or OT system

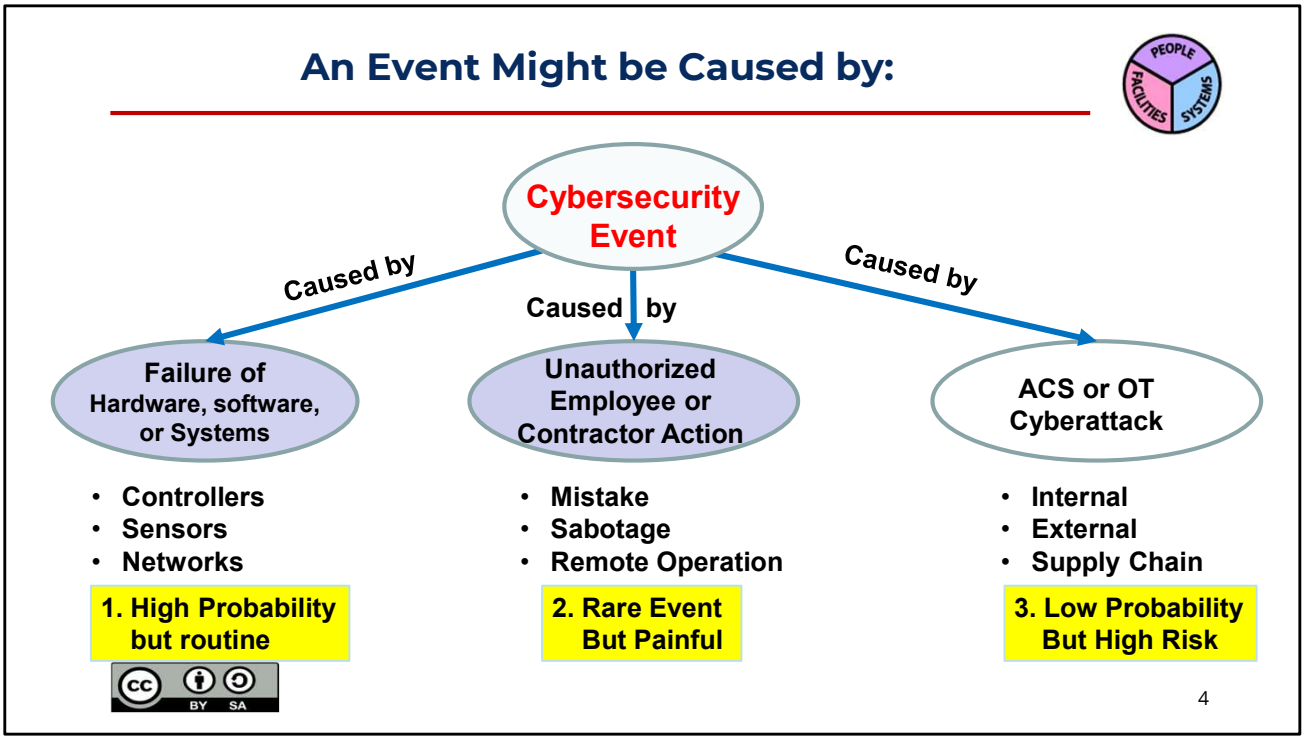
An Industrial Cybersecurity Incident Could Be

- **An Internal attack, e.g.,**
  - Physically inserting a compromised device
  - Action by employee
- **An External attack, e.g.,**
  - Direct penetration of ACS from Internet or via radio networks
  - Compromising the IT, and from there attacking an ACS or OT device or network.
- **A Supply chain attack, e.g.,**
  - Faulty software update or remote support
  - Tampered product (e.g. after repair)

3

An Industrial Cybersecurity Incident could be:

- An Internal attack, e.g.,
  - Physically inserting a compromised device
  - Action by employee
- An External attack, e.g.,
  - Direct penetration of ACS from Internet or via radio networks
  - Compromising the IT, and from there attacking an ACS or OT device or network.
- A Supply chain attack, e.g.,
  - A Faulty update or faulty remote service or support
  - Products that have been tampered with (e.g. after repair)



An Event (an occurrence or change) may be caused by:

- A failure of hardware, software or systems such as controllers, sensors or networks
- An action of a plant employee or contractor such as a mistake, sabotage, or remote operation
- A cybersecurity attack on ACS or OT systems. These may be Internal (plant people), External (external hackers), or Supply Chain (products or services).

The most common event is caused by a failure of hardware, software, or systems. This is high probability but routinely dealt with. impact may be limited by quick response.
The next most common event is probably an unauthorized action by an employee or contractor. These events are rare but may be difficult to detect and costly.
The least common event is probably an ACS or OT cyber-attack. These events risk plant safety and production and may be very difficult to detect.

How is Cybersecurity Investment Justified? (1 of 2)

An ACS/OT Cyber Attack is the least likely cause of a Cybersecurity Incident

- Product failures (computer or network hardware, software, or field sensor) are the most likely cause.
- Action by an employee or contractor (malicious or not) is the second most likely cause.

Any calculation of the annual cost of cyber attacks is very suspect

- (Probability of an attack) X (Probability of penetration) X (Probable damage) X (Probable Incidents per year). None of these can be reliably estimated !
- Probabilities are not linear relationships that can be multiplied together. They are statistical calculations ! Few people realize this.

5

How is investment in cybersecurity justified?

An ACS/OT Cyber Attack is the least likely cause of a Cybersecurity Incident (see Slide 4)
Product failures (computer or network hardware, software, or field sensor) are the most likely cause.
An action by an employee or contractor (malicious or not) is the second most likely cause.

Any calculation of the annual cost of cyber attacks is very suspect
Probability of an attack X Probability of penetration X Probable damage X Probable Incidents per year. None of these can be reliably estimated !
Probabilities are not linear relationships that can be multiplied together. They are statistical calculations ! Few people realize this.

How is Cybersecurity Investment Justified? (2 of 2)

Since it is impractical to quantify the risk associated with a successful cyber attack. Don't even try.

- Base the payback for increased security monitoring on the most probable cause of an Incident (a device or system failure).
- These failures also have the best data on MTBF, MTTR, and Cost of production loss.

Although it has the lowest probability of occurring, a cyber attack could prove to be the most expensive.

- It is therefore worthwhile to consider measures to minimize the probability and cost of a cyber attack

To do this, identify and minimize the Factors that may Drive Cyber Incidents in your facility.

6

How may an investment in improving cybersecurity be justified?

Since it is impractical to quantify the risk associated with a successful cyber attack. Don't even try.

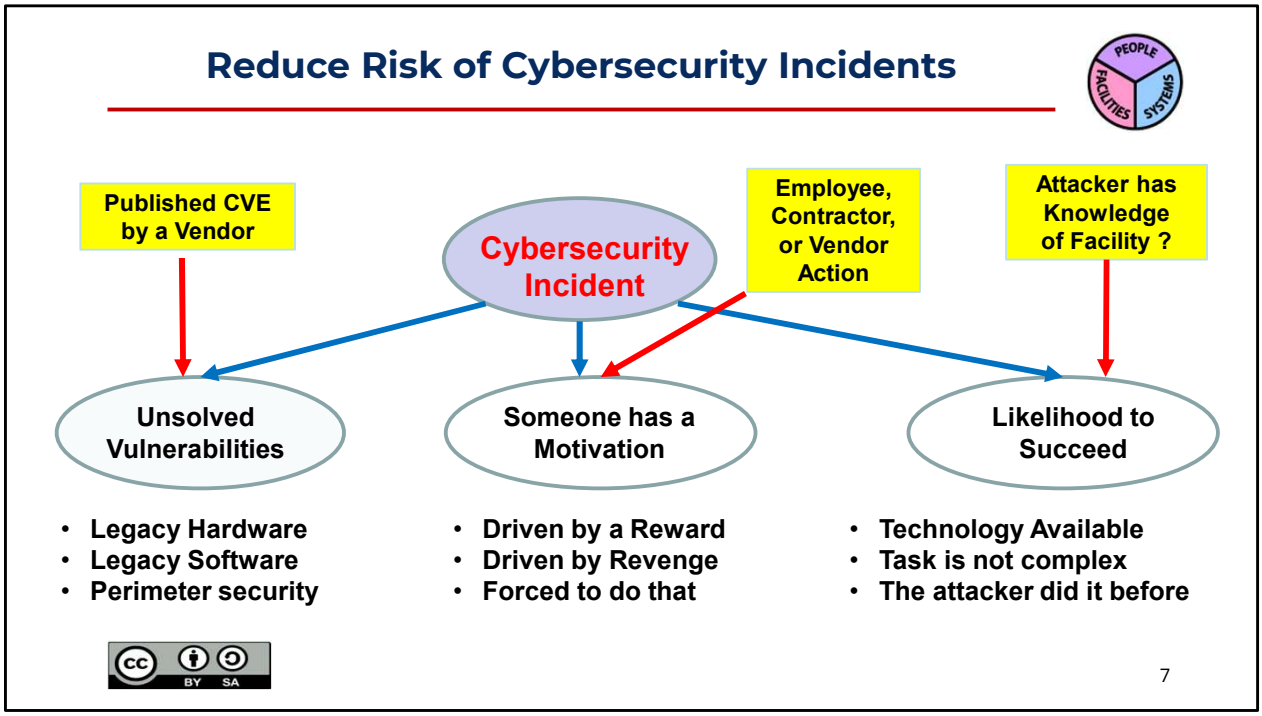
Base the payback for increased security monitoring on the most probable cause of an Incident (a device or system failure).

These failures also have the best data on MTBF, MTTR, and Cost of production loss.

Although it has the lowest probability of occurring, a cyber attack could prove to be the most expensive.

It is therefore worthwhile to consider measures to minimize the probability and cost of a cyber attack

To do this, identify and minimize the Factors that may Drive Cyber Incidents in your facility.

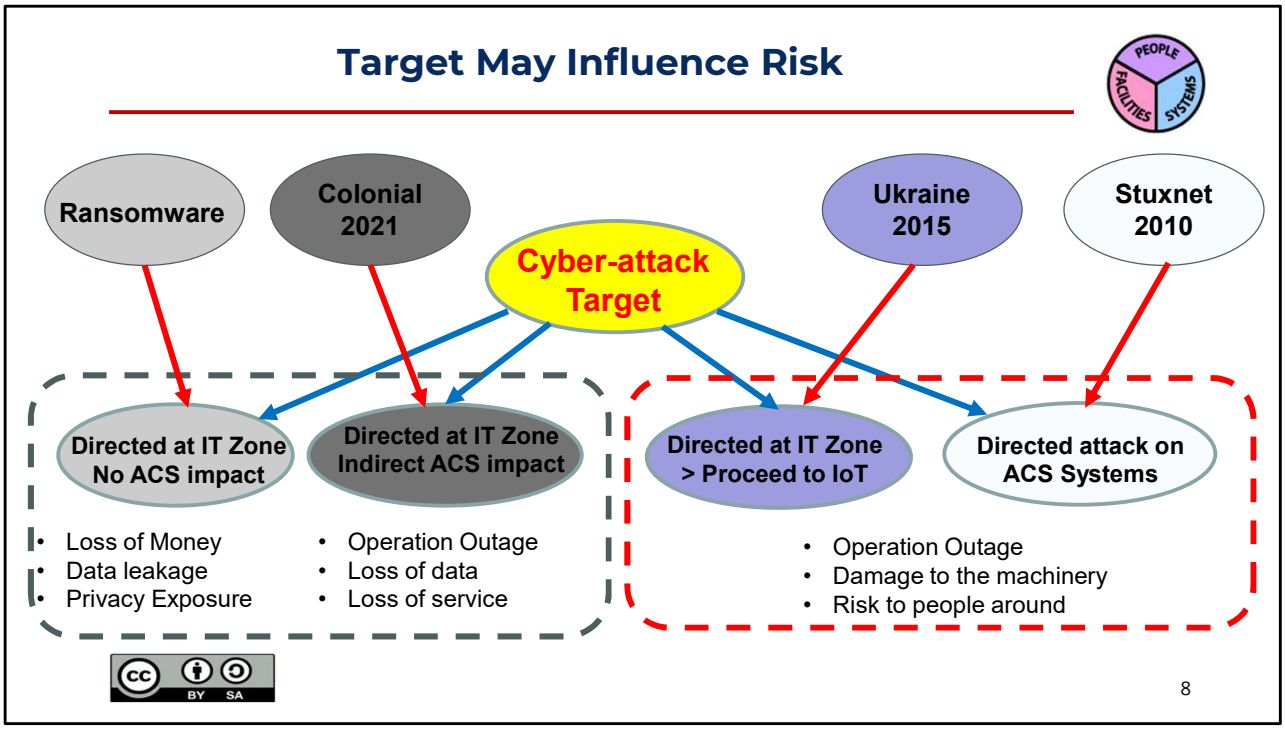


It is advisable to reduce factors that may drive cybersecurity incidents. For example:

- Ensure Common Vulnerabilities and Exposures (CVEs) for Legacy Hardware and Software are monitored and addressed as quickly as feasible. These may come from US CISA bulletins or directly from vendors.
- Ensure that Updates are delivered securely and updated promptly (see MLM-026-A and B: Patch Management)
- Verify perimeter security to ensure that physical access to industrial equipment and networks is not possible.

- Ensure that remote access is strictly controlled and limited to certified personnel. (see MLM-018 A to F - Minimum and Zero Trust)
- Manage password and physical access to currently authorized staff and immediately remove suspect or vulnerable personnel.
- Carefully Monitor for “cyber probes” and “sandbox” to limit their ability to gather information

- Maintain historical register of employees and vendor staff who have been given sensitive information.



The target of a Cybersecurity Attack may influence the risk to ACS or OT systems.

- Ransomware is rarely targeted at ACS systems as IT systems are more likely to involve sensitive information worth a ransom. In a few cases where ACS information was encrypted, victims just reloaded software and restarted plant control systems.

- Indirect ACS impact may occur if IT and ACS systems are not securely separated. The Colonial Pipeline incident would not have resulted in an Operation Outage if separation had been properly done and regularly tested.

- In some cases, ACS, OT and IoT penetration has been deliberately done through internet-connected IT systems. Since this requires penetration of several PERA Levels, a “defense in depth” strategy may not be effective.

- Directed attacks on ACS require sophisticated attackers who will be difficult to defeat with only “defense in depth”. Continuous monitoring for unusual activity, management of “Trust”, training and certification should be considered where risk is considered high (such as protecting critical infrastructure).

When a Cyber Attack is Detected

- First, identify what has been compromised and isolate it.
- Since IT systems are much more likely to be compromised than ACS systems, isolation of ACS and IT systems is the first and most crucial step.
- Isolation of ACS from IT MUST be assured and regularly tested.
- After ACS/IT isolation, the next most effective strategy is “defense in depth”
- Isolate production units (and their obsolete and vulnerable control systems and networks).
- Isolate supervisory systems and interfaces at Level 3 with “bullet-proof” interfaces
- “Zones and Conduits” may help segregate new facilities (when certified products are available); however, in the meantime, they are intellectually interesting, but of little practical use.

9

When a cyber-attack is detected:

- First, identify what has been compromised and isolate it.
- Since IT systems are much more likely to be compromised than ACS systems, isolation of ACS and IT systems is the first and most crucial step.
- Isolation of ACS from IT MUST be assured and regularly tested. Billions of dollars would have been saved in recent attacks, such as the Colonial Pipeline attack, by this simple step.
- After ACS/IT isolation, the next most effective strategy is “defense in depth” through control system and network segregation.
- Isolate production units (and their obsolete and vulnerable control systems and networks).
- Isolate supervisory systems and interfaces at Level 3 with “bullet-proof” interfaces upwards and downwards.

- “Zones and Conduits” may be help segregate new facilities (when certified products are eventually available); however, in the meantime, they are intellectually interesting, but of little practical use.

Key Messages

Base the justification of Cybersecurity on faster detection of all Incidents

- Risks and probabilities of cybersecurity incidents are not quantifiable, but the benefits of faster detection of maintenance and operation failures are.
- Better Cybersecurity Incident monitoring will reduce the cost of cost of device and system failures, lost production, employee errors, and cybersecurity attacks. This alone will usually justify the cost of improved cybersecurity.

How may we protect Automation and OT systems?

- Network and system segmentation and defense-in-depth.
- Vulnerability assessment and mitigation of all security risks, including "Physical Perimeter" security risks.
- Certify training and verify people including skills and Trust Level.

10

Key messages of this MLM include:

Base the justification of cybersecurity on faster detection of all incidents

Risks and probabilities of cybersecurity incidents are not quantifiable, but the benefits of faster detection of maintenance and operation failures are. Better Cybersecurity Incident monitoring will reduce the cost of cost of device and system failures, lost production, employee errors, and cybersecurity attacks. This alone will usually justify the cost of improved cybersecurity.

How may we protect Automation and OT systems?

Network and system segmentation and defense-in-depth.
Vulnerability assessment and mitigation of all security risks, including "Physical Perimeter" security risks.
Certify training and verify people including skills and Trust Level.

Further Information

- **Related MLMs on Patch Management, Trust & Risk Mitigation**
  - MLM-026-A: Patch Management for Owner Operators
  - MLM-026-B : Patch Management for Vendors
  - MLM-018 A : Concepts of Trust in Process Plants
  - MLM-018-B and MLM-018-C : Minimum Trust in Process Plant ACS
  - MLM-018-D and MLM-018-E : Limited Trust in Process Plant IT Systems
  - MLM-018-F : Minimum Trust in Process Plant OT Systems
  - MLM-016-A Typical Cybersecurity Attacks
  - MLM-016-B Cybersecurity Risk Definitions and Concepts
  - MLM-016-F Level 0 and 1 Cyber Vulnerabilities
  - MLM-019-A Cybersecurity Audits and KPIs

Please click here to provide feedback on this MLM.

Here are some links to related MLMs

Please use this link to leave us your comments. These will be shared with the author to help improve future versions.

Author

Daniel Ehrenreich

Daniel has over 33 years of experience with control of industrial operations and integration of cyber security solutions.

He is a control engineering consultant, workshop lecturer, and an expert in cyber secured operation for IACS.

Daniel is contributing his knowledge and expertise to multiple ISA 62443 workgroups.

Since 2016, acting as the Chairman of the annual ACS-Cybersec Conference taking place in Israel