Why Cybersecurity Matters in Industrial Context?

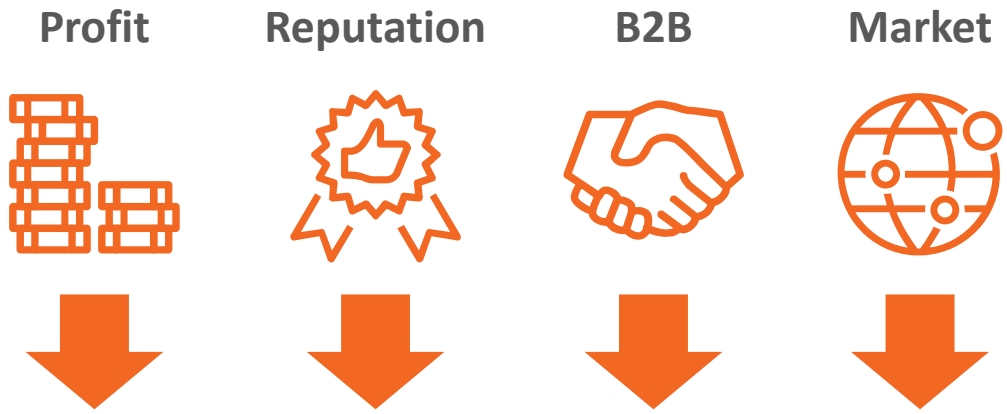

ANONYMOUS
SPY
LEAK

WHY INDUSTRIAL CYBERSECURITY?

SMART MANUFACTURING MAY NOT DELIVER ON ITS PROMISE IF IT IS LEFT UNSECURED

Industrial risks in manufacturing plants:

- Loss of life or injuries
- Production shutdown, supply chain disruption
- Product quality damage
- Manufacturing line damage
- Regulatory non-compliance
- Intellectual Property loss (e.g. recipes, optimization algorithms)



MAERSK

"Moller-Maersk puts cost of cyber attack at **up to $300m**."

Mondelēz International

"Cyber attack will **cut 3 percent** from revenue growth."

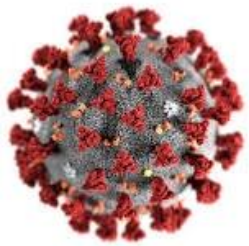
SAINT-GOBAIN

"The cyber-attack is estimated to have had an impact of **€220 million** on first-half sales."

MERCK

"Cyber attack halted production**, will hurt profits**."

COVID-19 INDUSTRIAL CYBER THREATS



The worldwide COVID-19 outbreak, which the World Health Organization (WHO) declared a pandemic on March 11, 2020, continues to impact the Industrial sector, raising an increased number of cybersecurity challenges :malware spread, disruption of operations, phishing campaigns, discontinuity of information security operations. Companies in all industries should plan for these challenges to persist for months and to have long-term effects.

A new campaign deploying the remote access **Trojan PoetRAT** targeted the government and **utilities sectors** in Azerbaijan, specifically targeting energy companies' supervisory control and data acquisition **(SCADA)** systems;

POND LOACH (a.k.a. OceanLotus and APT 32), attacked the Chinese health department and agencies of Wuhan municipality using COVID-19-themed phishing lures.
The POND LOACH group has been targeting Chinese **energy-related industries**, maritime agencies, **marine construction**, shipping companies and research institutes.

Potential Iranian Threat: A February 2020 FBI alert warned of a campaign using the Kwampirs remote access Trojan. Actors used Kwampirs against healthcare organizations and health-sector **industrial control systems (ICS)** as well as supply chains affecting numerous sectors.

We see an increased trend for **industrial espionage** , as nations and companies plan to improve resilience by reshaping supply chains

WHY NOW?

CHANGING
LANDSCAPE

Being connected is the NEW NORMAL but can increase cyberattack risk

Greater connectivity provides an opportunity for industrial equipment manufacturers to:

- **Improve service levels**
- **Be more responsive to dealers and customers**
- **Make better use of data**

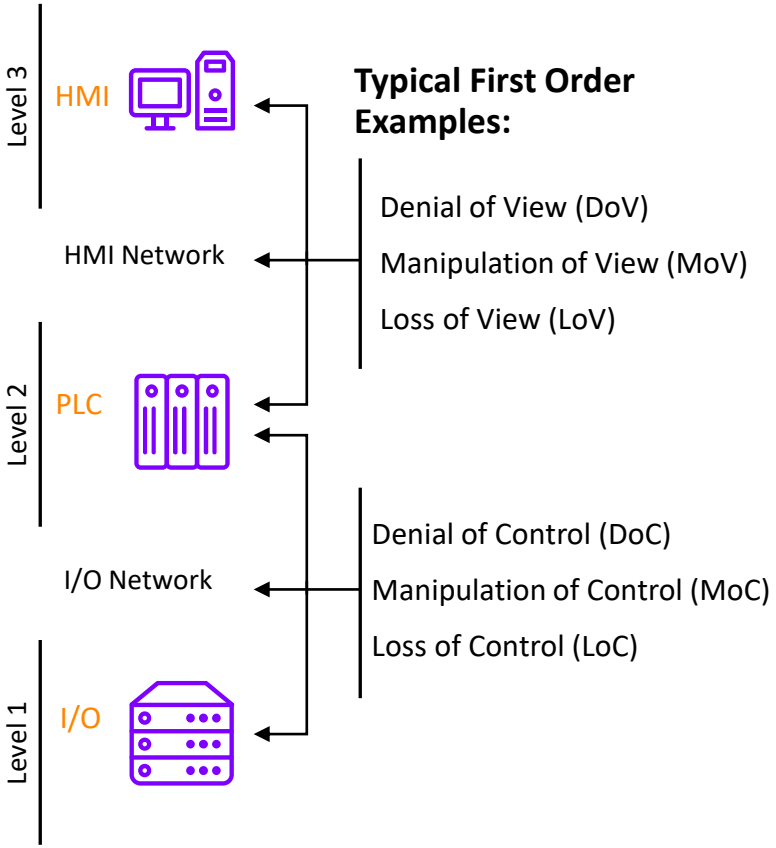
74%

of industrial equipment executives said that "cyberattacks are a bit of a black box, we do not quite know how or when they will affect our organization."

CYBER ATTACKER GOALS

WHEN ATTACKING INDUSTRIAL CONTROL SYSTEMS, DEVASTATING RESULTS CAN BE ACHIEVED

Attack Outcomes can be architecture dependent. While not always the case, certain outcomes are more likely in various points of the architecture.



First order events and cascade to second order events. Example: DoC at L1 can result in LoV at L3

Denial of View (DoV)

When the cyber attackers interfere with the information streams so that it is no longer possible to see the operational state of equipment being monitored – this could be through denial of service attacks, or other mechanisms in which telemetry cannot be seem by the operators.

Manipulation of View (MoV)

This is when the cyber attackers change the information streams that represent the operational state of the production process so that the operators are mislead into believing that equipment is operating normally when it is being misused by the attacker, or that the equipment is malfunctioning so that the operators take inappropriate recovery actions, which could result in the operators issuing incorrect or dangerous commands.

Loss of View (LoV)

A situation where the operator is receiving no operational updates from the remote processes and equipment being controlled. Attacks on the operating system running on the DCU in the control rooms causing the HMI to fail resulting in system components going into a fail safe state

Denial of Control (DoC)

A temporary inability to control ICS hardware or operational processes (e.g. a DoC attack on PLCs could be implemented by intercepting control messages and replaying expected responses, while at the same time causing the PLC to execute damaging operations)

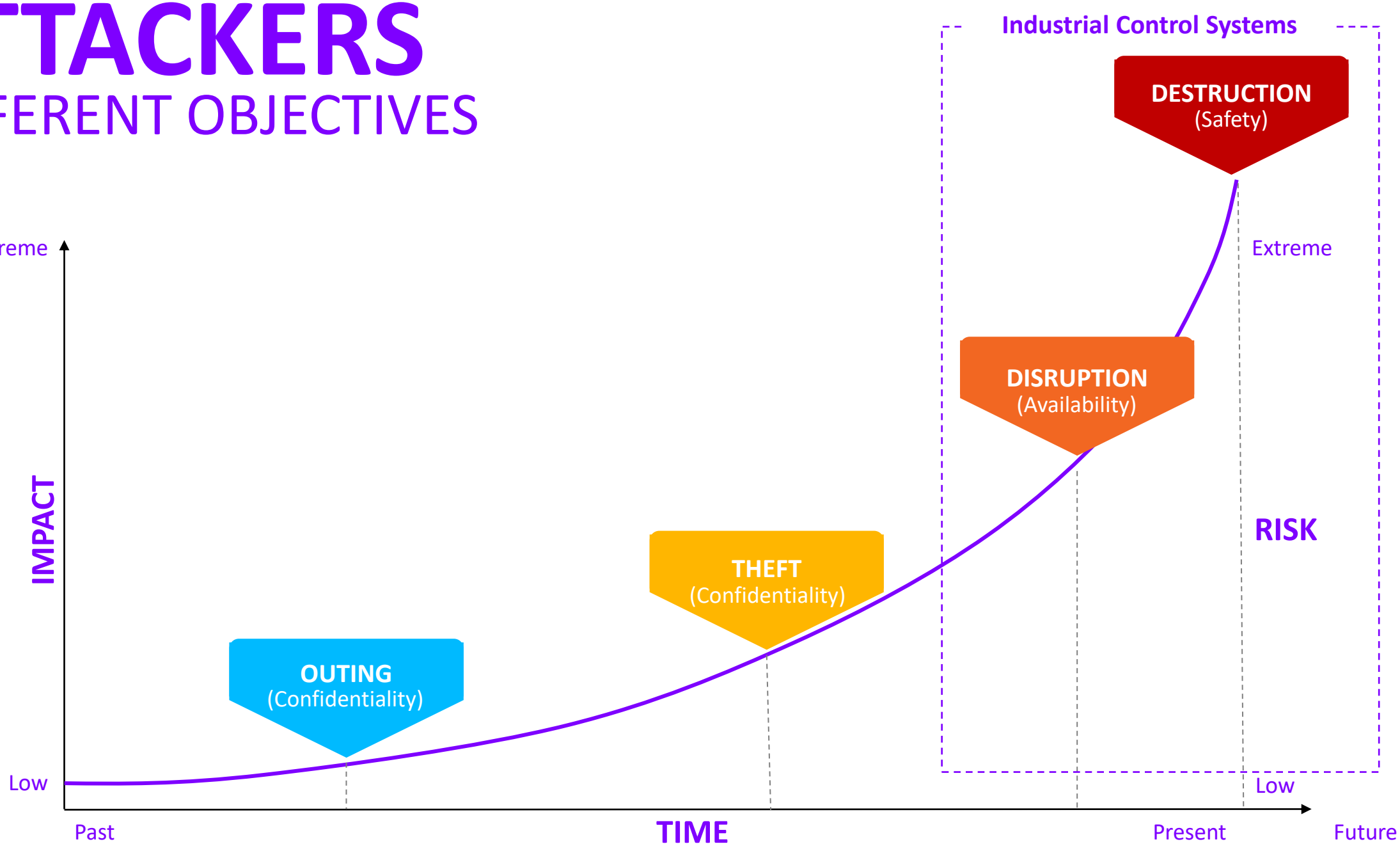
Manipulation of Control (MoC)

When control logic is interfered with to override or ignore legitimate operator commands. MoC could also be caused by MITM attacks and used by the attacker to interfere with or control operational processes or equipment

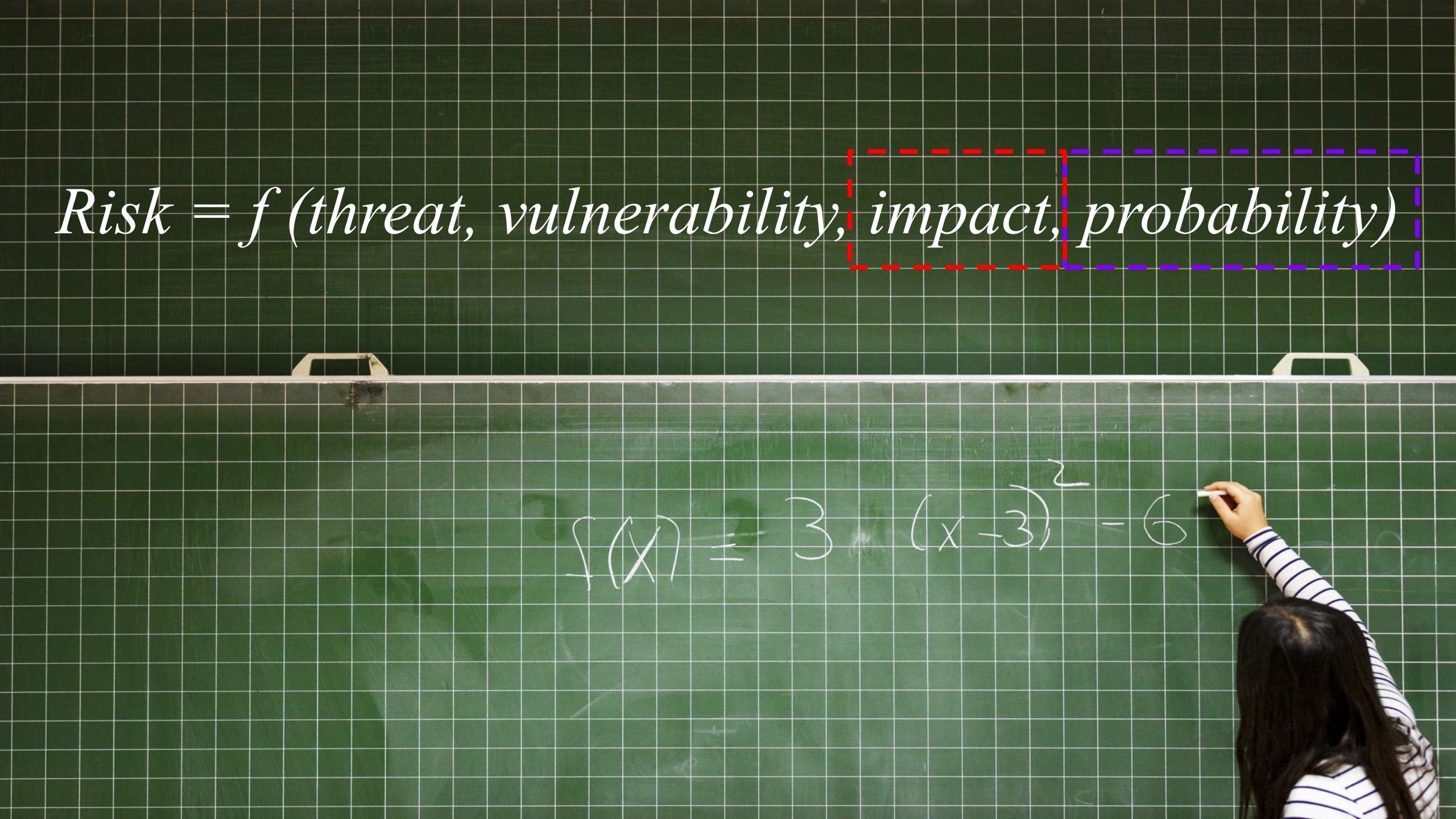
Loss of Control (LoC)

A sustained inability to control or correct operational behavior, potentially resulting in loss of service caused by equipment failure, or systems entering fail safe states. LoC attacks can occur in clear sight of operators with the HMI indicating that an attack is taking place, but with the operators unable to take preventative action. LOC may persist after an attack has completed, with requiring technicians to physically reset/replace the equipment

ATTACKERS
DIFFERENT OBJECTIVES



INFORMATION THEFT vs
INFRASTRUCTURE DESTRUCTION


Risk = f (threat, vulnerability, impact, probability)
f(x) = 3 (x-3)² - 6


PROBABILITY IS IRRELEVANT

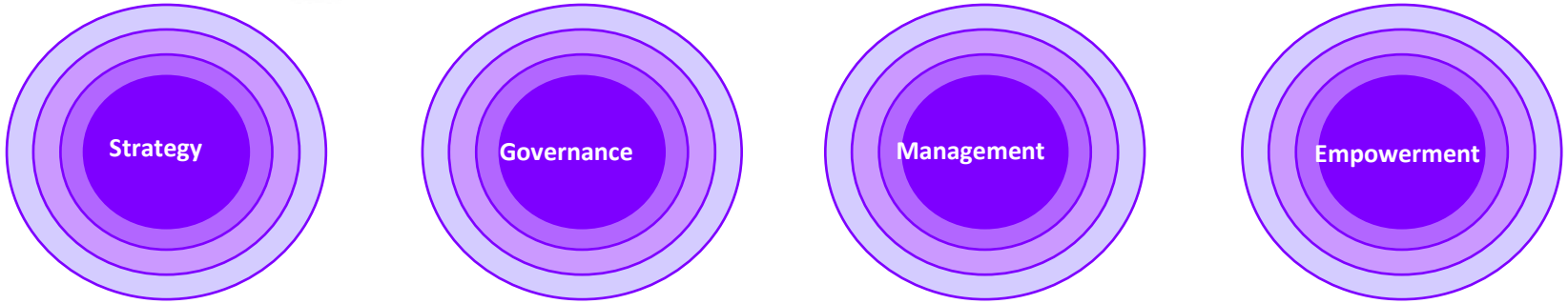
Industrial
Cybersecurity

NO WAY
TO REACH IT ALONE

Build your own

INDUSTRIAL CYBERSECURITY FRAMEWORK

by adapting and adopting applicable standards and regulations



INCREASE VISIBILITY

INTERNAL

(full infrastructure monitoring)

EXTERNAL

(threat intelligence)

Change actions to achieve cyber resilience at Industrial level

01

Secure core assets

Focus on the fundamentals. Regularly harden and protect core assets and pressure-test resilience.

02

Establish a security-by-design culture

Keep pace with the changing nature of connected environments. Develop a more proactive security posture that is fully operational from the outset.

03

Increase Visibility and Collaboration

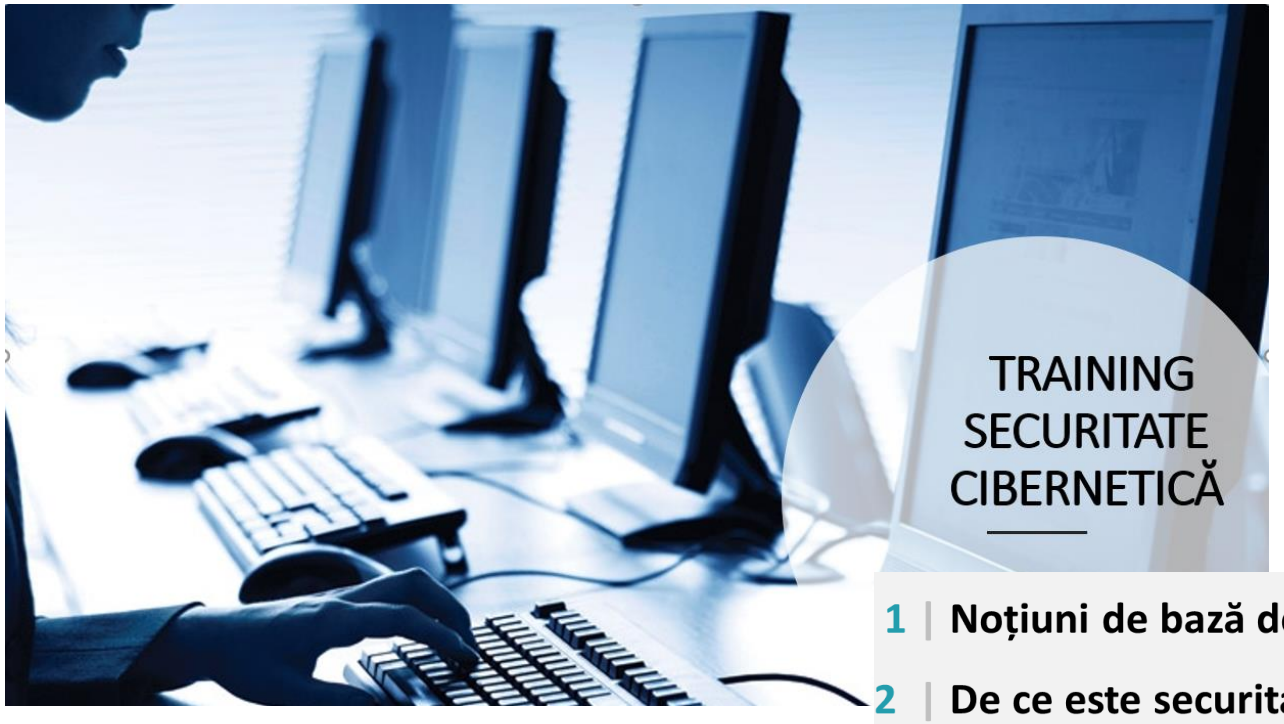
First step for being ready to protect your core assets is to have visibility on what's happening inside and outside your organization perimeter.

04

Prepare Tomorrow's Cybersecurity Talents

Start preparing and investing into Cybersecurity Talents. Find ways to attract and offer the right environment and culture to allow them to "flourish".

Training : Cybersecurity in context Industrial



1 | Noțiuni de bază despre securitatea informației

2 | De ce este securitatea cibernetică importantă

3 | Confidențialitatea datelor

4 | Social Engineering

5 | Convergența IT- OT

6 | Cum poate evoluția IIOT afecta securitatea ICS

7 | Securitatea si managementul furnizorilor

THANK YOU

Dragos Dabija
Security Director @ Digital14