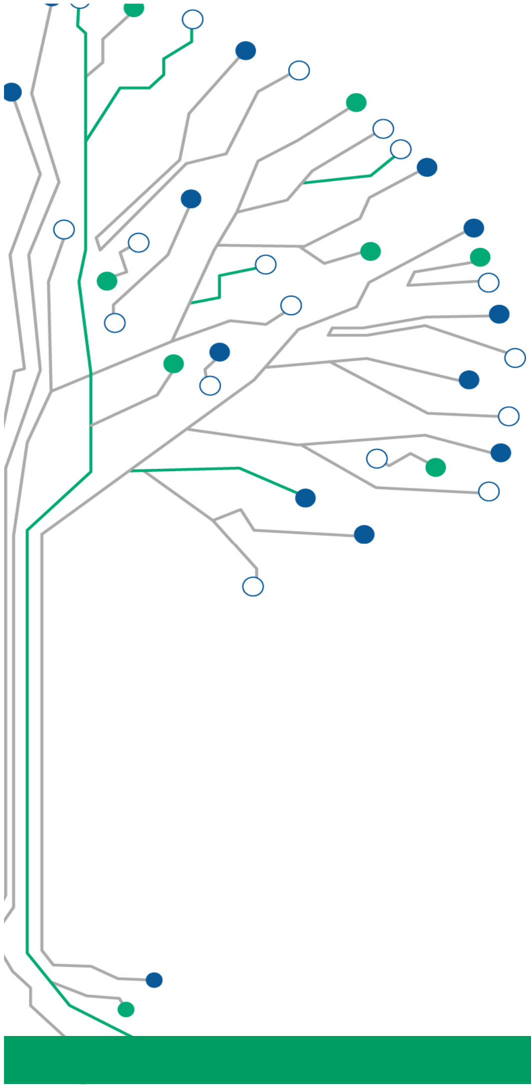


ANIE AUTOMAZIONE

ANIE FEDERAZIONE CONFINDUSTRIA

Cyber Security

V1_pdf version

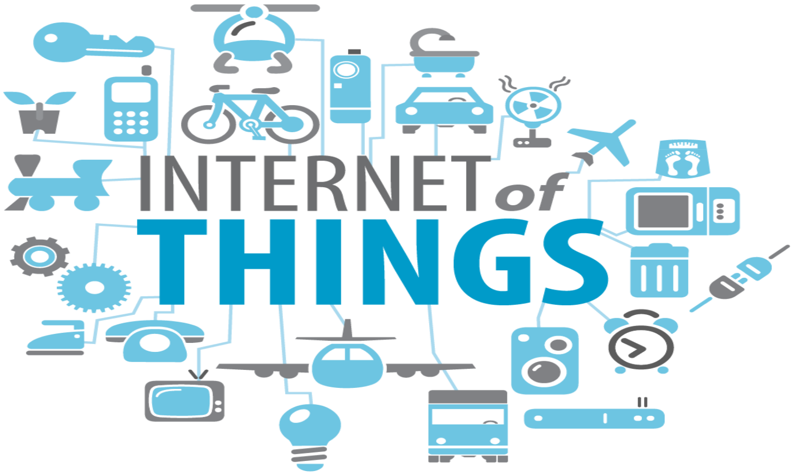
Massimiliano Spano

Domain Expert Mechatronics&Drives

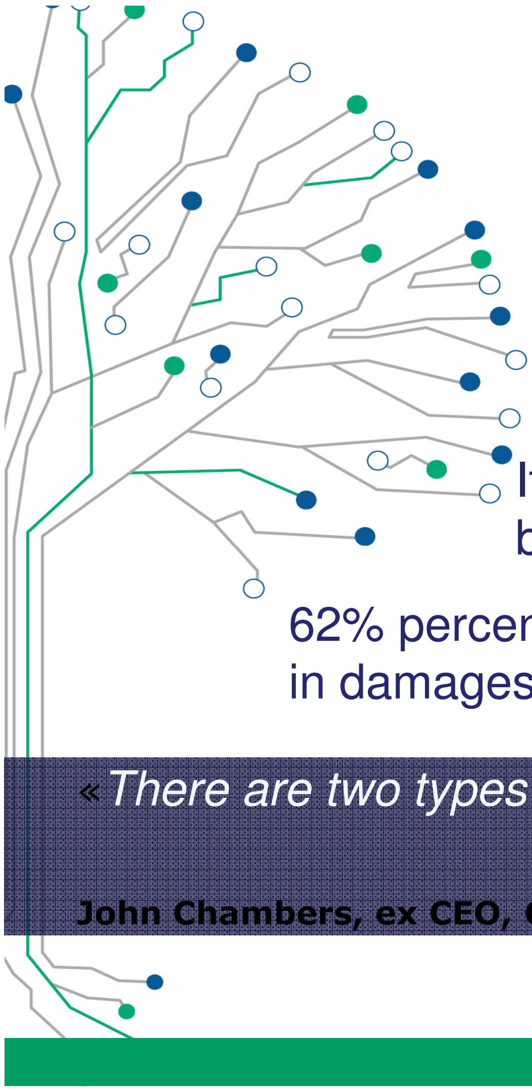
Rockwell Automation

YEAR	MARKET SIZE IN BILLION USD
2017	109
2018	164
2019	212
2020	248
2021	418
2022	594
2023	800
2024	1079
2025	1612

YEAR	MALWARE IN MILLIONS
2013	165,81
2014	308,96
2015	452,93
2016	580,41
2017	702,06
2018	812,67



The transition from closed networks to the Internet is accelerating, raising a growing security alert.



92% of the italians company have to admit they received a cyber attack during the last year.

It is estimated that Italy suffered damages in 2017 of 10 billion euros as a result of cybercriminal activities

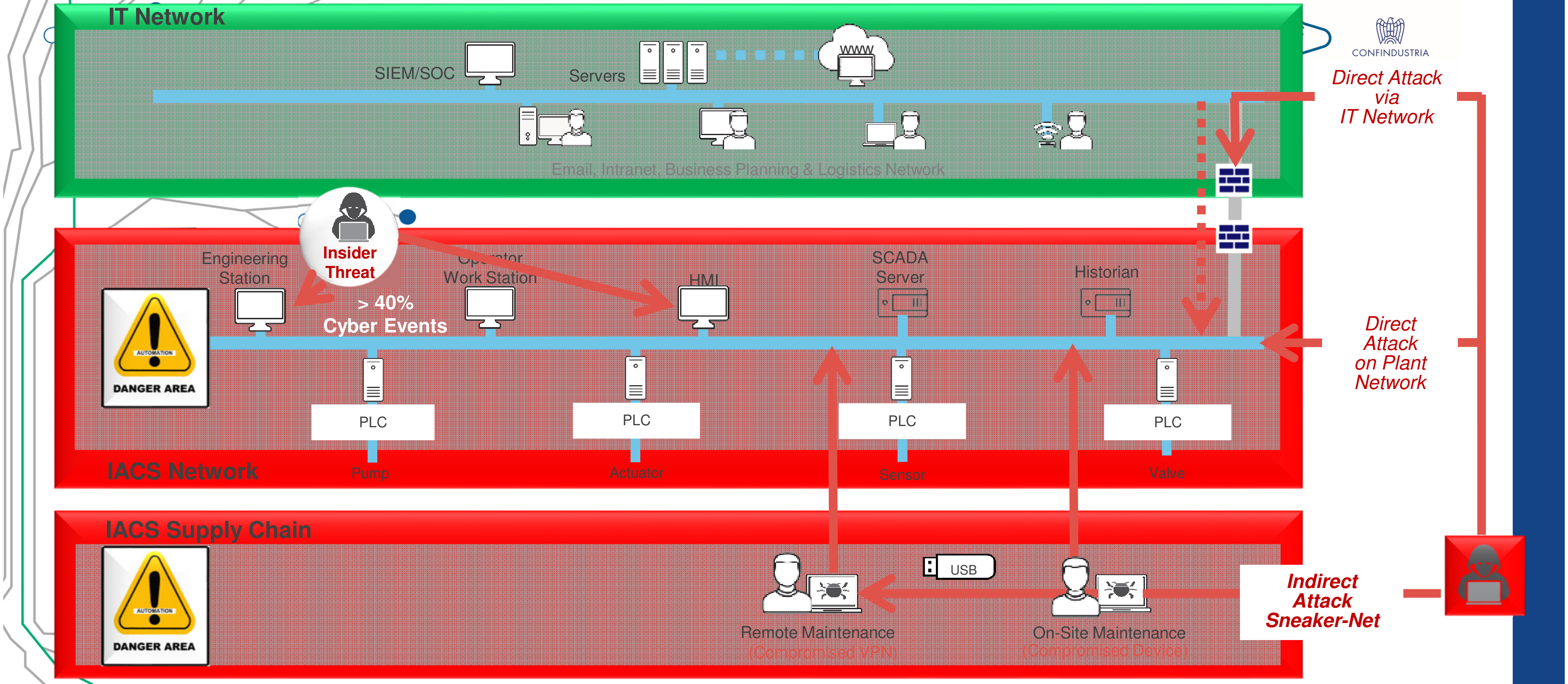
62% percent of the attacks in Italy resulted in damages of more than 80,000 euros.

> «*There are two types of companies: those who have been hacked,*
> *and those who don’t yet know they have been hacked.*»
>
> **John Chambers, ex CEO, Cisco**

IACS Threat Vectors

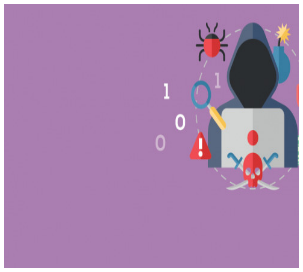
ANIE AUTOMAZIONE

CONFINDUSTRIA



What is Cybersecurity?

Does everybody have a Personal Computer Right?
Especially in the Companies Right?

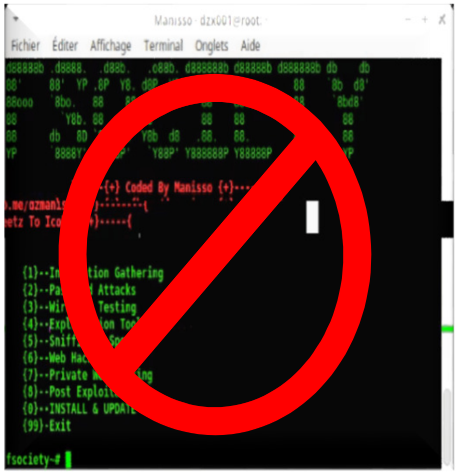


Do you wanna see how easily gain access to sensistive information?

Needs to interact with the customer by sharing commercial documents

What's the normal employees answer **today**?

No, I can't



```
d88888b .d8888.  .d88b.   .o88b. d888888b d88888b d888888b db    db
88'     88'  YP .8P  Y8. d8P                         88     `8b  d8'
88ooo   `8bo.   88    88                             88      `8bd8'
88        `Y8b. 88                   88   88                   88
88      db   8D `           Y8b  d8  .88.  88.                 88
YP      `8888Y'    P'      `Y88P' Y888888P Y88888P             YP

        -{+} Coded By Manisso {+}---
.me/ozmanis      }--------{
etz To Ico      +}-----{

  {1}--In      tion Gathering
  {2}--Pa     d Attacks
  {3}--Wir     Testing
  {4}--Expl    ion Too
  {5}--Sniff   Sp
  {6}--Web Hac
  {7}--Private        ing
  {8}--Post Exploit
  {0}--INSTALL & UPDATE
  {99}-Exit

fsociety~#
```

A big number of companies start to disable the USB ports on their employees PC

Many peoples and Companies have known this for years...
You never do this...Than...The Issue is Fixed?

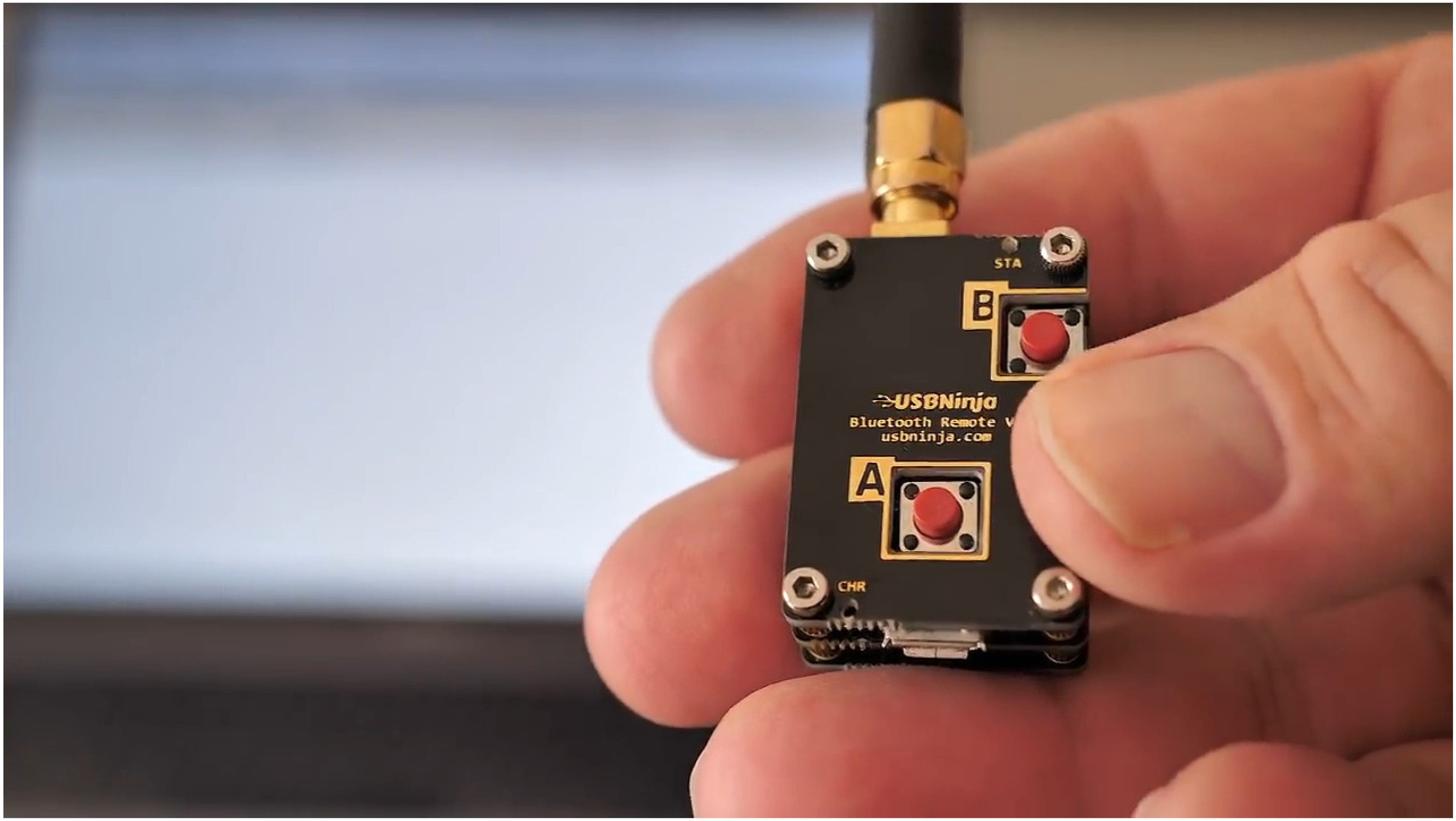
Absolutly not... You have to think about how the Hackers «Evolve» in their trade craft...
Here a simple example...

Employ or Manager needs a new smartphone

The Hacker known this needed by a dedicated work he’s doing from days

&...He prepare a special package, for them.. with the new Phone...

Plugged in for a normal smartphone recharge...

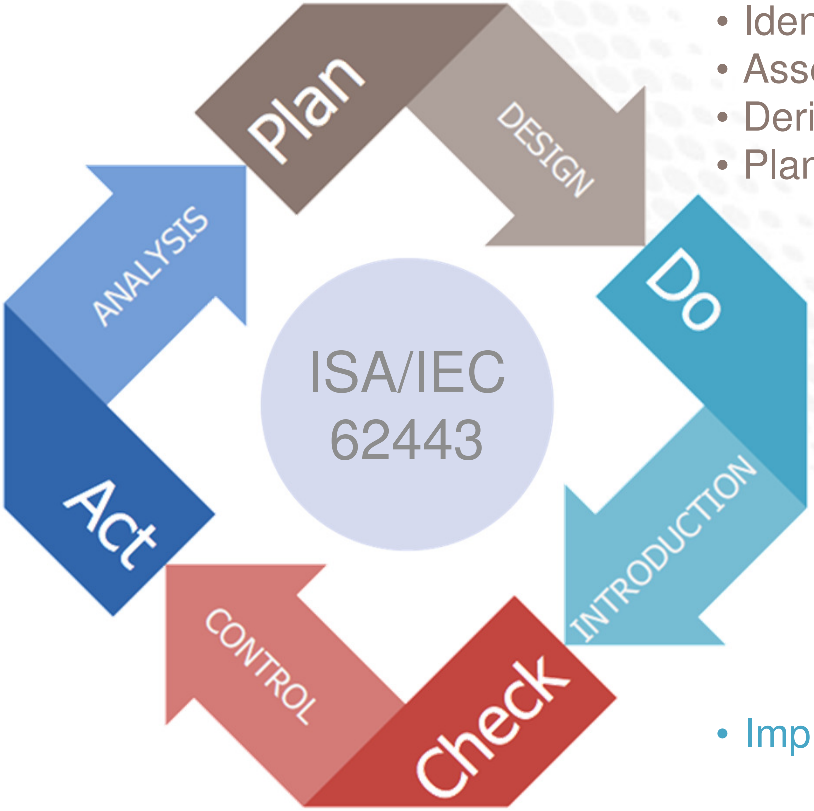

STA
B
USBNinja
Bluetooth Remote V
usbninja.com
A
CHR

Methodology

Plan-Do-Check-Act (PDCA)

- Continuous improvement

- Identify risk
- Assessing risks
- Derive measurements
- Plan your deployment



- Monitoring and testing
- Audit

- Implementing measures

DESIGN - IEC62443 3-3 Where Are You Today?

What is your Target Security Level?

Protect Against **Intentional Unauthorized Access Using Sophisticated Means with Extend Resources,** IACS specific Skills & High Motivation – **Nation-state**

Security Level 4

Protect Against Intentional Unauthorized Access Using **Sophisticated Skills** with Moderate Resources, IACS specific skills & Moderate Motivation – **Cyber Terrorism**

Security Level 3

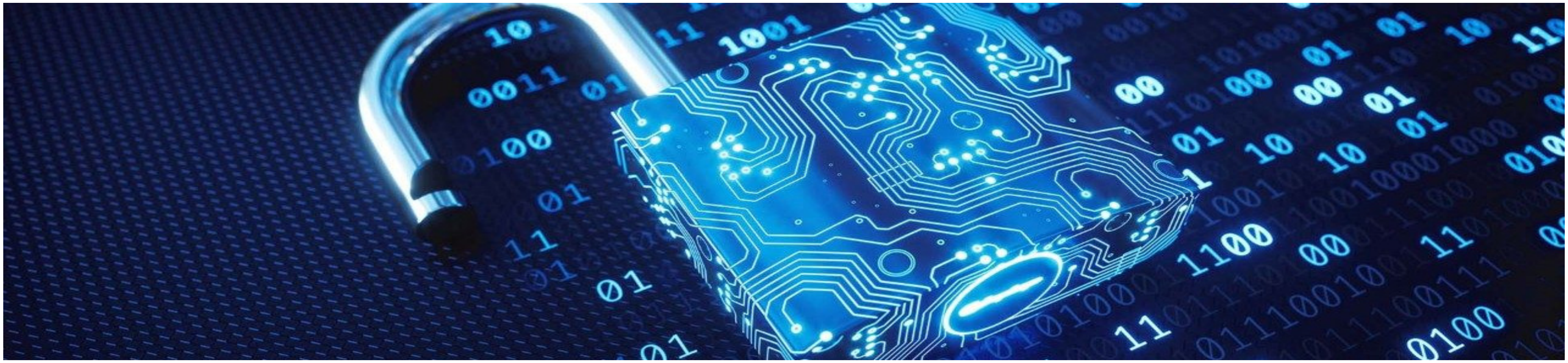
Protect Against Intentional Unauthorized Access Using **Simple Means** with Low Resources, Generic Skills, & Low Motivation – **Cyber Crime, Hackers**

Security Level 2

Protect Against **Casual or Incidental** Unauthorized Access – **Employee Error**

Security Level 1

Cybersecurity standards for IACS



Cybersecurity standards provide:

- Common **language** and **terminology** in the industrial sector
- A standardized **methodology**
- Guidance on how to answer questions like:
  - What is my **current** risk?
  - What would be a **more acceptable** level of risk for my company?
  - How can I get to this **more acceptable** level?

The Cyber Security

THANK YOU

it affects all of US

Rockwell Automation