CYBER RESILIENCE IN AUTOMATION

2023-Sep-11

Adam Griffen

Product Manager, ei^3

OMAC

The Organization for Machine Automation and Control

Introduction

Joined ei^3 in March, 2023: passion for Automation, IIoT, and AI

10 yrs experience in industry:

Operator > Technician > Engineer > Product Manager

8 yrs @Mettler-Toledo, Product Management, various roles relating to software engineering, SAP Variant Configuration Power User, Compliance Leader for Automation & Digital Security

International Application Engineering Camp @B&R Industrial Automation

ei3 METTLER TOLEDO B&R A member of the ABB Group OPC FOUNDATION OMAC The Organization for Machine Automation and Control UTAH VALLEY UVU UNIVERSITY OHIO STATE

OMAC
The Organization for Machine Automation and Control

ei3 At a Glance

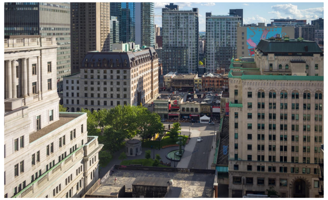
Trusted partner for Industrial IoT and AI for machine builders and manufacturers since 1999

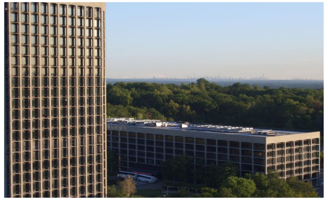
3 Locations, 3 Competencies

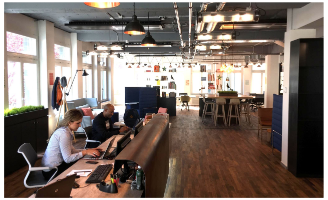
MONTREAL, CANADA
JAVA DEVELOPMENT

PEARL RIVER, NEW YORK
GLOBAL HEADQUARTERS

ZURICH, SWITZERLAND
DATA SCIENCE CENTRE







Sales Agents: BANGALORE, INDIA
TOKYO, JAPAN

Data Centres in: USA, Germany, China

Trusted by leading brands

American Packaging Corporation
BOBST
BROWN MACHINE GROUP
coperion
DÜRR
ECOLEAF
kp klöckner pentaplast
INYX
MILACRON® M·POWERED
PROCENTEC® Member of the HMS group.
STG
Shibaura Machine
SONOCO®
WestRock
Graphic Packaging INTERNATIONAL
CMM™
BMG
ADR Advanced Digital Readiness
ORBIS® Powered by Menasha Corporation
GESA

OMAC
The Organization for Machine Automation and Control

ei3 At a Glance

FOR MACHINE BUILDERS:

- Proven, white-labeled solution to get started on your digital transformation journey immediately
- Reduce warranty costs and technican's travel time with secure remote access
- Drive new after-sales services to deliver fast support to customers and improve brand loyalty

FOR MACHINE OWNERS:

- Achieve maximum ROI from your equipment and save costs by measuring, monitoring and controlling your key performance indicators with our powerful suite of IoT Applications
- Reduce downtime, improve quality, increase yield and lower energy consumption

150,000
machines & devices being monitored

10,000
connected facilities

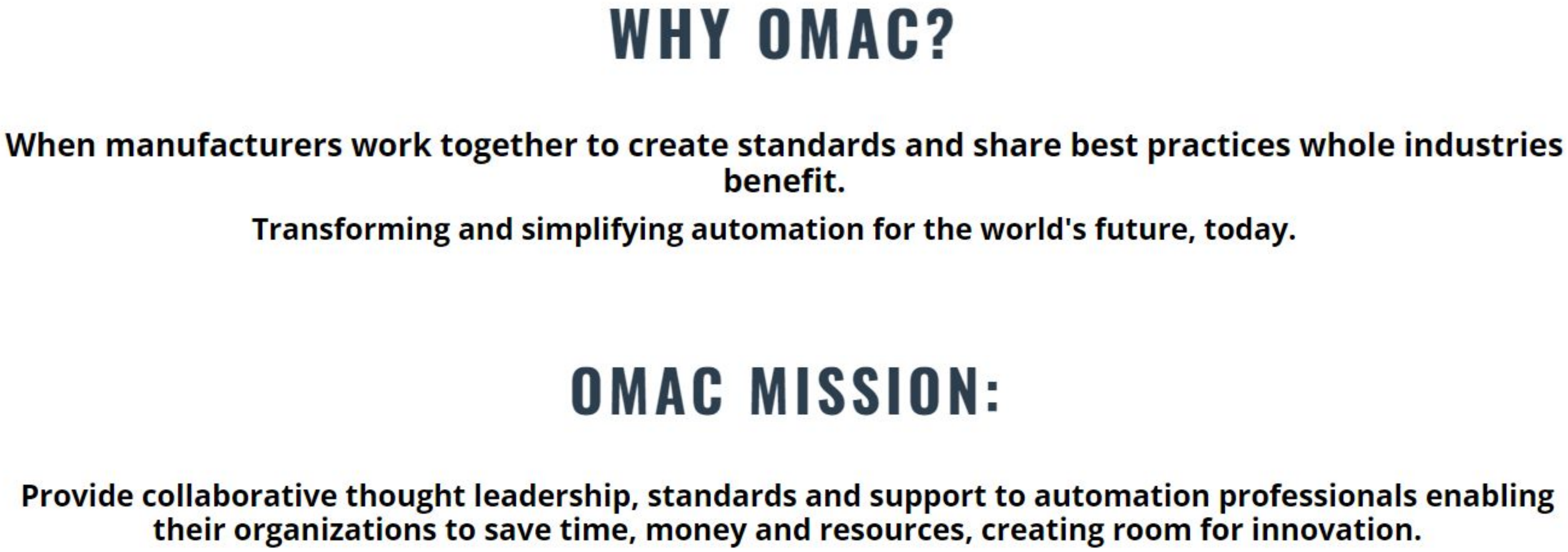
300 million
data points collected everyday

Visit https://ei3.com/

OMAC

The Organization for Machine Automation and Control

Org. for Machine Automation & Control



WHY OMAC?

When manufacturers work together to create standards and share best practices whole industries benefit.

Transforming and simplifying automation for the world's future, today.

OMAC MISSION:

Provide collaborative thought leadership, standards and support to automation professionals enabling their organizations to save time, money and resources, creating room for innovation.

Members

- 60+ corporate members and growing
- Since 1994
- End users include Nestle, P&G, Arla Foods, WestRock, etc.
- OEMs include ProMach, Bobst, Milacron, Mettler-Toledo, etc.
- System integrators include: CONTEC, EOSYS, Rovisys, etc.
- Technology providers include: Rockwell, Siemens, Mitsubishi, ei^3, Cisco, etc.
- See full list here

Partner Organizations

PMMI™ The Association for Packaging and Processing Technologies

PMMI OpX™ Leadership Network
Moving Operational Excellence Forward

OPC® FOUNDATION

o3neida

NIST

ARC Advisory Group

ISA™

Georgia Tech

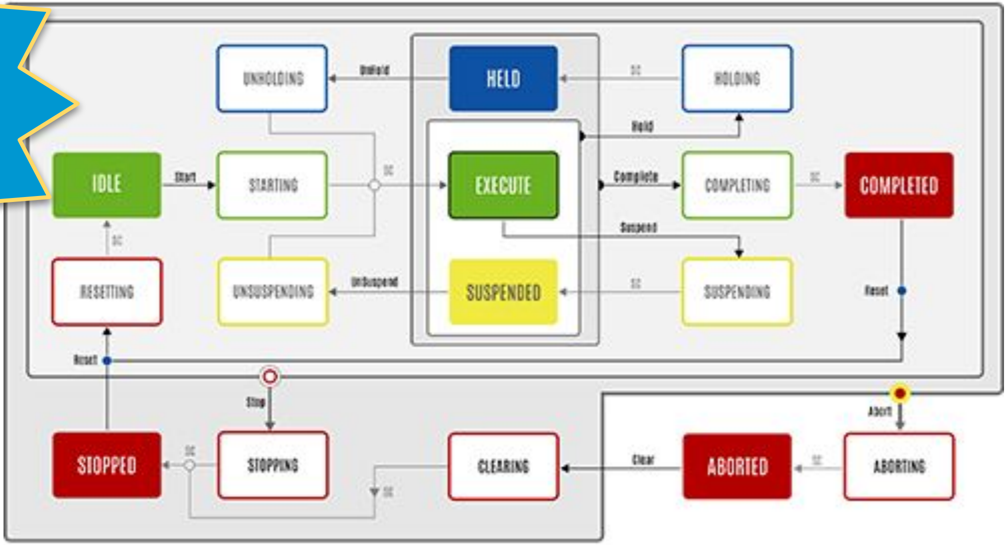
AUTOMATION FEDERATION

csia™ control system integrators association

PLCopen®
for efficiency in automation

PackML

OMAC's Most Widely Adopted Standard



Digital Transformation Workgroup

Shape the Future of Automation with the OMAC Packaging Workgroup (OPW)

Drive Digital Twin Manufacturing with the OMAC Manufacturing Workgroup (OMW)

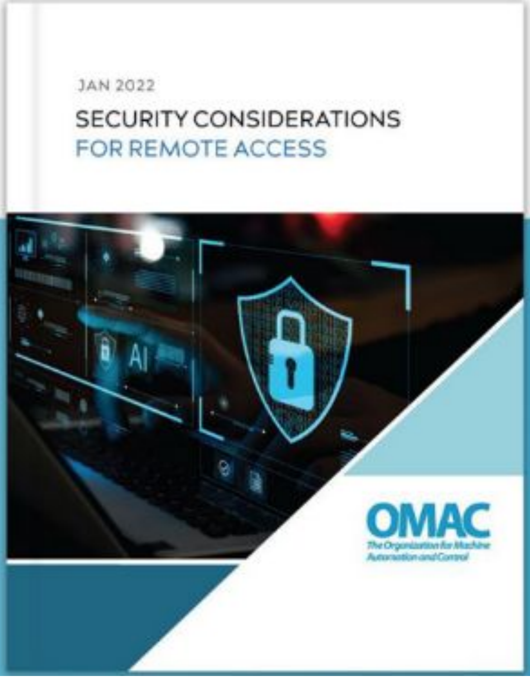
Create Remote Access Best Practices with the OMAC Digital Transformation Workgroup (DTW)

Digital Transformation Workgroup

JAN 2021

Practical Guide for Remote Access to Plant Equipment

OMAC
The Organization for Machine Automation and Control



JAN 2022

SECURITY CONSIDERATIONS
FOR REMOTE ACCESS

OMAC
The Organization for Machine Automation and Control

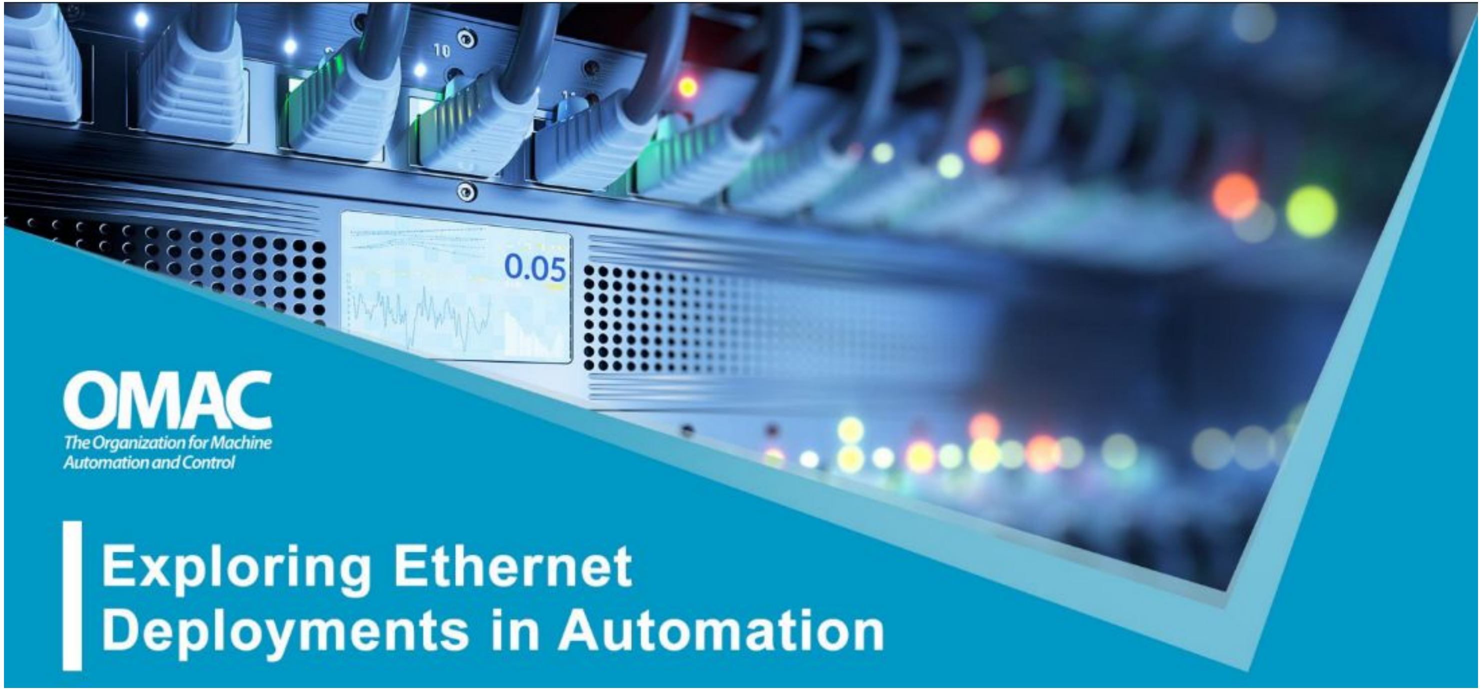
OMAC
The Organization for Machine Automation and Control

FEB 2023

Practical Considerations for
Data Governance

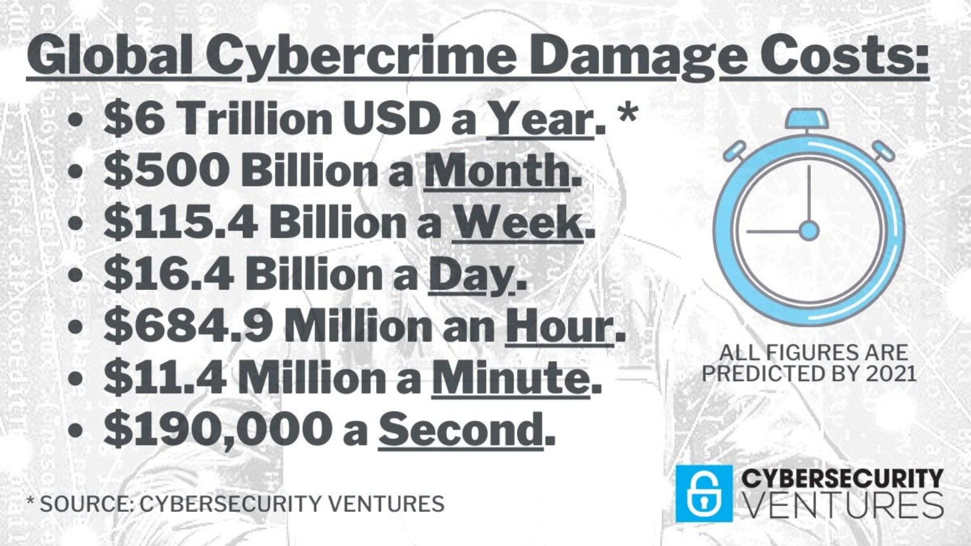
Segmenting,
Sharing
and Securing
Industrial Data

Industrial Ethernet Initiative


0.05
OMAC
The Organization for Machine Automation and Control
Exploring Ethernet Deployments in Automation

OMAC
The Organization for Machine Automation and Control

Cybercrime, Warfare, & Terrorism



Global Cybercrime Damage Costs:

- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

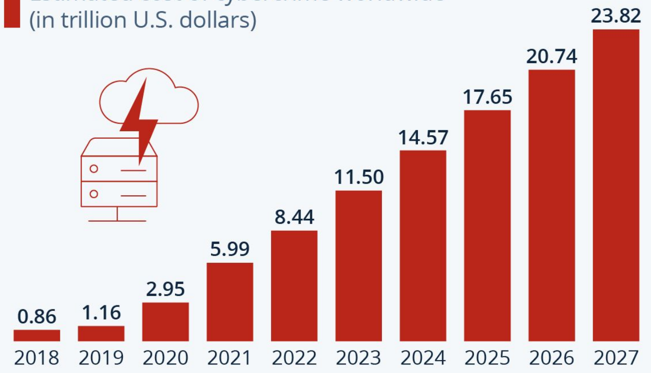
ALL FIGURES ARE PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

statista

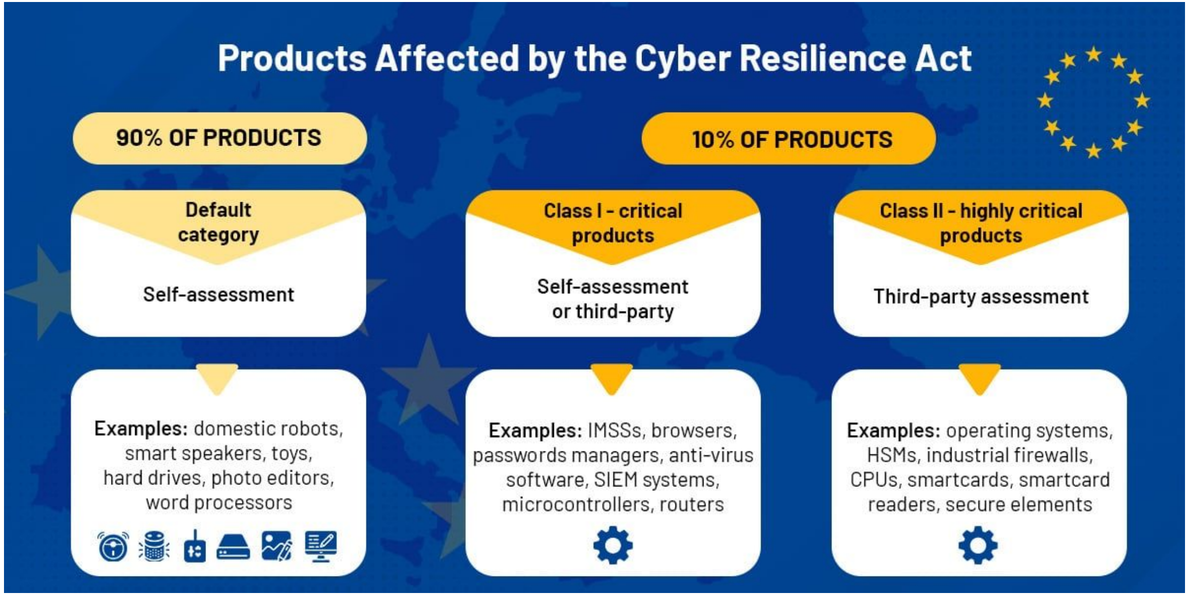
Cyber Resilience Task Force

© European Union

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

- High-level, non-technical 5 page summary of the act for executive leadership
- Understand the scope, impact, and timeline of the new legislation
- Practical first steps to begin journey towards compliance

EU Cyber Resilience Act



Products Affected by the Cyber Resilience Act

90% OF PRODUCTS

Default category

Self-assessment

Examples: domestic robots, smart speakers, toys, hard drives, photo editors, word processors

10% OF PRODUCTS

Class I - critical products

Self-assessment or third-party

Examples: IMSSs, browsers, passwords managers, anti-virus software, SIEM systems, microcontrollers, routers

Class II - highly critical products

Third-party assessment

Examples: operating systems, HSMs, industrial firewalls, CPUs, smartcards, smartcard readers, secure elements

Source: Blaze Cyber Security Penetration Testing Services:
EU CYBER RESILIENCE ACT – WHAT IT MEANS FOR DIGITAL PRODUCTS

Status of the EU's CRA

- September 2022: Commission proposed first draft with two year provision to prepare for enforcement
- July 2023: Council came to agreement on changes to the legislation, updated scope of products to comply among other changes
- Next Steps: Final negotiations between member states and European Parliament followed by establishment of date the act goes into effect

OMAC Summary for Executives

Security properties in digital products

Collaborate with experts

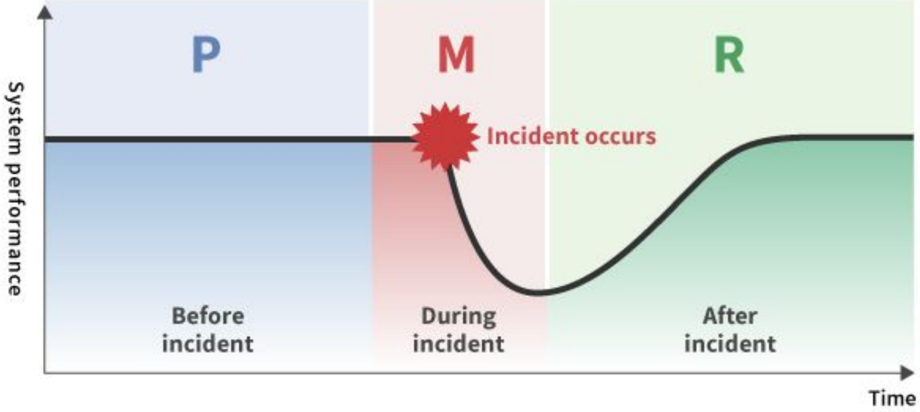
Security vulnerability handling procedures

Comply with EU regulations

3rd party certification for critical products

Apply best practices for industrial cyber security

What is Cyber Resilience?



Prepare
(System operation time)
Maximize system performance (extend P)

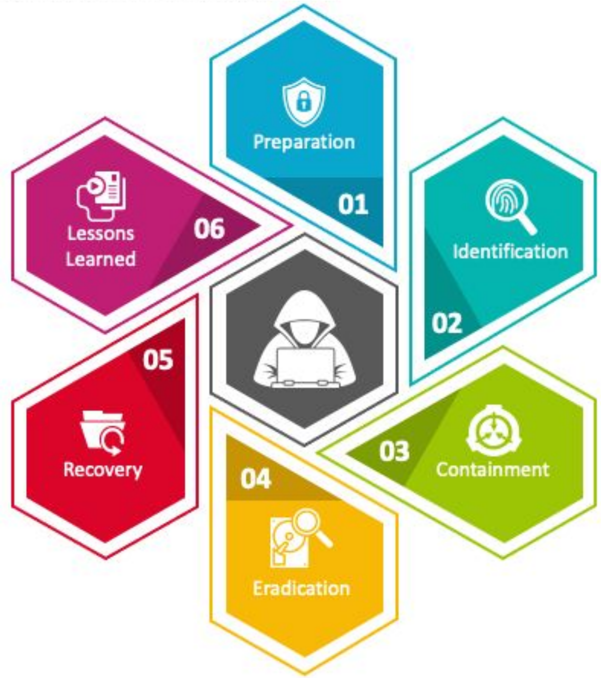
Mitigate
(Losses caused by incident)
Minimize incident impact (decrease M)

Response & Recovery
(Response and recovery time)
Rapid recovery (shorten R)

Source: Toshiba Cyber Security Report 2023

How does Cyber Resilience Work?

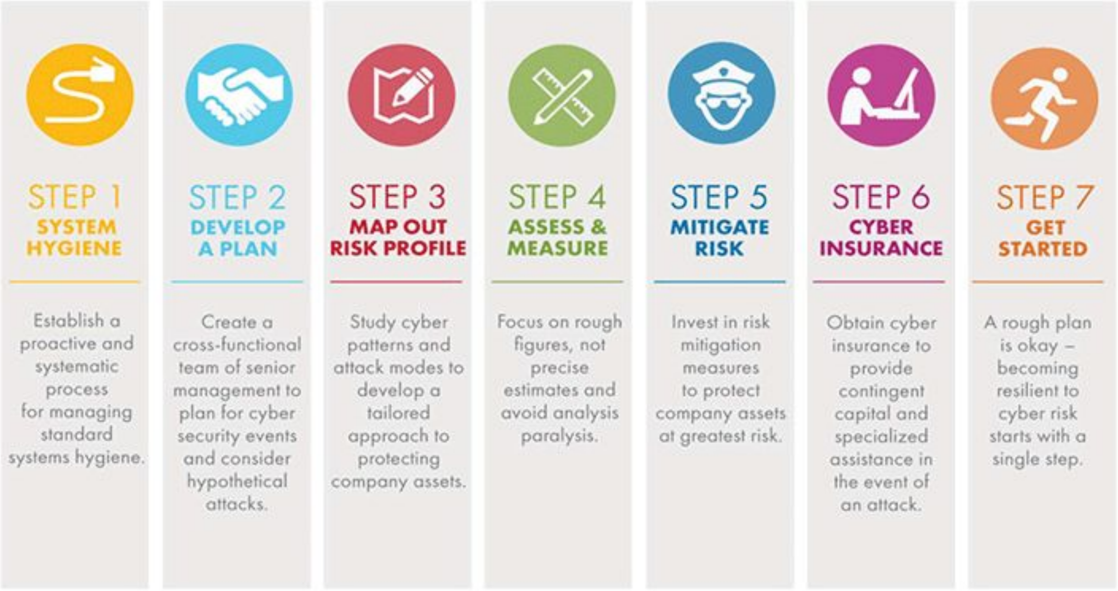
Cyber resilience is a continuous cycle of ongoing activities to counter current methods of attackers.



[Source: Compass IT Compliance *Incident Response Management: What Is It and How to Implement It*]

How to Achieve Cyber Resilience?

Follow best practices implementing cyber resilience, including cyber insurance!



STEP 1
SYSTEM HYGIENE

Establish a proactive and systematic process for managing standard systems hygiene.

STEP 2
DEVELOP A PLAN

Create a cross-functional team of senior management to plan for cyber security events and consider hypothetical attacks.

STEP 3
MAP OUT RISK PROFILE

Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.

STEP 4
ASSESS & MEASURE

Focus on rough figures, not precise estimates and avoid analysis paralysis.

STEP 5
MITIGATE RISK

Invest in risk mitigation measures to protect company assets at greatest risk.

STEP 6
CYBER INSURANCE

Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack.

STEP 7
GET STARTED

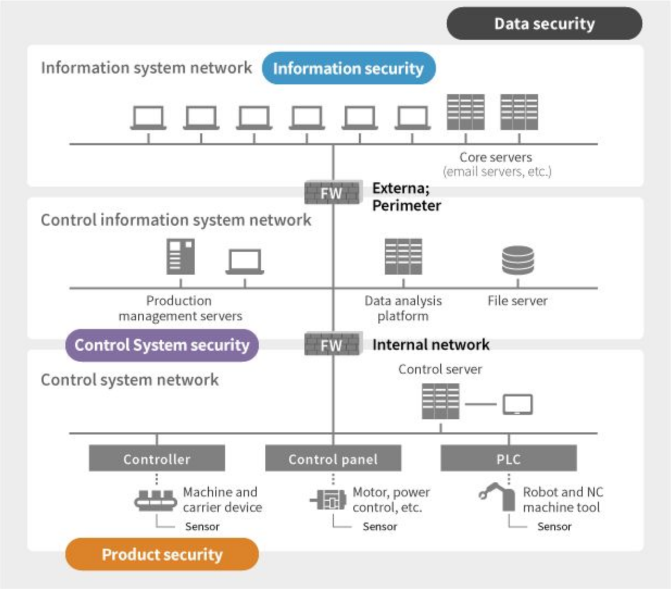
A rough plan is okay – becoming resilient to cyber risk starts with a single step.

Source: MHA Solutions Insurance & Benefits *Cyber Resilience in 7 Steps*

The Organization for Machine Automation and Control

What to Secure in Automation?

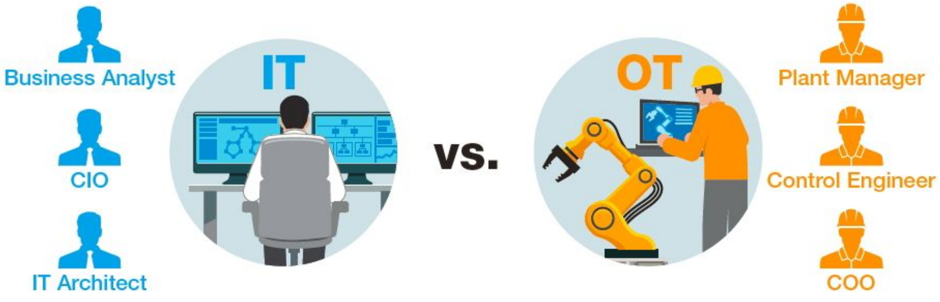
For key groups of assets to secure in automation



Source: Toshiba Cyber Security Report 2023

Impact of IT-OT Convergence

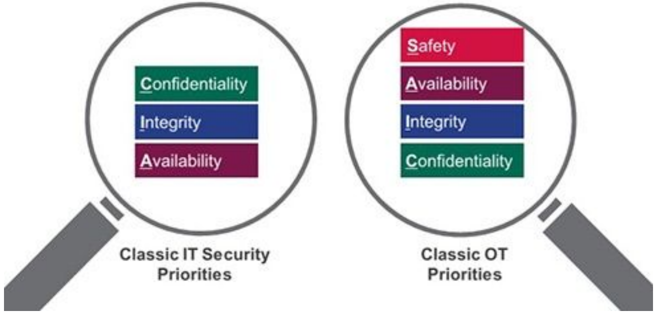
IT-OT convergence is both a **driving factor of the growing need** for cyber resilience in automation and **key to successfully implementing** cyber resilience in automation

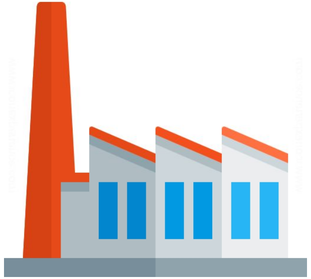


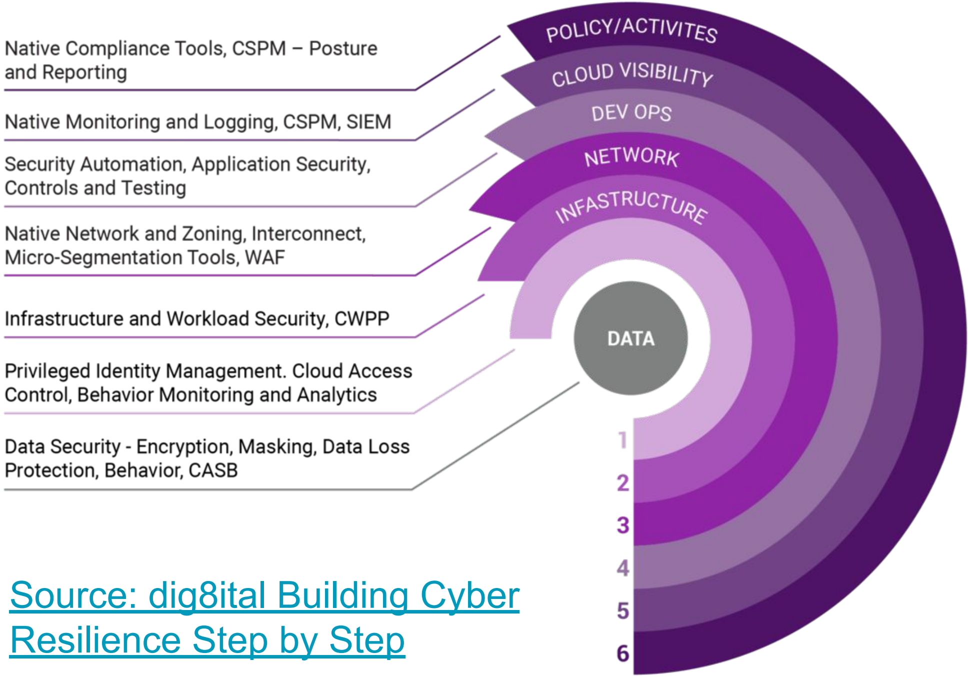
No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

Source: Control Engineering Magazine *Decoding OT data secrets*

Elements of Cyber Security







Native Compliance Tools, CSPM – Posture and Reporting

Native Monitoring and Logging, CSPM, SIEM

Security Automation, Application Security, Controls and Testing

Native Network and Zoning, Interconnect, Micro-Segmentation Tools, WAF

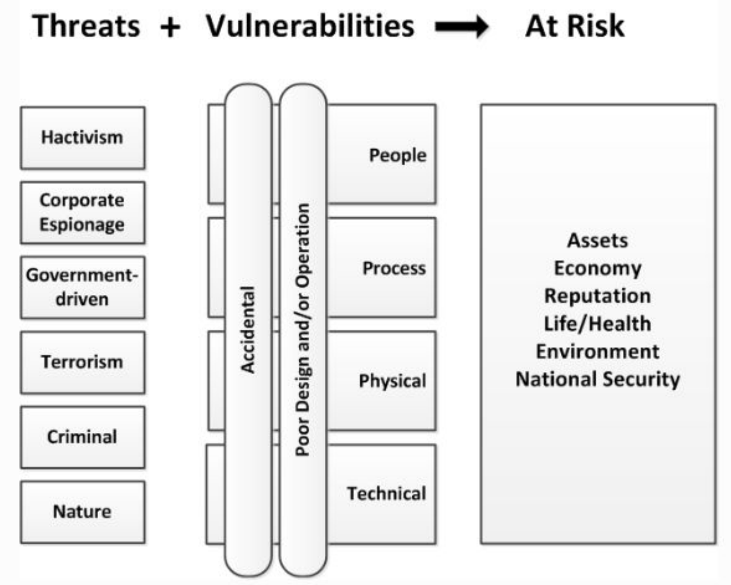
Infrastructure and Workload Security, CWPP

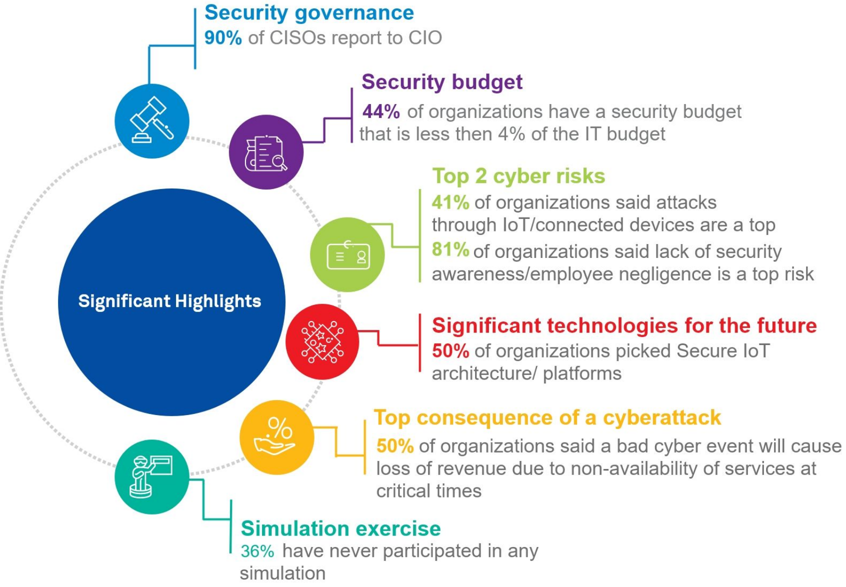
Privileged Identity Management. Cloud Access Control, Behavior Monitoring and Analytics

Data Security - Encryption, Masking, Data Loss Protection, Behavior, CASB

Source: dig8ital Building Cyber Resilience Step by Step

Risk and Cost Management





Security governance
90% of CISOs report to CIO

Security budget
44% of organizations have a security budget that is less then 4% of the IT budget

Top 2 cyber risks
41% of organizations said attacks through IoT/connected devices are a top
81% of organizations said lack of security awareness/employee negligence is a top risk

Significant technologies for the future
50% of organizations picked Secure IoT architecture/ platforms

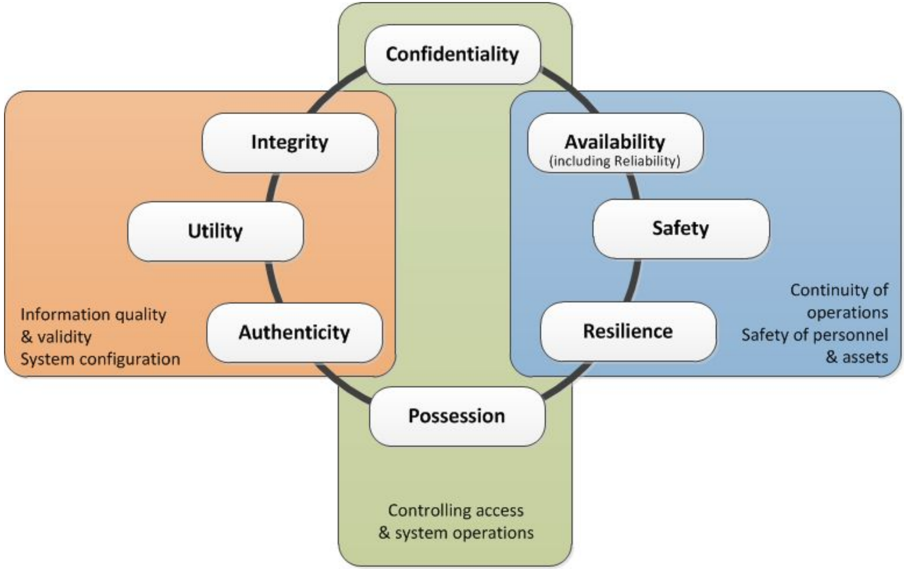
Top consequence of a cyberattack
50% of organizations said a bad cyber event will cause loss of revenue due to non-availability of services at critical times

Simulation exercise
36% have never participated in any simulation

Source: Wipro Digital Transformation Consulting Services

Adopting a Cyber Resilient Culture in Automation

- Data governance
- Legacy systems
- Compatibility with existing IT security
- Collaboration with 3rd parties (system integrators, OEM service technicians)
- Workplace safety is paramount



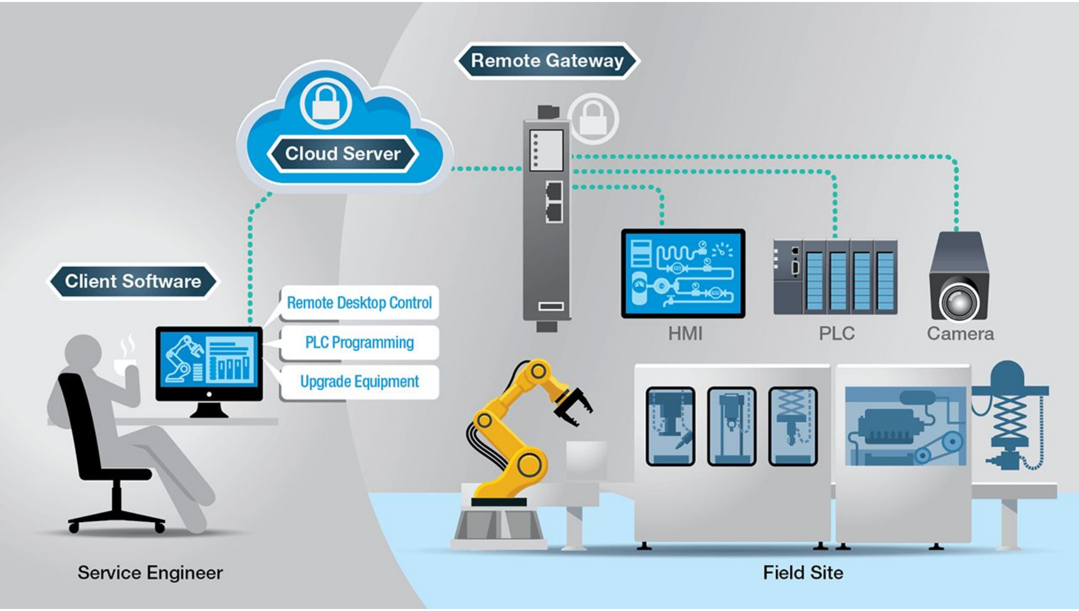
Source: International Journal of Electrical and Computer Engineering *CSPCR: Cloud Security, Privacy and Compliance Readiness -A Trustworthy Framework*

Maximize Rewards to Justify Costs

OMAC
The Organization for Machine Automation and Control

Avoidance of internet connections in automation does not reduce the cost to secure assets.

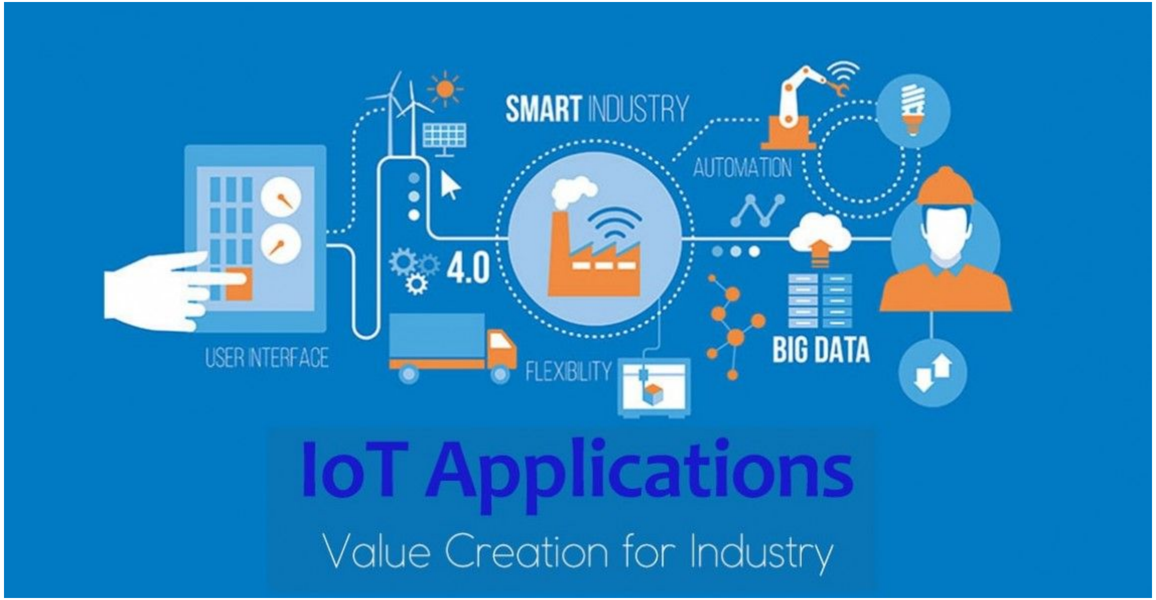
However, remote access delivers the fastest ROI for Industrial IoT, and can recover the cost of cyber resilience within weeks to months of implementation.



Source: Industrial Ethernet Book *Five key considerations for secure remote access solutions*

Maximize Rewards to Justify Costs

Collecting data in the cloud and use of IoT and mobile applications deliver even greater value than remote services, enabling the full power of data

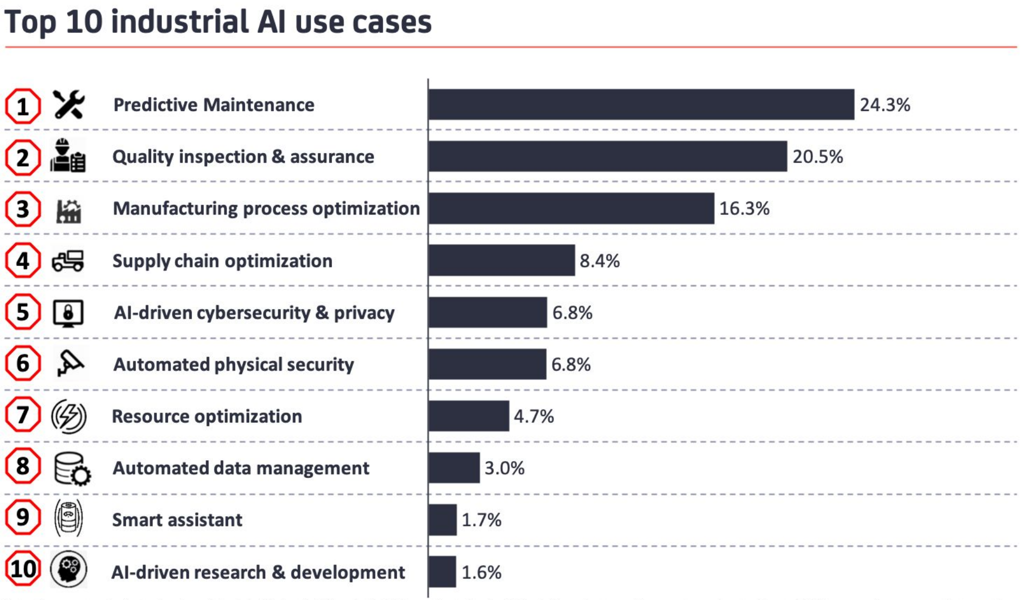


Source: Raya Fiber Pars Company IoT Applications Create Value for Industry

The Organization for Machine Automation and Control

Maximize Rewards to Justify Costs

AI back by data science and machine learning are rapidly changing how business design their products, provide service, maximize equipment uptime, and much more… Advantages achieved only with internet connections in automation and cloud-hosted data.



Source: IoT Analytics Top 10 Industrial AI Uses Cases

Start Your Cyber Resilience Journey

❑ Prioritize cyber resilience as a crucial cost of business

❑ Allocate resources to mitigate risks proportionate to the risks

❑ Seek expert guidance early

❑ Partner with the right technology and service providers

❑ Conduct cyber risk assessments for products and systems

❑ Involve all stakeholders, Engineering/Development, IT, Production, Quality, Service, Legal Counselors

❑ Apply best practices in remote access, cybersecurity for industrial systems, data governance

❑ Adopt Industrial IoT and begin using remote access and data to generate incremental revenue to recover the security budget and grow

Activity #1

Case Studies

- Colonial Pipeline Attack
- Stuxnet
- Havex
- BlackEnergy

Survey Question: Does your organization use any of the types of industrial control systems attacked in these case studies?

Responses to the survey at PackExpo LV 2023 revealed that virtually all of the packaging industry uses the types of system attacked in these well-known cases studies!

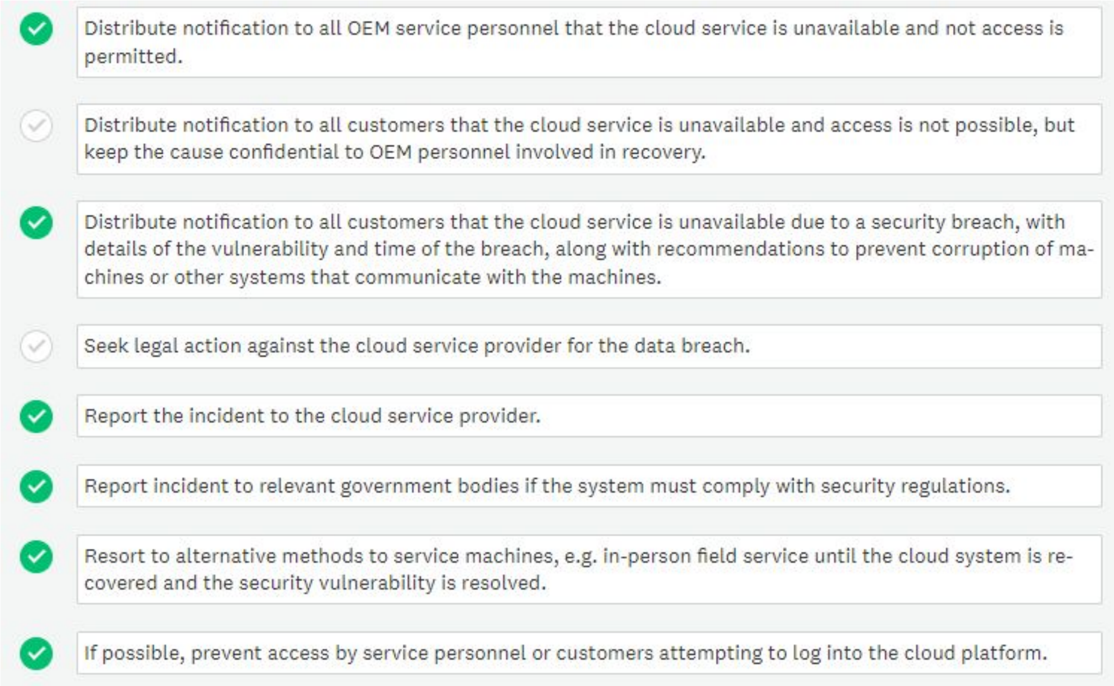
Activity #2

Response to an Attack

A machine builder offers a 3rd party cloud-based remote access service and data analytics solution for their machines. The OEM developed the service platform independently and maintains security directly. One day, the central system is corrupted because due to delays applying a security patch, allowing a security vulnerability to be exploited. Which steps should the OEM take in response to the incident?

OMAC
The Organization for Machine Automation and Control

Correct Answers to Activity #2



- ✅ Distribute notification to all OEM service personnel that the cloud service is unavailable and not access is permitted.
- ○ Distribute notification to all customers that the cloud service is unavailable and access is not possible, but keep the cause confidential to OEM personnel involved in recovery.
- ✅ Distribute notification to all customers that the cloud service is unavailable due to a security breach, with details of the vulnerability and time of the breach, along with recommendations to prevent corruption of machines or other systems that communicate with the machines.
- ○ Seek legal action against the cloud service provider for the data breach.
- ✅ Report the incident to the cloud service provider.
- ✅ Report incident to relevant government bodies if the system must comply with security regulations.
- ✅ Resort to alternative methods to service machines, e.g. in-person field service until the cloud system is recovered and the security vulnerability is resolved.
- ✅ If possible, prevent access by service personnel or customers attempting to log into the cloud platform.

Responses to the survey at PackExpo LV 2023 revealed that liability, transparency, and confidentiality create challenging circumstances for businesses who fall victim to cyber attacks… further justifying the need to follow best practices and seek cyber insurance.

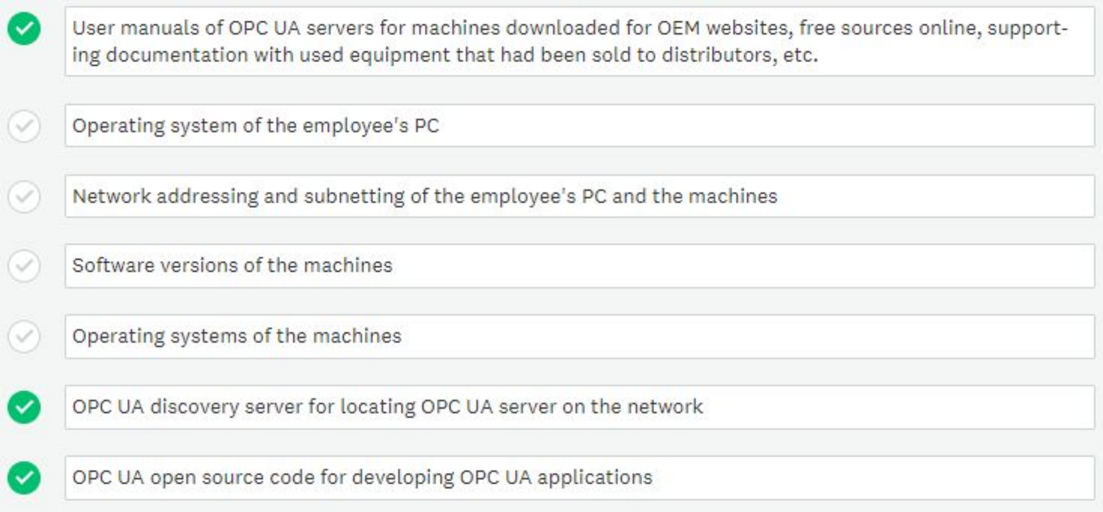
Activity #3

OMAC
The Organization for Machine
Automation and Control

Information Used by Attackers

An end users automates recipe management on their machines using OPC UA communication with a central database. One day, personnel realize that all the machines' active recipes have been set to incorrect values, and the OPC UA communication with the central database no longer functions, so the machines cannot easily be set to the correct recipe parameters. Upon investigating, the root cause was malware downloaded from a spear phishing email, opened by an employee. The employee is a system integrator who had connected directly to the machine's using OPC UA on their own PC when developing the automation with the central database. This malware stole OPC UA security certificates from the employee's PC, scanned for OPC UA servers in the PC's network, attempted to establish connections with machines that did not require authentication or that used default credentials, and continuously set parameters to random values until it was detected and disconnected. The manufacturer lost $5M due to 12h of downtime. The spear phishing email knew the employee's identity, their role as a systems engineer, the list of machines and models in the factory, and the use of OPC UA communication. All this information came from a User Requirement Specification (URS) the employee had created when procuring the machines. It is unknown whom or how the URS leaked into the hands of the attacker. Other than the details in the URS, what information might the attacker have used?

Correct Answers to Activity #3



- ✅ User manuals of OPC UA servers for machines downloaded for OEM websites, free sources online, supporting documentation with used equipment that had been sold to distributors, etc.
- ○ Operating system of the employee's PC
- ○ Network addressing and subnetting of the employee's PC and the machines
- ○ Software versions of the machines
- ○ Operating systems of the machines
- ✅ OPC UA discovery server for locating OPC UA server on the network
- ✅ OPC UA open source code for developing OPC UA applications

Responses to the survey at PackExpo LV 2023 revealed that most professionals are surprised by how little information about their business would be required to launch a cyber attack. Moreover, much of the needed information is in the public domain, and attackers can often find more information from illicit sources.

OMAC

The Organization for Machine Automation and Control

Thank you!