Rockwell Automation

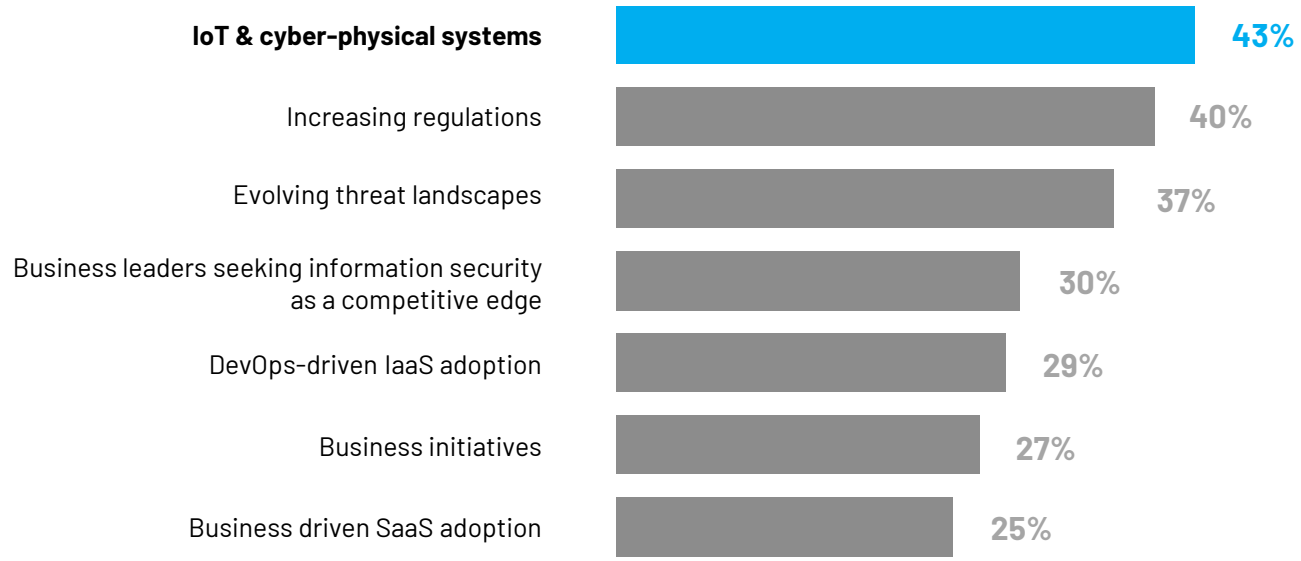
OT Cybersecurity

A Risk-Based Approach

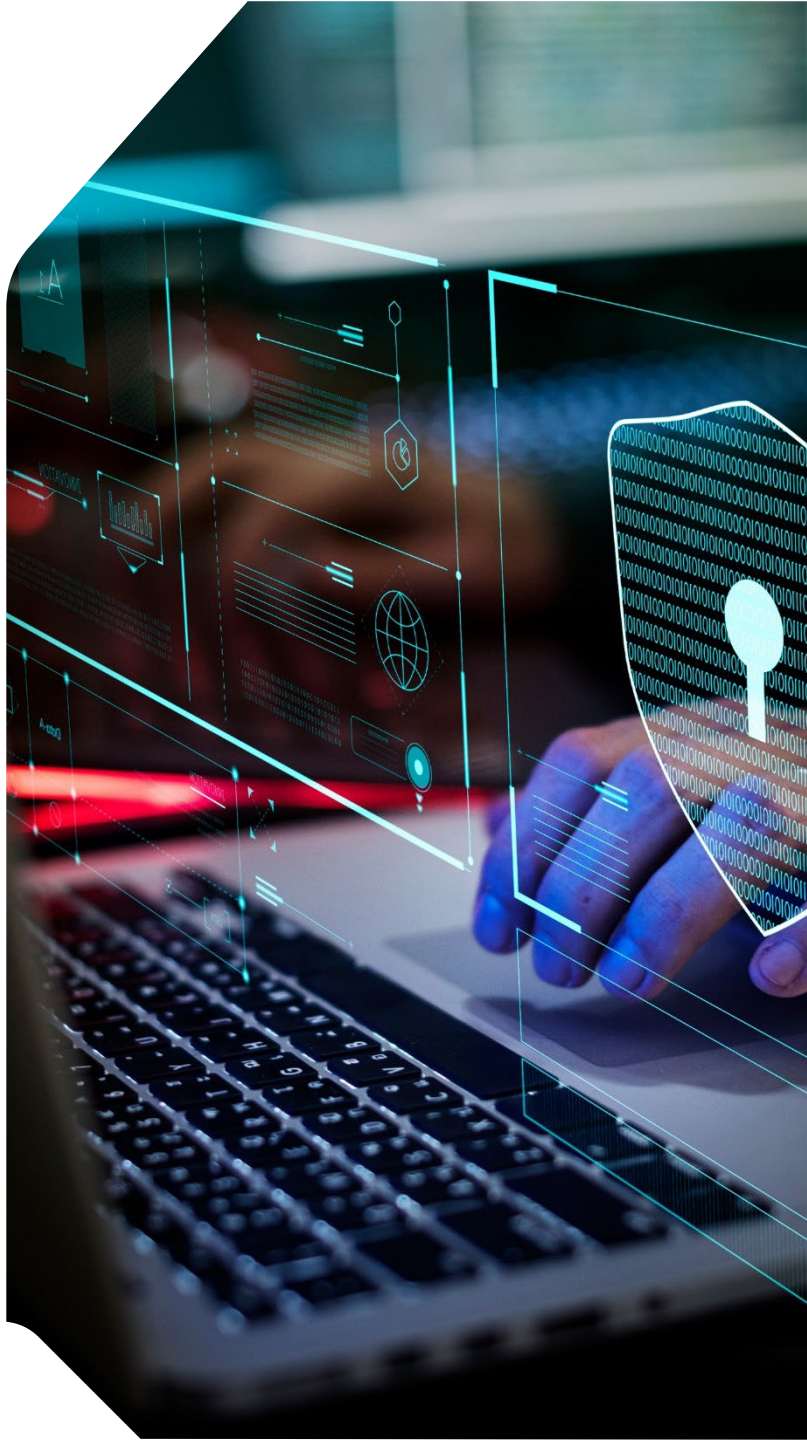
STEVEN HARTZFELD • CS BDL • 04•14•2022

expanding **human possibility**®

Top drivers impacting information security function and controls in the next 3-5 years



> **"Most organizations are still in the awareness phase for [IoT Security], but with attack vectors expanding and helpful tools only just emerging, security and risk management leaders need to update their current threat management strategies."** *- Gartner and Thielmann*



IT/OT CONVERGENCE

TRANSACTIONAL INFO

Priority is pervasiveness of data and confidentiality of such data

Architectures are ubiquitous in nature and consist of multi-tiered systems to encourage wide accessibility

Endpoints are of homogenous make and multi-purpose with short lifespans

Outcomes are digital

REAL-TIME DATA

Priority is on reliability and integrity of the system, uptime is key

Architectures are of proprietary nature and consist of isolated, task- specific systems.

Endpoints are of heterogeneous make and task-specific with long lifespans

Outcomes are physical

Cyber crime pays, and it's only getting worse

IN THE LAST 3 YEARS

$12+B

in damages due to ransomware attacks

53%

of industrial manufacturers have experienced a cybersecurity breach in their facility

WHY ARE INDUSTRIAL COMPANIES A TARGET?

Legacy unpatched infrastructure and a lack of skilled resources to properly manage cyber risk. The adversaries know these environments have many vulnerabilities and if attacked can mean major consequences for the infected.

WHY ARE COMPANIES STRUGGLING TO ADDRESS THIS?

Most industrial automation environments are poorly inventoried. If you do not know what is connected in the environment, you cannot secure it.

Source: *Cybersecurity Ventures. LNS Research Study.*

ICS-Focused campaigns, attacks

SolarWinds – software supply chain attack

Israeli National Water Supply – targeted command & control systems

Taiwan State Energy Company – ransomware attack

56% of gas, wind, water, solar utilities breached in prior year*

Majority of IT security pros most concerned about critical infrastructure

2021 – Oldsmar, Florida Water Treatment Facility, JBS Foods, Colonial Pipeline, Accenture

2010

STUXNET

Worm targeting SCDA and modifying PLCS

OPERATION AURORA

APT cyberattack on 20+ high tech, security & defense companies

2011

NIGHT DRAGON

Worm targeting SCDA and modifying PLCS

DUQU

APT cyber attack on 20+ high tech, security & defense companies

2012

SHAMOON

Virus targeting energy sector largest wipe attack

FLAME

Virus use for targeted cyber espionage in the Middle East

GAUSS

Information stealer malware

2013

RED OCTOBER

Cyber-espionage malware targeting government & research organizations

2014

HAVEX

Industrial control system Remote access trojan & information stealer

HEARTBLEED

Security bug and vulnerability exploited by attackers

2015

BLACK-ENERGY

Malware injected into Ukrainian power company network, cut power to the affected region

2016

BLACK-ENERGY

Malware injected into power company network;, attackers cut power to the affected region

OP GHOUL

Spear-phishing campaign targeting Middle East industrial organizations

2017

NOTPETYA

Ransom malware based on stolen NSA exploits the impacted ICS systems

INDUST-ROYER

Malware targeting electric utility – used in 2016 Ukraine grid attack

WANNACRY

General ransomware which impacted ICS systems

2018

SHAMOON3

Wiper oil & gas, telecom & gov Southeast Europe & Middle East

OPERATION AURORA

APT 20+ high tech, security & defense companies

2019

LOCKER-GOGA

Ransomware with wiper capabilities

BITPAYMER

Ransomware big game hunting

MAZE

Ransomware and stole/ exposed information

2020

EKANS RANSOMWARE

Design specially to target critical ICS process

RYUK RANSOMWARE

Encrypts network drives and other user resources while also deleting backups

2021

RANSOMWARE

Major brewing company

RANSOMWARE ATTACK

Canadian company's refusal to pay ransom resulted in detailed plans of military spy plane leaked on the dark web by hackers

UNAUTHORIZED ACCESS

Water system compromised - probably due to poor password security, and an outdated operating system

*https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1600101948/siemens-cybersecurity.pdf
**https://info.claroty.com/the_state_of_industrial_cybersecurity_form

New requirements for industrial cybersecurity

Digital transformation creates cyber risk to industrial operations that needs to be mitigated

	INSIDERS	TERRORISTS	HACKTIVISTS	CYBERCRIMINALS
The situation	• Assets communicating with proprietary protocols • Emerging Technologies with new communication methods • Dissolution of the traditional Purdue Model	• Limited understanding of the inherent risk of OT environments • Gaps of understanding to compensating controls • Unclear how to prioritization risk mitigation	• Opportunistic attacks such as ransomware still active • Targeted cybercriminal attacks for financial gain • Targeted nation state-sponsored actors projecting power	• IT Security tools do not have native visibility into OT environments • Decision makers need a comprehensive view of enterprise risk
The new requirements	• Visibility into assets, network communications and processes • Visibility into brownfield (OT) and greenfield (IIoT, IoT) assets	• Determine the inherent risk of OT assets • Prioritize risk mitigation actions to reduce risk • Understand residual risk after controls are applied	• Monitor remaining risks for signs of attacks • Establish a resilient detection model to spot different attack vectors	• Connect OT security into IT security architecture • Provide a comprehensive view of OT risk to decision makers

NIST Cyber Security Framework (CSF)

A proactive approach to industrial cybersecurity

Attack continuum

Identify & Protect

- Asset inventory services
- Qualified patch management
- Vulnerability and risk assessments
- ICS security zone and countermeasure deployment

Detect

- Real-time threat detection services
- Remote monitoring and administration services
- Incident handling and response
- Incident response and disaster recovery planning services

Respond & Recover

- Backup and recovery solutions

BUILD A SECURE, ROBUST, FUTURE-READY NETWORK FOR YOUR CONNECTED ENTERPRISE

IDENTIFY

Assessment, Asset Identification & Migration Services

Asset inventory intelligence is the first critical step to understanding cybersecurity risk. Once identified, improving overall risk posture with proactive countermeasures is the next step in improving cyber hygiene, while outlining capital and operational requirements for financial planning and prioritization

1

Assessment
SERVICES

Risk Assessment

Comprehensive network assessment

Penetration Testing

Vulnerability Assessment

2

Asset Identification
SERVICES

Security posture survey

Asset identification and vulnerability via threat detection services platform deployment

Physical or Digital Data Collection via MyEquipment™

3

Migration Planning
SERVICES

Legacy automation hardware migration

Process system server migration

Comprehensive (OT) network design and implementation

4

Software Planning
SERVICES

Automation software migration

Anti-virus management

Qualified patch management

PROTECT

ICS Countermeasure Deployment Services

Deployment of countermeasures are steps taken before a cyber incident, beginning with safe, secure segmentation of the logical and physical network and enhanced by perimeter hardening, end point protection, and physical to virtual migration services

1

Perimeter Hardening

SERVICES

Firewall design and implementation

Secure remote access

2

IDMZ Deployment

SERVICES

Comprehensive design and implementation

IDMZ functional specification and documentation

3

End Point Security

SERVICES

USB cleansing

Application whitelisting

Anti-malware management

4

Infrastructure

MIGRATION SERVICES

Physical to virtual server migrations

Pre-engineered (OT) data center deployment

Legacy (OT) data center migrations

ThinManager deployment

DETECT

Threat Detection Services

During an attack, reducing real-time risk by continuous monitoring and operational response is the next step in the attack continuum

1

Software Deployment & Configuration

SERVICES

Continuous threat detection deployment

Pre-configured hardware and remote configuration

Scalable site or enterprise management deployment

2

Threat Detection Managed

SERVICES

Security alert review, system tuning, training and configuration of the threat detection platform

Monitoring and administration of infrastructure hardware

RESPOND

Network and Cybersecurity Managed Services

Across the attack continuum, enabling real-time support will provide monitoring, administration, and management of OT infrastructure, automation hardware, and software applications by complementing or augmenting on-premises workforce with 24x7x365 remote domain expertise and SOC Feed capabilities

1

OT Network Managed
SERVICES

Remote hardware configuration

Network backup, storage and documentation

Warranty management

Network troubleshooting and performance monitoring

2

Antivirus Management
SERVICES

Virus definitions

Scheduled management

Quarantine and anti-malware remediation

3

OT Firewall Managed
SERVICES

Web proxy management

Security appliance monitoring

Warranty management

4

Application Managed
SERVICES

Real-time application status and health

Alarm management and notifications

Lifecycle management

5

Data Center Managed
SERVICES

Hardware environment, VM status, backup and OS monitoring

Storage management, switch configurations, virtual image management

Warranty management

Managed Services Coming Soon!

Secure Remote Access

IDMZ

End Point

RECOVER

Backup and Recovery Services

Recovery time and readiness to restore operations after a cybersecurity incident can be minimized with both on-premises and off-premises services, 24x7x365 with domain expertise

1

FactoryTalk® AssetCentre
SERVICES

Policy creation and administration

User management

Configuration management

Automation software backup and recovery

2

Virtual Backup Management
SERVICES

On-premises data center backup

Off-premises administration

3

Onsite Field Labor Recovery
SERVICES

Data center server replacement

Firmware upgrades

Application restoration

This recommended approach improves risk posture with limited capital expenditure and shortened implementation timelines

ESTABLISH ASSET VISIBILITY
- Conduct asset inventory analysis and vulnerability awareness

DETERMINE CURRENT RISK POSTURE
- Conduct risk assessment
- Conduct penetration testing for OT environment
- Review and establish framework and standards

DEVELOP BASE CYBERSECURITY HYGIENE PROGRAM
- Develop unified IT and OT stakeholder governance model
- Develop anti-malware strategy
- Execute legacy physical server to virtual server migrations
- Deploy anti-virus management measures
- Execute (OS) infrastructure patching services and software patching schedule
- Create backup and recovery plan

OT NETWORK READINESS
- Conduct comprehensive OT level network assessment
- Complete comprehensive design of logical OT network and IDMZ to create segmentation

This approach is a more foundational way to improve overall cybersecurity risk posture with moderate capital investments and defined operational expenditures

COMPREHENSIVE INSTALLED BASE REVIEW AND MIGRATION

- Conduct physical or digital installed base evaluation to identify legacy or new automation, software or network devices connected or un-connected to plant networks
- Modernize legacy automation assets, process systems, and software platforms

DEPLOY SEGMENTATION BETWEEN IT AND OT ENVIRONMENT

- Complete comprehensive IDMZ design and implementation
- Complete comprehensive OT network implementation
- Implement secure remote access platform

SECURE ENDPOINTS

- Deploy OT endpoint security platform
- Implement modern device level network or machine level network

DEPLOY CONTINUOUS THREAT DETECTION

- Deploy scalable threat detection services platform and tune system
- Develop and execute continuous risk management program

MONITOR AND MANAGEMENT OT ENVIRONMENT

- Applications, data centers, firewalls, IDMZ, network, and threat detection platform 24x7x365

CREATE DISASTER RECOVERY PLAN

- Deploy and adjust disaster recovery plan

This approach outlines a comprehensive OT cyber strategy providing a multi-year approach and blueprint to all elements of an adaptive program approach. This would include detailed financial capital planning, cultural change management outcomes, and workforce skills gap mitigation by providing security managed services

MODERNIZE PLANT(S) OR ENTERPRISE INSTALLED BASE

- Migrate all legacy automation hardware, software, process systems or platforms
- Migrate all remaining physical servers to full compute infrastructure virtual environments

MODERNIZE OT NETWORKS

- Implement detailed logical and physical networks from design including IDMZ implementations
- Deploy micro-segmentation strategy

DEPLOY CONTINUOUS MONITORING CAPABILITIES

- Implement secure remote access and end-point protection platforms

EXPAND TO INTEGRATED SECURITY MANAGEMENT AND ADMINISTRATION

- Network, firewall, data centers, applications, threat detection platforms, antivirus, endpoint, secure remote access, IDMZ and patch management

AUGMENT WORKFORCE WITH SECURITY OPERATIONS CENTER

- Integrate OT telemetry with security operations teams or with 3rd party managed service provider

DEVELOP INCIDENT RESPONSE HANDLING

- Create and deploy incident response workflows, procedures, and teams to increase speed of recovery

Planning the roadmap

A step-by-step approach

PROCESS

STRATEGY REVIEW

- Review current risk-based approach or framework
- Understand future operating vision
- Review current cybersecurity strategy
- Understand collaborative stakeholder needs
- Create alignment around a single vision for cybersecurity framework

ACTIVITY

Leadership interviews, workshops, governance model(s)

IDENTIFY OPPORTUNITY

- Conduct asset inventory and vulnerability assessment
- Determine applicable standards of cybersecurity implementation requirements
- Identify sample facilities to review and understand operating practices
- Determine which areas across the attack continuum are areas of primary focus
- Identify risk impact and tolerance for immediate projects

ACTIVITY

Plant visits, performance data review

BUSINESS CASE

- Align IT and OT stakeholder needs and ROI
- Develop project or program costs, time horizon and commitment to prioritizing capital or operational expenses
- Identify operational improvements that meet investment requirements
- Determine financial stakeholder approval cycles and requirements
- Evaluate and document workforce skills requirements to support strategy

ACTIVITY

Analysis, stakeholder inputs

COST ESTIMATES

- Develop initial cost estimates for pilot facilities or enterprise roadmap needs
- Plan costs and resourcing requirements; Customer/Rockwell and partners to understand and plan for a multi-year implementation and investment planning

ROADMAP

- Projects, pilots or facilities that meet investment requirements are sequenced
- Organizational stakeholders and teams are aligned on outcomes
- Program management philosophy is documented and established
- Initiative can be funded in CapEx/OpEx over multi-year stages
- Project timelines and resources are estimated to allow effective planning

ACTIVITY

Working sessions, leadership review

EXPANSION OF CYBERSECURITY EXPERTISE

with the acquisitions of Avnet and Oylo

Two cybersecurity providers that bring cutting edge cyber security resources and skills that allow an acceleration of the Rockwell Automation cybersecurity business.

200+
Domain experts available for global deployment

20+
Years of combined **cyber experience** in IT/OT

CUSTOMER OUTCOMES

Provide visibility to cyber risk in OT environment

Deploy security controls at scale to manage risk

Continuously manage and monitor OT cyber risk

WHAT SETS US APART?

IT/OT domain expertise

Industry expertise

Discipline global delivery

24x7x365 Managed Support

2021 TRENDS AND TOP CUSTOMER CHALLENGES ASSOCIATED WITH CYBER SECURITY THREATS

Increase in IoT initiatives to drive productivity exposes security risks due to connected IT/OT Infrastructure and expand the attack surface to threat actors

Increased need for secure remote access to enable a remote workforce, even once the COVID-19 vaccine becomes widely available.

Continued challenges in patching and maintaining cyber hygiene on OT devices due to the severe interruption of services

Breaking News

- ***Wednesday, April 13, 2022***
  - DoE, CISA, NSA, and FBI release joint advisory re: PIPEDREAM
- ***PIPEDREAM – Advanced, ICS-Specific Malware Toolset***
- ***"…the most expansive [ICS] attack tool… ever documented."***
- ***"…like a Swiss Army knife with a huge number of pieces"***

  -VP of Threat Intelligence, Dragos, Inc.
  - Array of tools to disrupt or take control of ICS device function
  - Only the 7th documented ICS-specific malware
  - New threat actor (APT) "CHERNOVITE"
- ***Has not yet been deployed in the wild***
  - Same mitigating steps discussed here apply

Key Points and Takeaways

- ***There is no silver bullet***
  - Defense-in-depth strategy mitigates risk of incident AND impact
- ***Know your risks***
  - Includes understanding your asset risks and business risks
- ***Examine risk holistically***
  - Strike a balance between business and security risk mitigation
- ***Work with trusted partners on a roadmap***
  - Rockwell Automation and others can help
- ***Don’t get phished!***
  - There is no Nigerian prince who wants to give you $Millions

Thank you

www.rockwellautomation.com

Rockwell Automation

expanding human possibility®

PUBLIC