



# BAS & Cybersecurity



# Presenter




**Brian Meyers**  
Senior Product Manager

# Learning Objectives

- Identify potential operational opportunities provided by modern control systems.
- Understand key risk factors around modern control systems.
- Understand Methods for making cybersecurity teaming easier & more productive.
- Coming Soon...

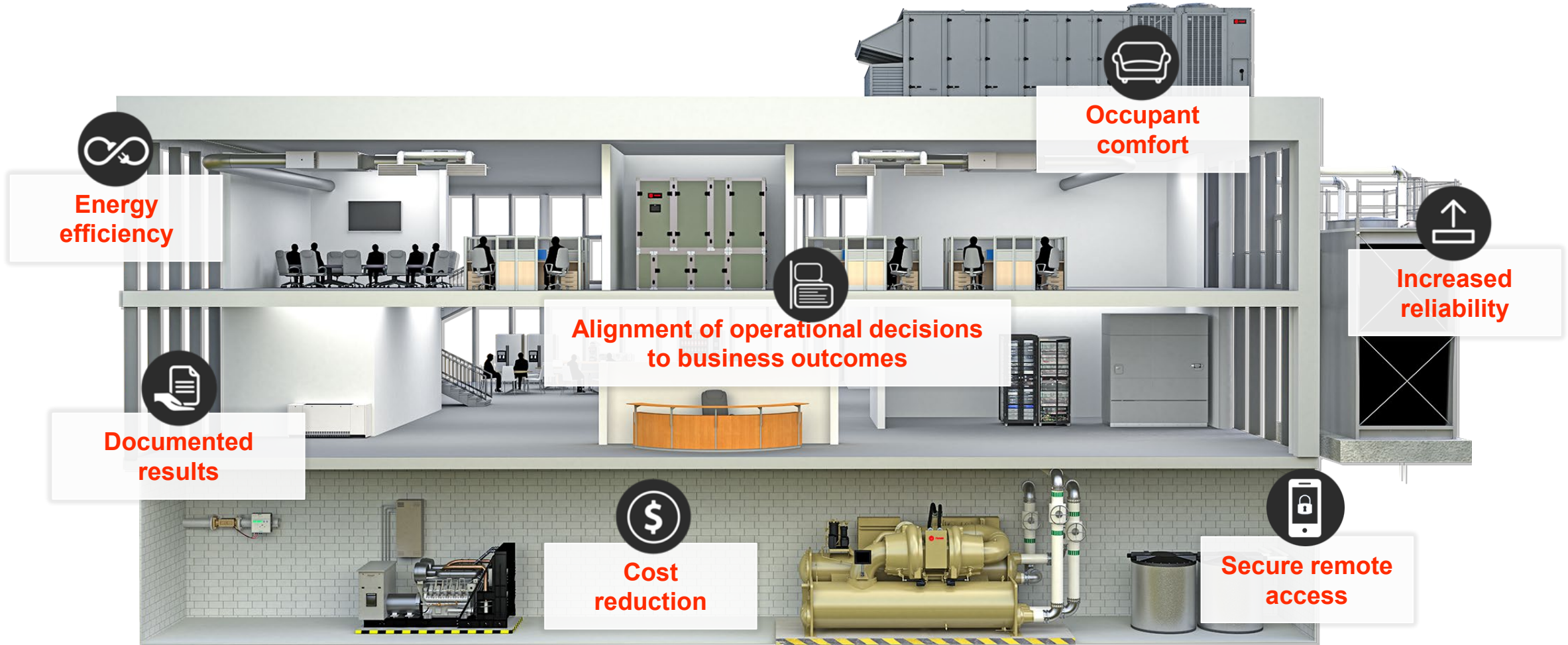
Add your  
questions to  
the chat for  
the Q&A  
session!



A photograph of two men in a server room. The man on the left is wearing a yellow safety vest over a blue shirt and glasses. The man on the right is wearing a grey sweater over a blue shirt and is holding a silver laptop. They are both looking at the laptop screen. The background consists of several rows of server racks with blue and green lights.

**Modern control systems can  
provide new opportunities...**

# Building Owners are looking to streamline operations



# Convergence of Information Technology (IT) and Operational Technology (OT)

- The COVID-19 global pandemic has accelerated the Convergence of IT & OT (Figure 5)
- 61% of OT professionals expect this acceleration will continue post pandemic (Figure 4)
- OT professionals' opinions of Cybersecurity importance has changed dramatically. Figure 11 shows:
  - 14% drop in “impede operational flexibility”
  - 14% increase in “create business concerns”.

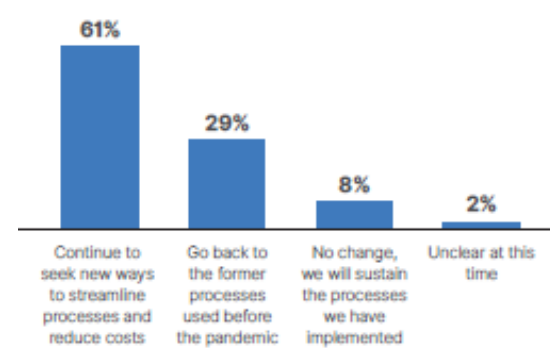


Figure 4: Post-pandemic work process adjustments.

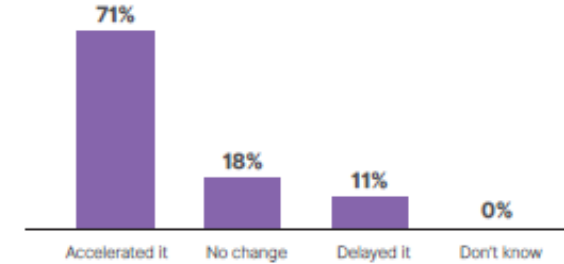


Figure 5: Pandemic impact on IT-OT convergence.

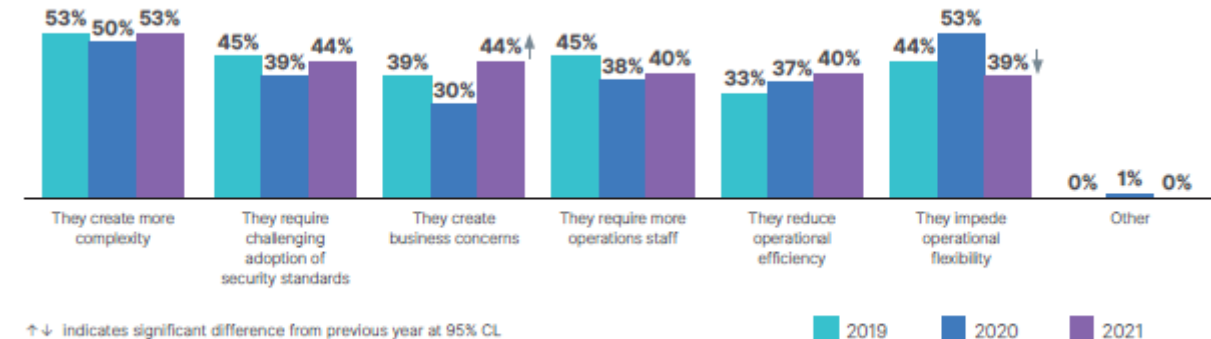


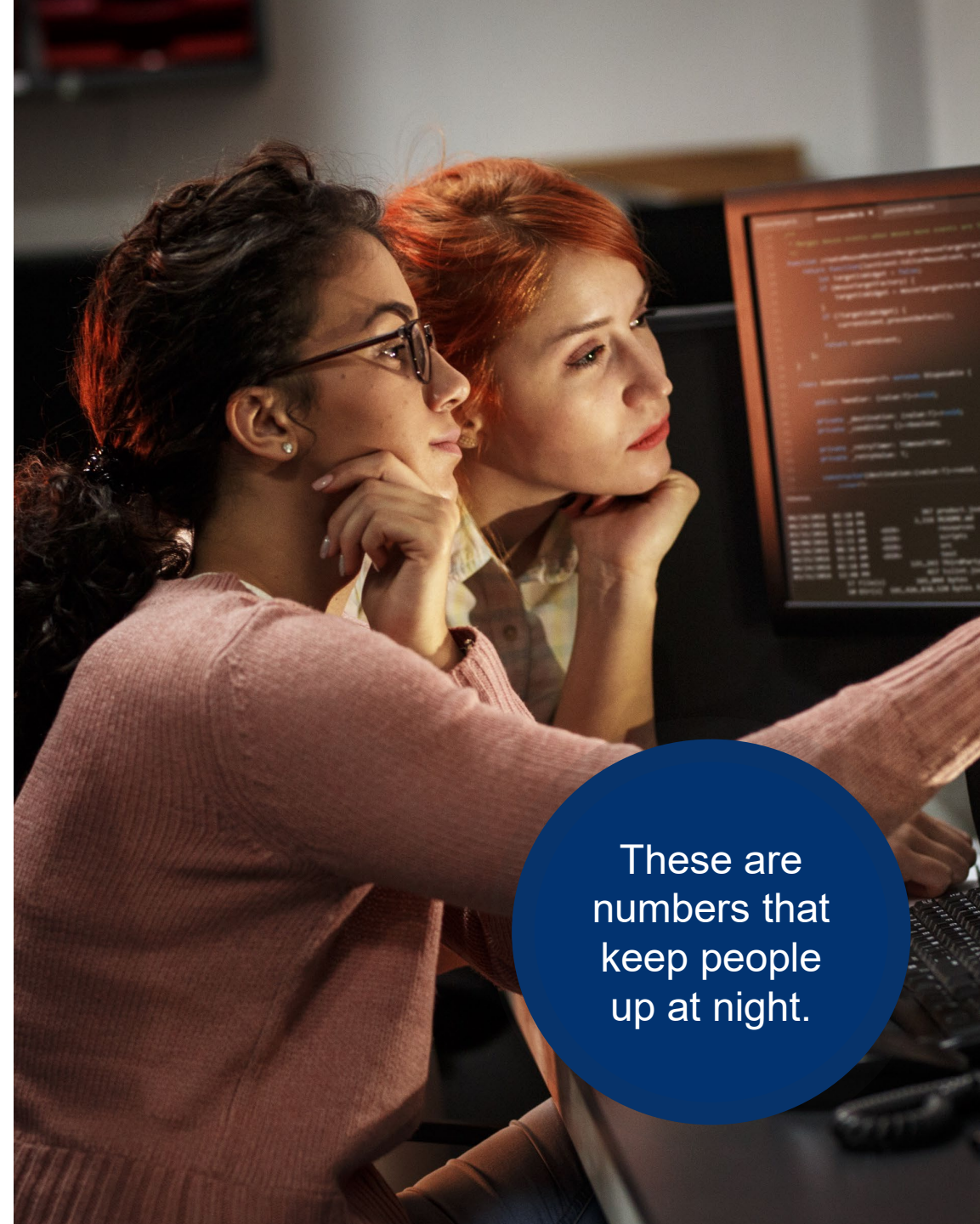
Figure 11: How cybersecurity solutions can negatively impact OT professional success (in top 3).



**...and can present new risks**

## A few background facts

- There were 2,935 publicly reported breaches in the first three quarters of 2020, with the three months of Q3 adding an additional 8.3 billion records to what was already the “worst year on record.” (Security Magazine® - Dec 2020)
- The global average cost of a data breach is \$3.9 million (IBM® – Aug 2020)
- Healthcare is the most expensive industry for a data breach at \$6.45 million (IBM® – Aug 2020)
- Data suggests that cybercrime cost businesses over \$2 trillion total in 2019 (Juniper® - May 2015)
- **Security threats against industrial control systems (ICS) and operational technology (OT) more than tripled in 2020 (Dragos, Inc® - Feb. 2021)**

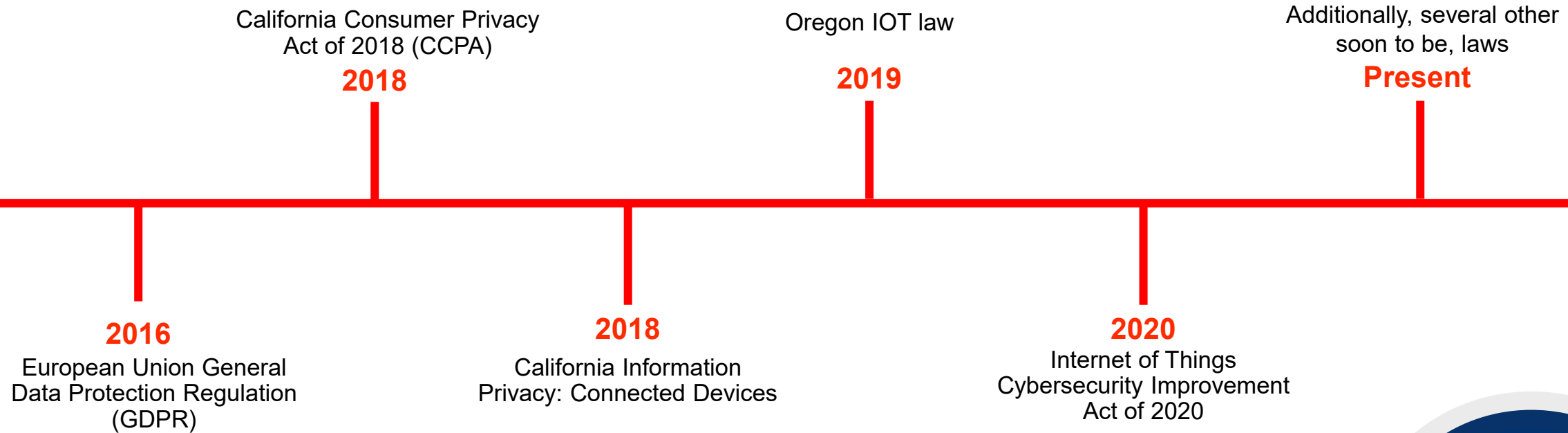


These are numbers that keep people up at night.



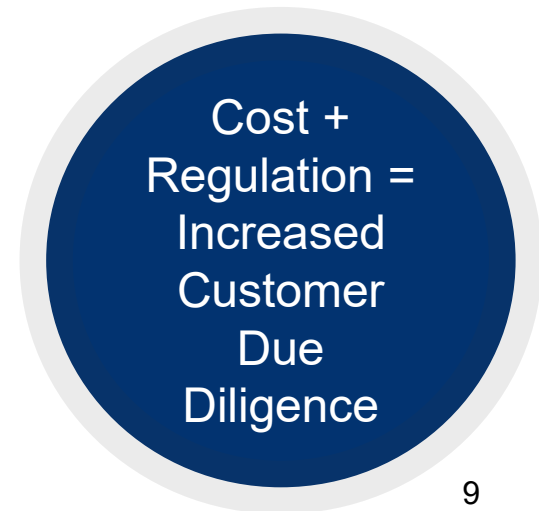
# Compliance as a first step... but is it a moving target?

Privacy/Security requirements & regulations have been inconsistent...



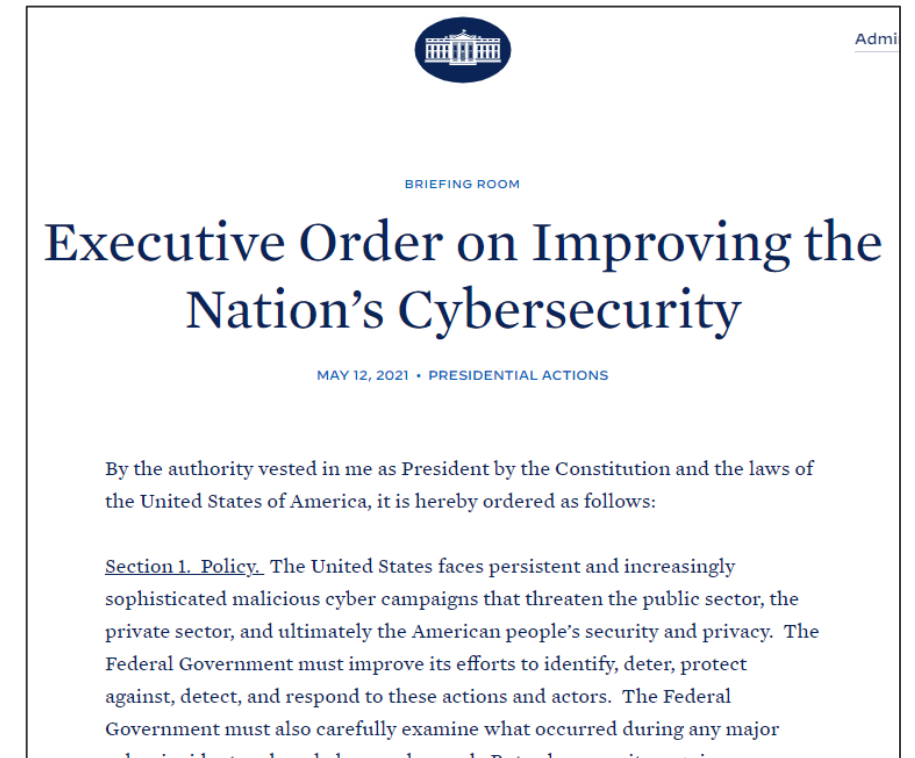
...However best practices have been remarkably consistent

- Restrict physical controller access
- Network isolation (firewalls, VLANS)
- Secure credentials (no sharing, complexity)
- Keep systems up to date



# Recognized importance of standards & regulations.

- Existing requirements and regulations have not slowed the pace of incidents.
- **Presidential Executive Order (May 12, 2021):**
  - “Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.”
  - “The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).”
  - “It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.”
- **This Executive Order contains explicit actions to drive public and private sector action. These actions will:**
  - Drive Product Standards
  - Standardize Vulnerability Disclosures
  - Improve Contract language
  - Identify other gaps and solutions



[Executive Order on Improving the Nation's Cybersecurity | The White House](#)

A photograph of two men in a workshop setting. The man on the left is wearing a red shirt and glasses, looking towards the man on the right. The man on the right is wearing a blue shirt and glasses, looking back at the man on the left. In the background, there is a large industrial machine, possibly a lathe, and several framed certificates or diplomas on the wall. A semi-transparent white banner is overlaid across the middle of the image, containing the text 'Risk Mitigation...' and 'A shared responsibility.'

# Risk Mitigation...

**A shared responsibility.**

# NIST®: Cybersecurity Framework

## Key Framework Attributes

*Principles of Current and Future Versions of the Framework*

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



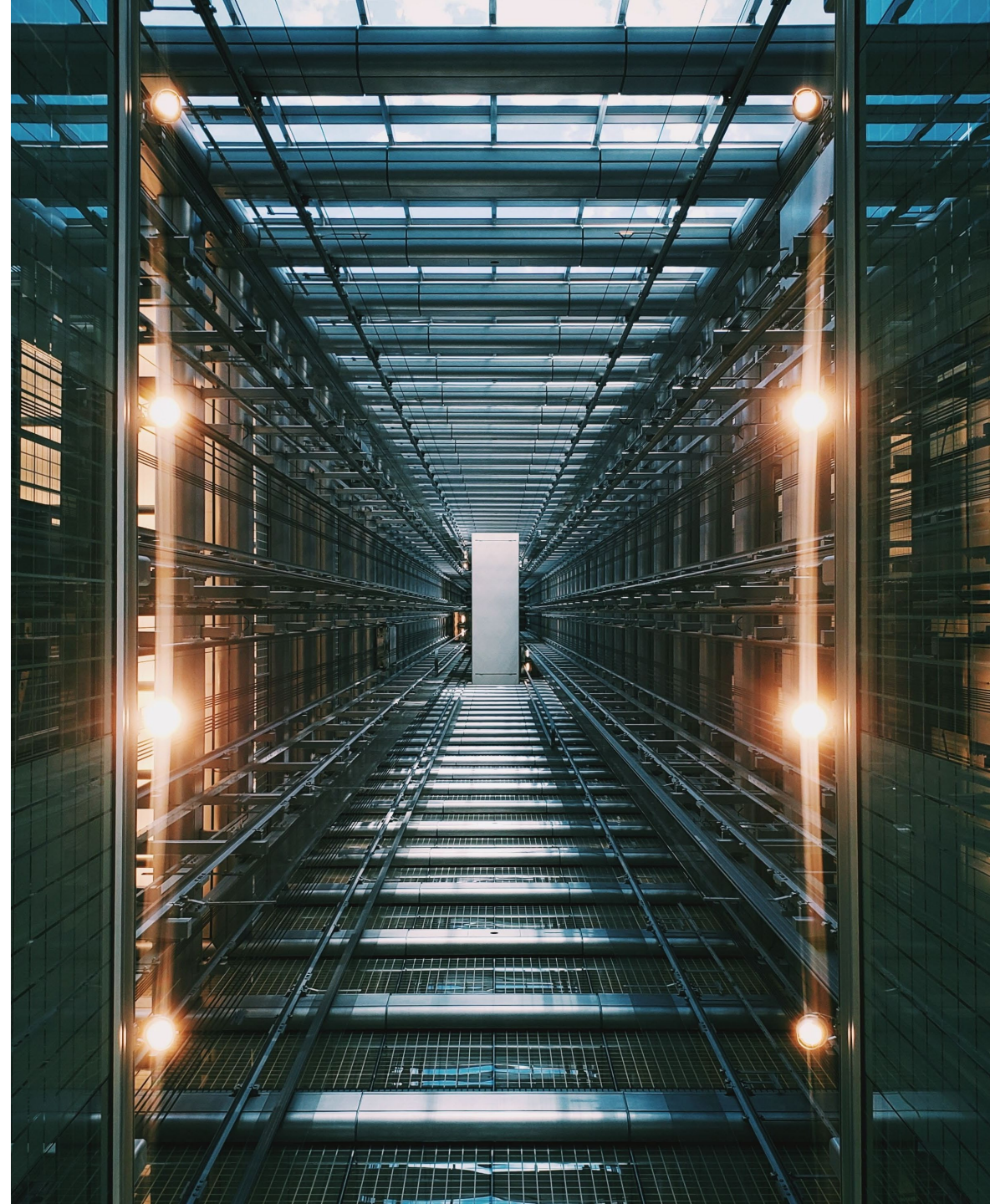
The living document is constantly evolving. How do we stay aligned?

No single person owns all these elements. Teaming is required.

[NIST Cybersecurity Framework](#)

## Challenge: cybersecurity teaming has been an inconsistent part of BAS

- Project specifications traditionally focused on OT, not IT/Security...
- Control system installers are historically reluctant to engage IT unless they need something...
  - Network drop
  - Static IP address
  - Protocol capture
  - Virtual/Physical Server
- **...as a result, important gaps can exist**
  - IT Requirements for controllers/hardening
  - System maintenance (Firmware/Software updates)
  - Auditing (software versions, firewalls, user credentials, etc.)
  - Vulnerability/Incident Response
  - Cybersecurity evolution (Zero Trust, BACnet/SC)



# Risk mitigation... How to ease the challenge



## Teaming

- Proactive communication bridges gaps
- Project specifications drive product requirements, installation best practices, and maintenance

## Secure Product

- Secure products as a foundation
- Out-of-box solutions can reduce common mistakes

## Secure Installation Practices

- Secure product not enough
- Best Practices must address installation process, user management, etc.

## Maintenance

- Controller Life Cycle
- Planned system maintenance
- Vulnerability Management

# Proactive communication bridges gaps

Communication with IT & Facility Managers is essential to address teaming gap:

- Clear communication of the “the why...”
- Standard terminology & diagrams (IT often requires specific keywords)
- Protocols and technology - “the how...”
- Facility Managers should be a part of the conversation to ensure sustainable solution.



# Project Specifications



- Specifications need to include security in project specifications
  - Customer value (e.g., remote access) and associated security controls (e.g., no exposed firewall ports)

The project's  
Control  
Contractor shall  
provide secure  
remote access to  
the building  
automation  
system (BAS)

Secure  
remote access to  
the BAS shall not  
require additional  
software to be  
installed on the  
client device  
(VPN)

Secure  
remote access to  
the BAS shall not  
require ANY  
inbound ports on  
a firewall to be  
“exposed” or  
“forwarded”



# Secure Product

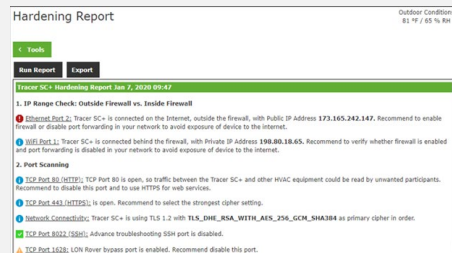
Teaming

Secure Product

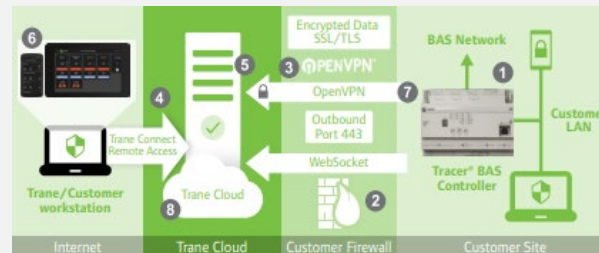
Best Practices

Maintenance

- Secure Product is the foundation for a securely deployed BAS
- Lack of product standards (constantly evolving) – early alignment with IT is critical
- Cybersecurity features are complex – out-of-box-solutions can reduce common application mistakes while simplifying IT engagement and maintenance



Hardening Report enables self scan for secure installation documentation



Secure Remote Access built-in, enables industry-standard IT connection methods



Cellular Module avoids internet exposure



## Tracer Ensemble Cloud

The Tracer Ensemble Cloud system provides software as a service (SaaS), hosted and managed by Trane. In this option, Ensemble is connected to your systems but doesn't require you to have a server or IT support, reducing both up-front costs and ongoing support.

Cloud services provides automatic maintenance for ongoing security software updates

# Secure Installation Practices

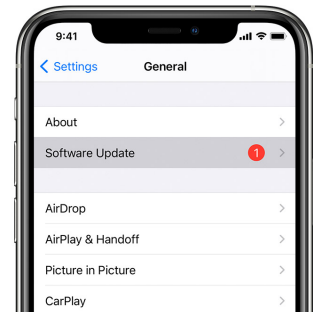
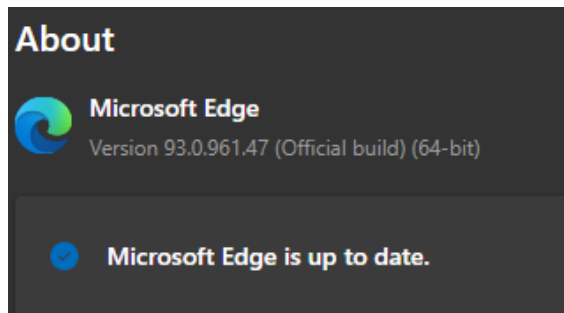
- Secure products aren't enough, secure installation practices are required. Examples include:
  - Restrict physical controller access
  - Isolate controls from other network devices (VLAN/Firewall)
  - Use secure remote access solutions that don't require exposed/forwarded firewall ports
  - Ensure secure user credentials that aren't shared
  - Have a well-documented process and owner to keep system up to date



# Maintaining firmware & software versions



- Consumer solutions often have automatic updates built in...
- These solutions eliminate active user ownership.



[Update your iPhone, iPad, or iPod touch - Apple Support](#)

- Harder to implement in a commercial environment.
- When BAS manufacturer produces a feature upgrade, bug fix, security patch then what...
- Specifications & contract terms must drive:
  - Clear understanding of controller lifecycles
  - Ownership & plan for scheduled & unscheduled updates
  - Appropriate maintenance intervals (frequency, day of week, time of day, etc.)

Controls manufacturer shall be responsible to perform software/firmware version updates according to the following schedule...

# Vulnerability Management

- Software vulnerabilities are a reality
- Defense in Depth is a necessary strategy
- Communication of vulnerabilities is changing
- Diligence is required to address vulnerabilities promptly
- Ownership for risk mitigation is paramount



[ICS-CERT Advisories | CISA](#)



Requirements on communications and ownership for patch deployment is essential.



**Coming soon...**

# BACnet® Secure Connect

- BACnet Secure Connect
  - Adds encryption to the BACnet/IP data link
  - Addenda to BACnet standard is published
  - Still a few gaps to interoperability (work in progress)
  - Broad commitment from manufacturers

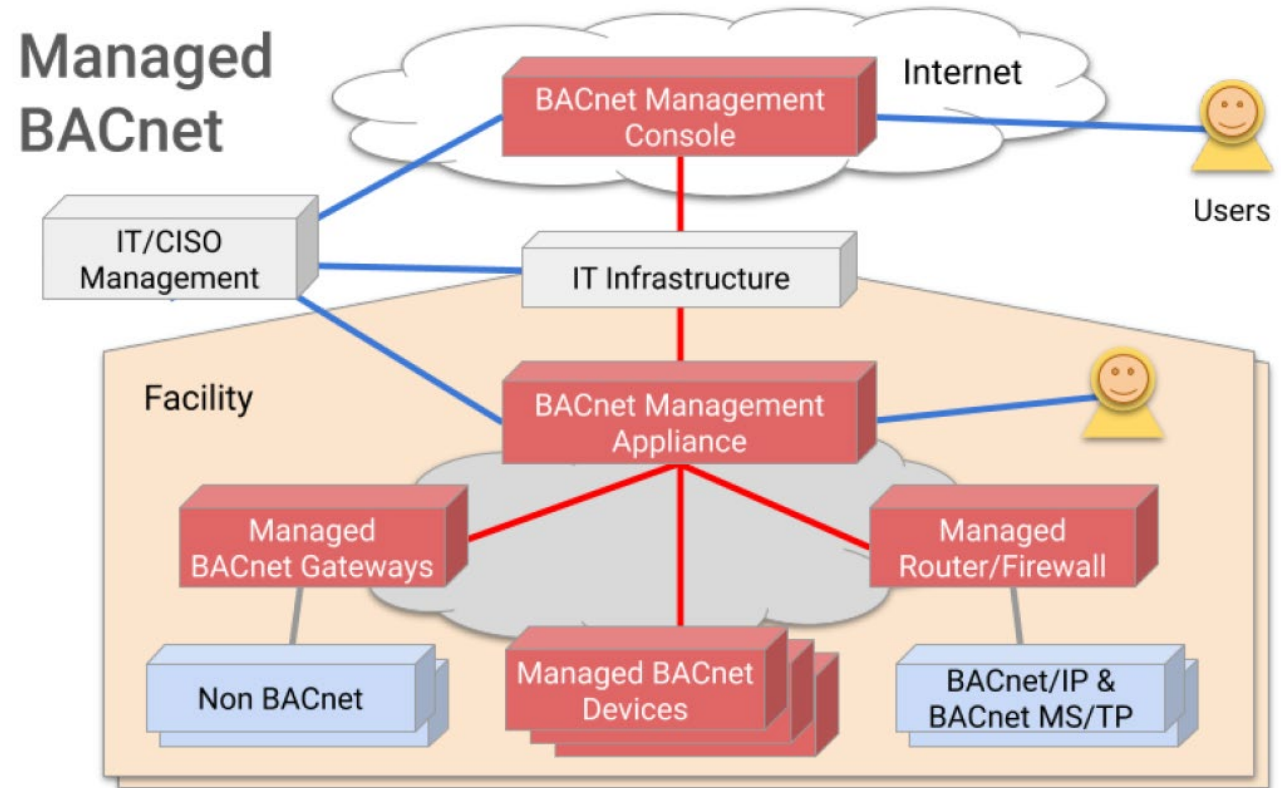


[BACnet Secure Connect Interoperability Acceleration Program \(bacnetinternational.org\)](http://bacnetinternational.org)



# Managed BACnet

- Industry-wide Interoperable Standard
- Resilient Framework
- Securely manage BAS/OT systems
- IT infrastructure and best practices
- Small single commercial buildings to multi-site global portfolios



Source: [Managedbacnet.org](http://Managedbacnet.org)

# Summary

- Modern Building Automation Systems present significant operational opportunity
- Additional risks due to evolving world
- Secure Product, Installation Practices, and Maintenance are required to mitigate risk
- Change is accelerating - teaming and clear ownership required







All trademarks referenced in this document are the trademarks of their respective owners.

© 2021 Trane. All Rights Reserved.

TRANE  
TECHNOLOGIES™