Building Automation Systems

Cybersecurity Best Practices & Lessons Learned

Kevin T. Smith

TRIDIUM

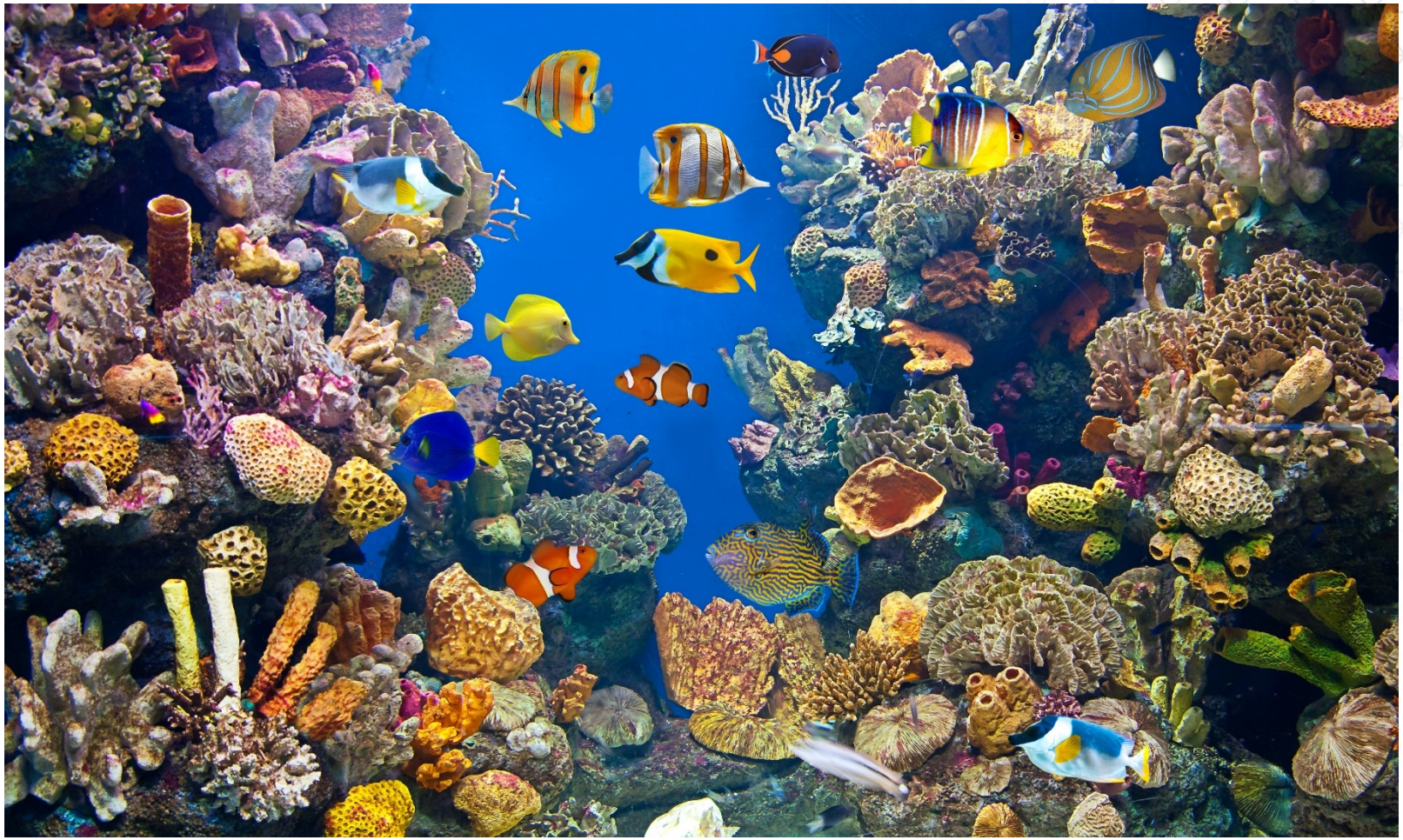
Who's Watching Your Building Now?

TRIDIUM

Recent (& Common) Building System Attacks

- **Ransomware & Malware Events**
  - Exploiting Email, Web Browsing Systems, USB
- **Insecure remote access**
  - Exploiting OT network to attack IT & other network(s)
  - DOS attacks on building system components
  - Exploiting unpatched systems
  - Changing control functionality
- **Self-Inflicted**
  - “Larry Code”
  - “Shadow OT/IT” exploited
  - System changes without testing

Every Device on Your Network Affects the Whole



TRIDIUM

An Organizational, Holistic View

Security Configuration of your network
(IT departments)

→ **Is Your Network Segmented with Defense-In-Depth Principles?**

Built-in capabilities of your connected products *(Vendor)*

→ **What are your connected products?** → **How Secure Are They?**

What ELSE is connected to your network?
(IT departments, End Users, "Shadow IT")

→ **And what are THEY connected to?**
(external connections, cloud services, other networks)

Configuration of your connected products
(Integrators, Administrators)

→ **How Cyber-Aware are your integrators?**

How Are Your Products Being Used?
(End Users)

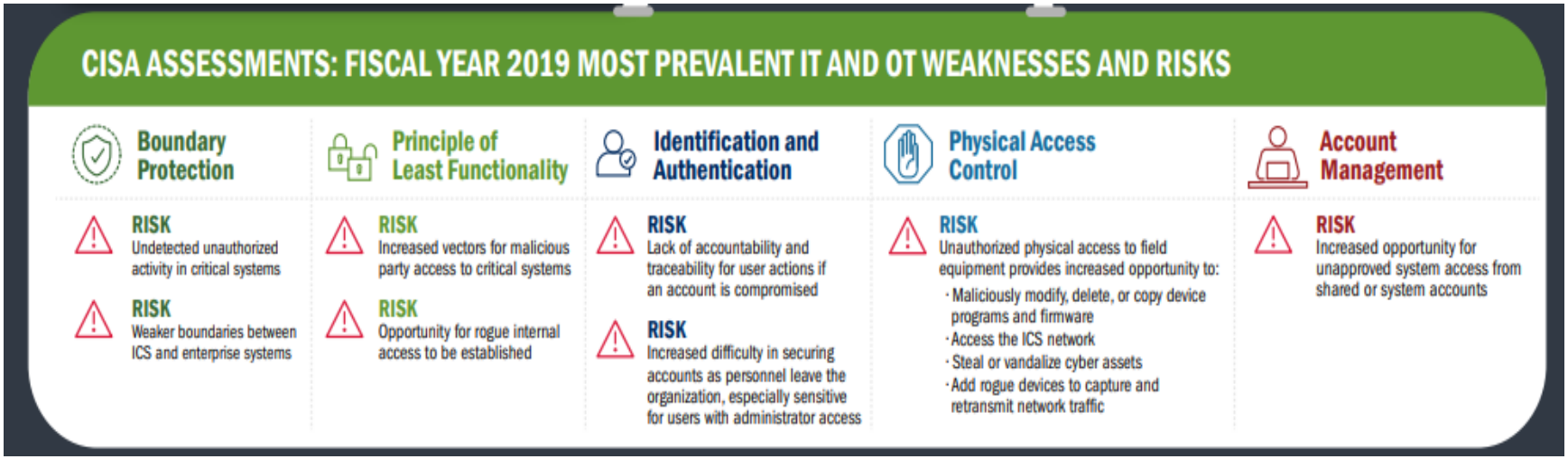
How Cyber-Aware are your end-users?

If you think *technology* can solve your security problems, then you don't understand the *problems* and you don't understand the *technology.* *-Bruce Schneier*

TRIDIUM

Best Practices

- Last month, CISA, the Department of Energy, and the UK's NCSC released "Cybersecurity Best Practices for Industrial Control Systems



Risk Management & Governance

- Understand Your Assets
- Understand Your Risks
- Understand Who Is Managing What!
- Periodic Risk Assessments
- Review ISA/IEC 62443 & NIST CSF for guidance on policies & procedures
- Federal Systems & Government Requirements for Risk Management Framework? Last month's Tridium talk

TRIDIUM

The Network

ICS NETWORK ARCHITECTURE

- Utilize segmentation of networks where possible.
- Implement a network topology for ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Use one-way communication diodes to prevent external access, whenever possible.
- Set up demilitarized zones (DMZ) to create a physical and logical subnetwork that acts as an intermediary for connected security devices to avoid exposure.
- Employ reliable and secure network protocols and services where feasible.

ICS NETWORK PERIMETER SECURITY

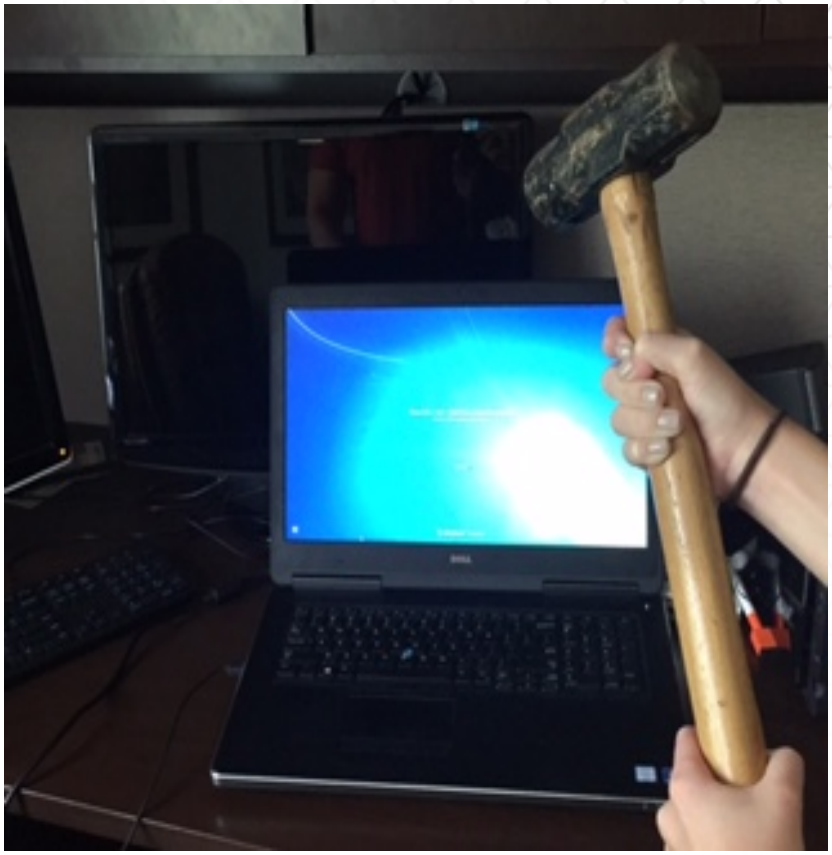
- Configure firewalls to control traffic between the ICS network and corporate IT network.
- Utilize IP geo-blocking as appropriate.
- Harden the remote access process to reduce risk to an acceptable level.
- Use jump servers as a central authorization location between ICS network security zones.
- Do not allow remote persistent vendor or employee connection to the control network.
- Catalog and monitor all remote connections to the network.

TRIDIUM

Physical Security

PHYSICAL SECURITY

- Lock down field electronics and set up alerting mechanisms for device manipulation such as power removal, device resets, and cabling changes.
- Ensure only authorized personnel have access to controlled spaces that house ICS equipment.
- Use multi-factor authentication, guards, and barriers to control logical and physical access to ICS equipment and facilities.



TRIDIUM

Due Diligence – Before You Buy

SUPPLY CHAIN MANAGEMENT

- Adjust ICS procurement process to weigh cybersecurity heavily as part of the scoring and evaluation methodology.
- Invest up front in secure ICS products, evaluating security against current and future threats over the projected product lifespan.
- Establish contractual agreements for all outsourced services that ensure: proper incident handling and reporting, security of interconnections, and remote access specifications and processes.
- Consider ICS information integrity, security, and confidentiality when contracting with a cloud service provider.
- Leverage test labs to test vendor-provided software for malicious code and defects before implementation.

TRIDIUM

Proactive & Active Management

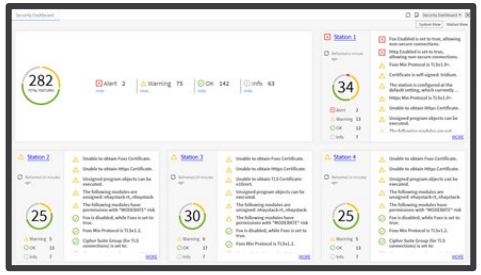
HOST SECURITY

- Promote a culture of patching and vulnerability management.
- Test all patches in off-line test environments before implementation.
- Implement application whitelisting on human machine interfaces.
- Harden field devices, including tablets and smart phones.
- Replace out-of-date software and hardware devices.
- Disable unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Implement and test system backups and recovery processes.
- Configure encryption and security for ICS protocols.

SECURITY MONITORING

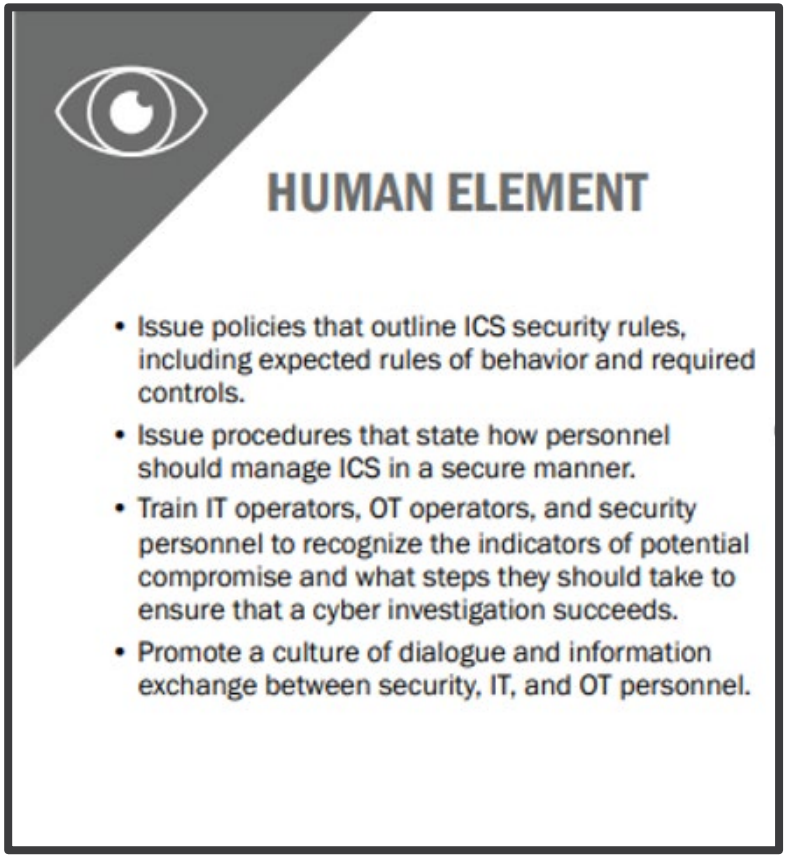
- Measure the baseline of normal operations and network traffic for ICS.
- Configure Intrusion Detection Systems (IDS) to create alarms for any ICS network traffic outside normal operations.
- Track and monitor audit trails on critical areas of ICS.
- Set up Security Incident and Event Monitoring (SIEM) to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts.

niagara4



TRIDIUM

People - The Biggest Risk



- Train People in Cybersecurity Processes (in every part of the business)
- OT & IT – Establish ground rules & culture of teamwork, understand responsibilities
- Building System Owners -
  - Make Sure those managing your building systems understand Best Cyber Practices
  - Contractually put in Cybersecurity Requirements - Ex: Ask To See Security Dashboard for Security Posture, Require Third Party Risk Assessment after Installation

TRIDIUM

Capabilities & Controls in Niagara

Security Processes

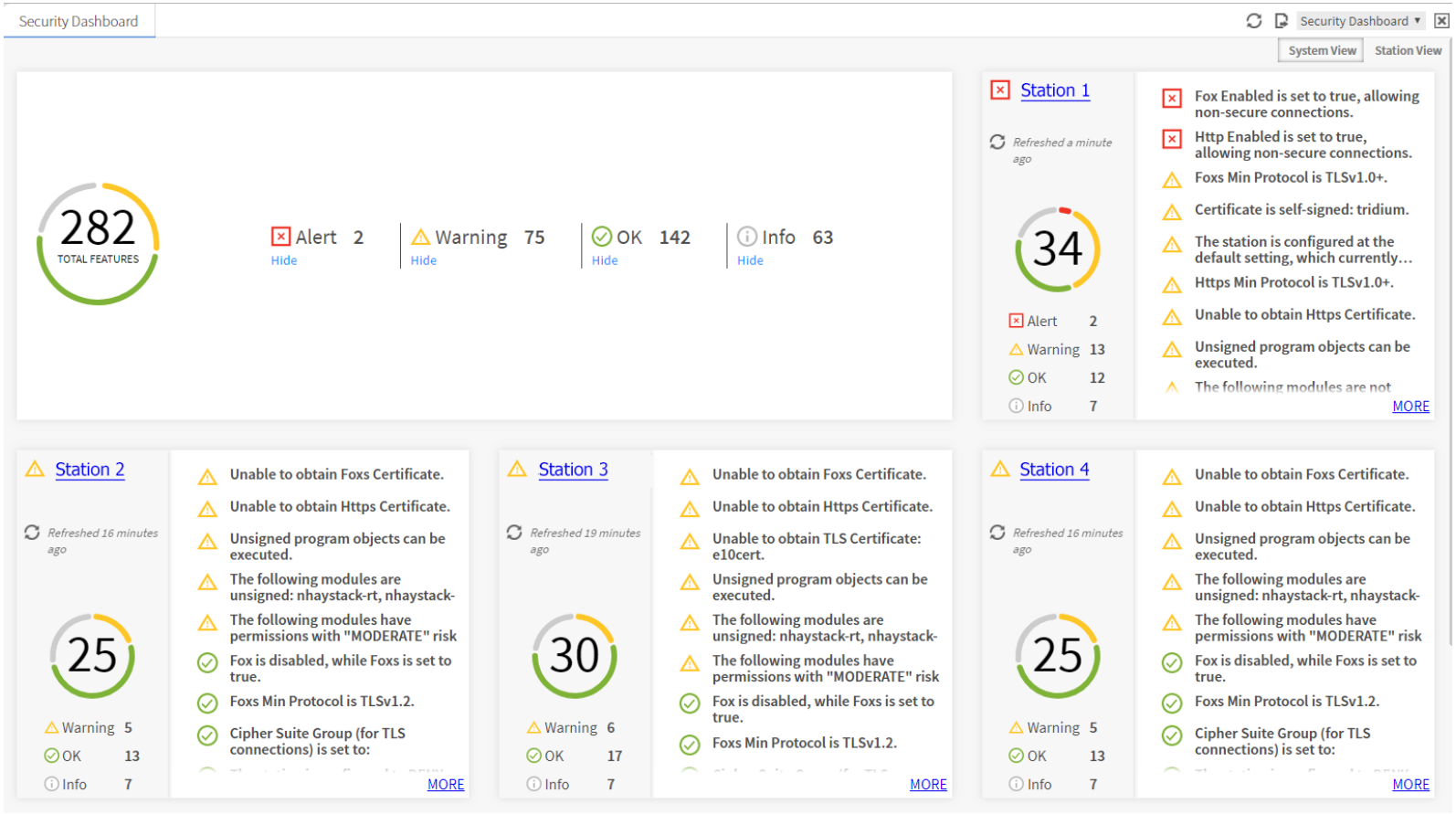
Tridium's Security Processes at a Glance

Security Requirements	Based on ISA 62443-3-3 Security Level 4 for Critical Infrastructure - Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
Internal Reviews by Tridium's Product Security Team	• Security Design Reviews, Security Code Reviews • Security Threat Modeling • Automated Security Tests for ISA 62443-3-3 Security Requirements • Reviews for vulnerabilities in third party libraries • Static Code Analysis and Binary Code Analysis • Risks managed in Risk Register according to CVSS Score
Reviews by External Teams	• Routine and Periodic Robust Security Testing by External Organizations on new and existing releases – partnering with commercial and government entities, throughout the year • Penetration Testing, Abuse Case Testing, Security Code Reviews
Reviews by Internal Security Auditor, CTO, and CCB approval	• 5 Phase Process, where all security artifacts from above are reviewed, and must have CTO signoff before Tridium CCB meets to vote on each phase
Risk Management Process with Deadlines on mitigating all found threats	• All known security vulnerabilities have visibility at the highest level, with 30-day, 60-day, 90-day, 120-day requirements for mitigation based on CVSS Score
Product Security Incident Response Team	• Robust process for investigating vulnerabilities, mitigating threats, and communication response. • Work closely with US Government re: Advisories
Support	• Routinely patch potential vulnerabilities, release security update builds, and send communications to the Niagara community

niagara4 Security capabilities

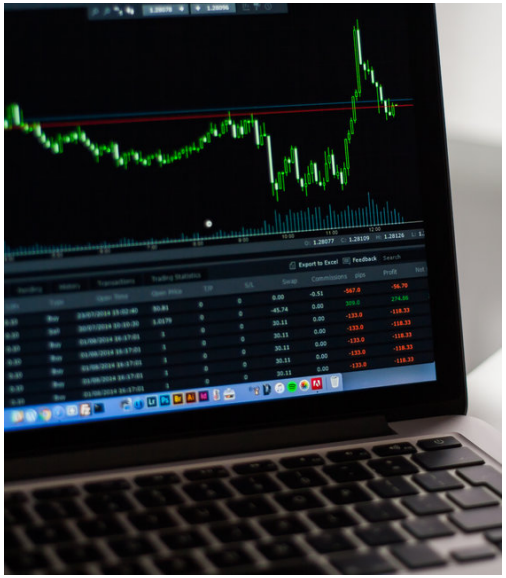
Authentication	Pluggable schemes provide flexibility;defaults are the most secure; Multi-Factor Authentication (MFA) now an option with Google 2 Factor Authentication; Niagara 4.8 includes digital certificate authentication (Kiosk Mode) & 802.1x device network authentication
Identity infrastructure and PKI integration	Can integrate with any PKI infrastructure,LDAP directories, Kerberos, and SAML 2 Identity Providers for Single Sign-On; Niagara 4.8 also includes 802.1x device authentication to the network; 4.9 includes SAML IDP integrated with Niagara
Role-Based Access Control	Provides access control for users by security role
Encryption of all communications	All communications encrypted by default
Encryption at rest	Sensitive data is encrypted on disk
Digitally signed code,validated at run-time	Assures that core framework code can't be altered or manipulated;
Hardware Security: JACE-8000 Secure Boot & HSM	Hardware root-of-trust; Only boots our digitally-signed trusted software, providing assurance against alteration; Also, Hardware Security Module provides hardware protection of private key for device authentication
Common-sense user account management	Configurable security mechanisms for attack prevention (lockouts, password strengths, etc.)
Authorization of Third Party Code	Controls what individual software components can do In 4.9, we require 3rd party module signing by default & provide visibility to administrator
Auditing of all user activity	User access is logged to customized levels New for 4.9! Enhanced Security Audit Log & security facets
Security Situational Awareness	Niagara 4.8+ Security Dashboard provides an actional view into security posture of your systems & other connected Niagara systems on your network

Security Dashboard in Niagara 4.8 (and Beyond)



Providing an Instant View of the Security Posture of Your Stations … so that you can adjust your settings for the best security.

Our “Secure by Default” principle



1. Make security easier: default to the most secure configurations
   - All transmissions encrypted
   - Users forced to have strong password strengths
   - Users set up with the strongest authentication mechanism
   - User lockouts upon consecutive bad log-ins
2. Force administrators to do the right thing
   - Factory default password must be changed after commissioning
3. Do the right thing, regardless of configuration
   - Encrypt sensitive information at rest
   - Digitally Signed Code: validated at run-time
   - JACE-8000 Secure Boot: trusted software validated at boot-time
4. Provide stronger configuration options based on best practices
   - Articles, documentation, TridiumTalks provide detailed guidance

We provide strong security capabilities – but it is important for our our partners and customers to configure and manage Niagara correctly!

TRIDIUM

Tridium Resources

- Niagara Hardening Guides
  http://www.tridium.com/en/resources/library

- Tech Bulletins
  - https://docs.niagara-community.com/category/tech_bull
- Niagara 4 documentation
  - Station Security Guide (ships with Niagara)

- "Meeting Government Security Requirements with the Niagara Framework" ", Tridium Talk, May 2020
- "After the Breach – How Can My Building Recover from a Cyberattack?", New Deal for Buildings Article, January 2020.
- Tridium White Paper, Cybersecurity and the IoT – Threats, Best Practices, and Lessons Learned, 2019.
- "Do You Know Your Building Automation System Cybersecurity Risks?", FacilitiesNet, November 2019.
- "Reduce the Cyber Risks to Your Buildings". AutomatedBuildings.com, September 2019.
- "Cybersecurity Considerations in Smart Buildings" (video), August 2019.
- "Towards a Cybersecurity Partnership in Connected Buildings", Realcomm, February 2019.
- "Harden Your Buildings Against Cyber Threats" (video), October 2018.

white paper

Cybersecurity and the IoT—Threats, Best Practices and Lessons Learned

Kevin T. Smith, Chief Technology Officer, Tridium

The market for the Internet of Things (IoT) is continuing to grow at a phenomenal pace. According to a 2018 report from the analyst firm GlobalData, the global IoT market has reached $130 billion and is predicted to rise to $318 billion in 2023.[1] IHS Markit forecasts that the IoT market will grow from what was an installed base of 15.4 billion devices in 2015 to 75.4 billion devices in 2025.[2] Other market research firms are releasing similar staggering statistics, and while estimates vary, all parties agree: network-connected devices and their capabilities are and will continue to be a disruptive force in the way that everyone does business.

Adding network connectivity to any "thing" can certainly provide great value, but it also brings along with this connectivity potential risks related to network security

But over 15 years ago—long before anyone had ever heard of the IoT—Tridium developed the Niagara Framework, a general-purpose, open and extensible software framework built for the purpose of connecting, managing and controlling any device over computer networks. A general-purpose IoT framework that allows integrators to connect and control devices, regardless of protocol and manufacturer, Niagara has changed the way that organizations do business, putting the "smarts" in smart buildings and data centers, providing significant cost savings and capabilities. Over the years, this experience has given us much insight into the areas of device connectivity and control, automation, analytics and cybersecurity.

Cybersecurity should be a concern for any user or owner of connected devices. In our fast-paced world of ever-changing technology, the cyber threat landscape continues to evolve at an alarming rate. With recent cybersecurity incidents showing unprecedented growth in the frequency, scale and sophistication of advanced cyberattacks, combined with the number of high-profile data breaches and hacks hitting the front pages of newspapers on an almost weekly basis, it should not be a surprise that most organizations are taking a newfound interest in protecting the systems on their networks.

Regarding the IoT, adding network connectivity to any "thing" can certainly provide great value, but it also brings along with this connectivity potential risks related to network security. In the past few years, we have seen web cameras, baby monitors, smart refrigerators and even cars electronically hacked. We have seen an alarming rise in data breaches costing organizations billions of dollars. We have seen the rise of security and privacy concerns related to smart devices. We have seen an alarming rise in malware threats infecting computers and smart devices. We have seen the increase of hacker-friendly tools and websites that allow

[1] https://www.itwire.com/internet-of-things/85332-iot-technology-exploding-with-govt,-utilities,-manufacturing-dominating-market.html
[2] https://www.ihs.com/info/0416/internet-of-things.html

TRIDIUM

TRIDIUM

External Resources

Resources	Where to find it
US Cybersecurity & Infrastructure Security Agency	http://www.cisa.gov/
"Cybersecurity Best Practices for Control Systems" - CISA, US Department of Energy, and the UK's National Cyber Security Center (NCSC) - May 22, 2020	https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems
NIST Cybersecurity Framework (CSF)	http://www.nist.gov/cyberframework
"NIST Cybersecurity Framework and Building Automation Systems (BAS)" - Jan 2020	https://newdeal.blog/nist-cybersecurity-framework-and-bas-white-paper-fc5ff3b83542
NIST SP 800-82: *Guide to Industrial Control Systems (ICS) Security* NIST SP 800-61: *Computer Incident Security Handling Guide* *NISTIR 8228 – "Considerations for Managing IoT Cybersecurity & Privacy"*	Found in http://www.nist.gov/
United Facilities Criteria (UFC) 4-010-06	https://www.acq.osd.mil/eie/Downloads/IE/UFC_4_010_06.pdf
US CERT – *"Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies"*	https://www.us-cert.gov/ics/Recommended-Practices
Fred Gordy's May 2020 Building Cybersecurity Articles	Send him a LinkedIn Request