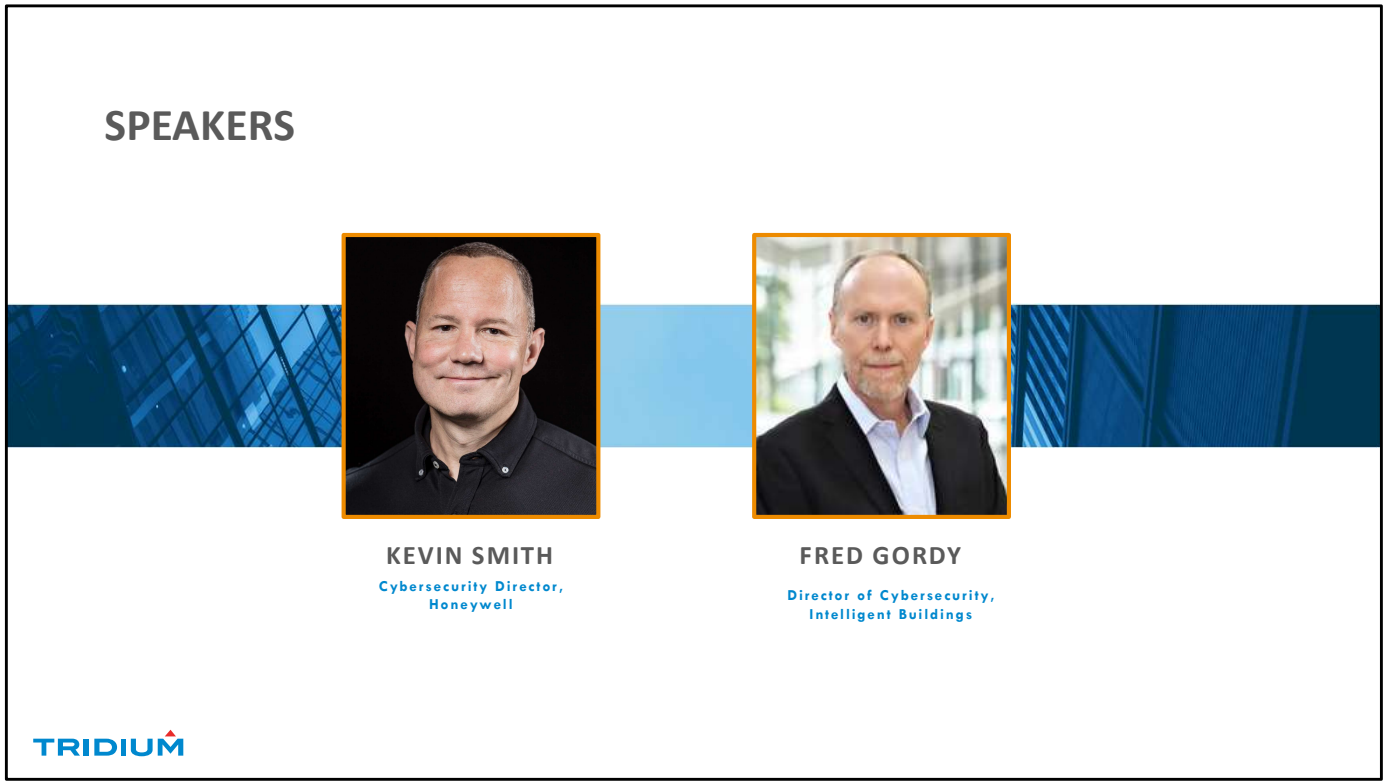

TRIDIUM talk
SPECIFIER SERIES
TRIDIUM

Good afternoon, and thank you for joining us today for our third webinar in the **TridiumTalk: Specifier Series**, "***Writing Cybersecure Specifications for Buildings: What You Need to Know***"

All of our events are recorded, so if you want to go back to hear our prior ***Niagara 101 for Specifiers*** or the ***Crafting Powerful Niagara Specifications*** sessions, you can easily have them replay from our website.

Today we are diving in more specifically on the subject of cybersecurity. I have the honor of introducing two industry leaders who are going to talk to you from their relative positions on this subject.



Thanks, Michael! As he just shared, I'm Kevin Smith – and unless you're new to the Niagara Community, you've probably seen my face before – I've been in the Tridium family for over 8 years now – I was originally hired to focus on cybersecurity of the Niagara Framework as we moved from Niagara AX to N4 – now almost a decade ago, and building in strong cybersecurity capabilities into Niagara and the JACE 8000 – I later became the CTO of Tridium, and then briefly the CPO, but I'm really more of a cybersecurity geek, so now I spend most of my time focusing on Cybersecurity for all of Honeywell.

Fred Gordy from Intelligent Buildings is no stranger to the Niagara community, either. I remember first seeing him at a Niagara Summit just about 8 years ago speaking on cybersecurity He has a long history in the building automation community, and I see him as one of the leading industry spokespeople for cybersecurity in smart buildings. Someone on LinkedIn recently paraphrased Jack Nicholson in the movie "A Few Good Men" about Fred saying "Way down deep inside, we want you on that wall, and we need you on that wall" educating us about cybersecurity and smart buildings. And I found that both funny and true.

Usually when I meet up with Fred, we usually exchange stories about cyberattacks that we've seen in the industry, how they happen, and how they could have been prevented. So I'm going to give a little bit of an introduction to this talk, Fred is going to talk about what he sees about the state of the industry today, what needs to happen, and then we're going to talk about what you can do as a specifier to make sure you put the right cyber

requirements in a spec, because it is incredibly important.

ARE WE NOW "NUMB" TO CYBERATTACK HEADLINES?

TRIDIUM

Forgive me for putting this picture on this slide – it's the ubiquitous "hacker" picture that you see often in the news media – he's got a hoodie, and it looks like he's reaching out through the Matrix to hack all your stuff. We see this picture a lot, and we see it a lot because it seems like every week, a new security breach, or new cyber attack, or new ransomware attack hits the headlines. And I feel like we see the headlines so much, we've become numb to it.

But it is true – certainly, we see more headlines on the IT (Information Technology) side than we do on the OT (Operational Technology) side, but we're starting to see those headlines more and more too. But for the most part, for buildings, organizations have typically tried to stay out of the press and the public eye, which may actually give us a false sense of security – thinking that everything's fine.

But the state of the industry is actually not fine – when I have my Tridium hat on, I get customers that reach out to me about attacks they've experienced - I've heard about customers where it took 6-8 months to recover from a cyberattack on their building networks. I've even heard stories where attackers breached physical security to perform attacks on JACES and supervisors.

And customers who’ve experienced those incidents take cybersecurity far more seriously than they did before and now realize that cybersecurity has to be a true partnership – with many stakeholders. It’s complex because in a building – you have lots of different types of roles. You have the building owner who owns assets. You have tenants who own assets. You have an IT department. You have facilities departments. You have contractors and integrators. And you have users. And they all have a role to play.

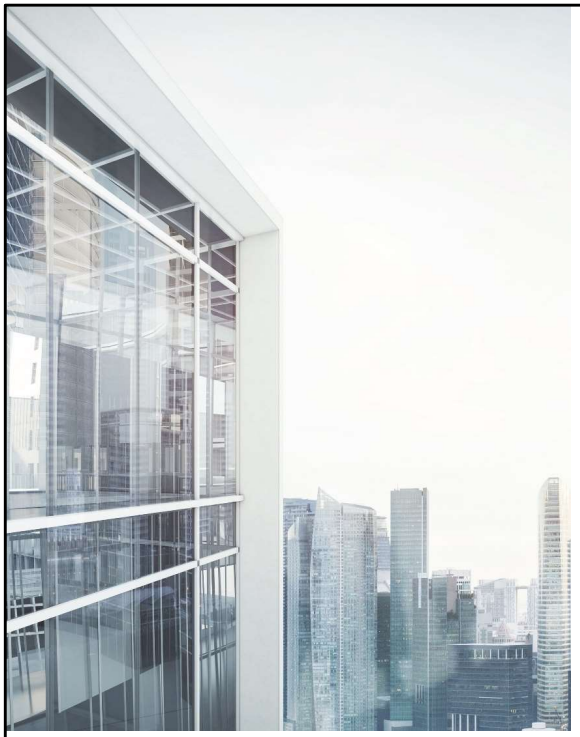
And you have to think about this when you’re writing specifications. And hopefully you got a chance to see Ed Merwin’s Tridium talk last week – “Crafting Powerful Niagara Specifications” – where he touched on this. Certainly, the specifier will own writing the spec, but it involves active input from a lot of stakeholders. It involves guidance on the products you’re going to bring in, how you bring them in, and it involves how things are going to be executed.

- For your buildings, you need strong cybersecurity standards for the products you bring in, and some of these may be dictated by organizational or local policy, rules, regulations that you have to adhere to, and involves a conversation with the key stakeholders – and most likely the building owner – or the building owner’s representative about the level of risk you’ll need to accept.
- You need to make sure that the vendors of any products you’re going to integrate with have strong cybersecurity capabilities, provide guidance on how to configure them securely, & you need to make sure vendors actually patch vulnerabilities in their products regularly.
- The systems in the building are going to have to be actively managed and watched & so there are going to be requirements about configuring audit logs & security visibility into your systems. .
- You’ll need requirements for your systems integrators in how they set up systems & rules for your contractors. And you’ll need requirements for the hand-offs and training.

So this is what the specifier needs to think about, and as this slide says, it’s complex, because a lot of people are involved. But the good news is – if you plan for that complexity, you’ll be in good shape.

So now I’m going to pass it to Fred - He’s going to go into some stats & real-world examples, and he’s going to talk about what’s needed in our industry. And then I’ll be back and I’ll talk about some of the specific requirements that you’ll have to think about .

- 2020 to 2021 attacks increased by 600%
- Ransomware is almost 100% avoidable (root cause – user misuse of application host)
- Unknown/undocumented network architecture allows the bad guy to “hang out” on the OT network and look for openings to the corporate network (Colonial Pipeline)
- Attacks on equipment are on the rise
- Killware is a new term coined by DHS head Alejandro Mayorkas (Oldsmar and San Fran – deaths have been attributed to Killware)



ATTACK EXAMPLES

92 DAYS TO RECOVER

- RAT allowed attackers to damage VFDs and Pumps
- Bricked controllers
- Chillers had to be inspected

RUSSIAN BASED MALWARE

- Malware released locally
- Damage to workstations
- No viable forensic data

CRYPTO MINING

- Building system PC running mining software
- Unknown length of time
- No viable forensic data

FORMER VENDOR EMPLOYEE WRECKS MULTIPLE DEVICES

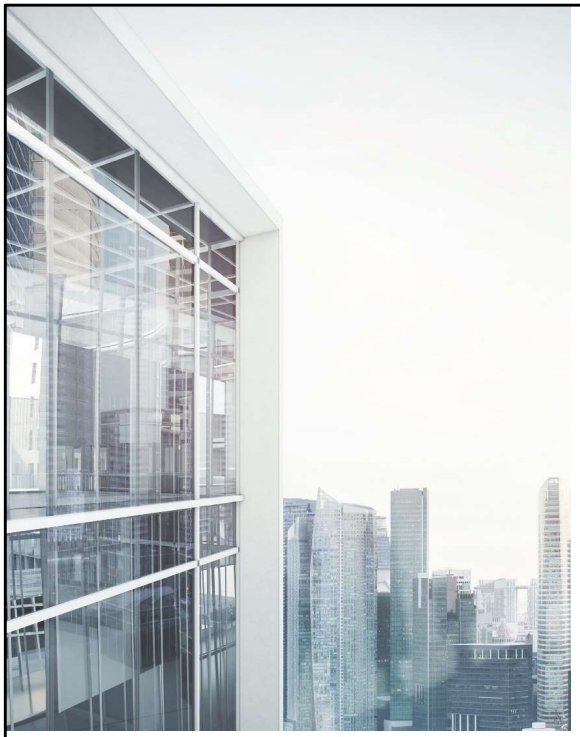
- TeamViewer installed by the vendor
- Single username and password
- Intimate knowledge of system

REMOTE MESSAGE EMPTIES BUILDING

- Exposed printer outputted “There is a bomb in the building
- Two hours before it was reported
- Tenant and productivity loss

TRIDIUM


LACK OF UNDERSTANDING
Implementing IT tools have caused almost 40% of system downtime
Some events have cost seven figures to rectify
VULVERABILITY MONITORING
50%
PATCH/UPDATE
40%
USER MANAGEMENT
5%
INTERVENTION
5%
TRIDIUM



ERROR EXAMPLES

SECURE AREA OPEN TO THE GENERAL PUBLIC

- RAT allowed attackers to damage VFDs and Pumps
- Bricked controllers
- Chillers had to be inspected

VULNERABILITY SCAN KNOCKS OVER 6.000 DEVICES

- Malware released locally
- Damage to workstations
- No viable forensic data

SOFTWARE PATCH CANCELS SURGERIES

- Building system PC running mining software
- Unknown length of time
- No viable forensic data

USER REMOVED DISCONNECTS NUMEROUS SITES

- Exposed printer outputted “There is a bomb in the building
- Two hours before it was reported
- Tenant and productivity loss

TRIDIUM

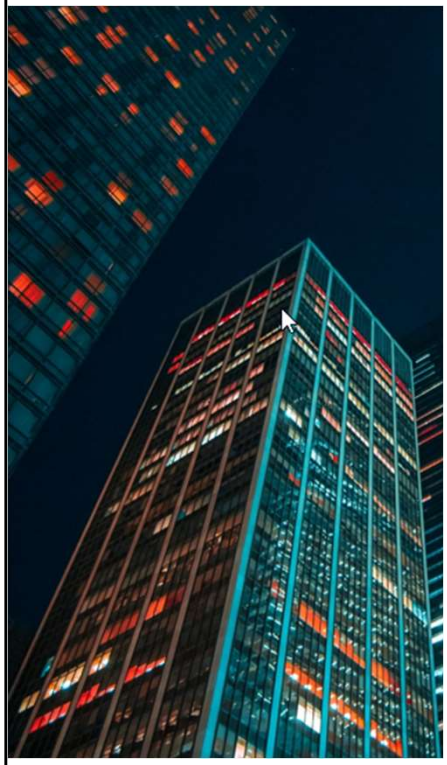

HOW DO WE FIX THIS?
TRIDIUM

Ask yourselves six questions. Answer NO to ANY of them, you don't have the fundamentals of building control cybersecurity.

TRIDIUM

- **Do I have a building control system cybersecurity program (governance, policies, roles & responsibilities)?**
- **Are all the devices and software that run my building(s) accounted for in an up-to-date asset inventory program?**
- **Do I have a complete, up-to-date list of each service provider that supports the systems within my buildings?**
- **Who controls access to my building control networks locally and remotely?**
- **Are all building control networks documented?**
- **Are all building control systems, including the devices throughout the building, accurately and consistently backed up?**

BCS/ISA 62443 RESPONSIBILITY MATRIX



Delegates Responsibilities

Selects Products

BUILDING OWNER/MANAGER

Examples:
- Building Owner
- Asset Manager
- Property Managers
- Corp IT

SERVICE PROVIDER

Examples:
- System Integrators
- Maintenance Support
- Network Manager

PRODUCT/TECHNOLOGY SUPPLIER

Examples:
- Building Automation Suppliers
- Control System Suppliers
- Building Technology Suppliers

Provides Services

Provides Products

62443-2-1	62443-3-2	62443-2-4	62443-3-3
Security Program Requirements for BACS Asset Owners	Security Risk Assessment & System Design	Requirements for BACS Service Providers	System Security Requirements & Security Levels

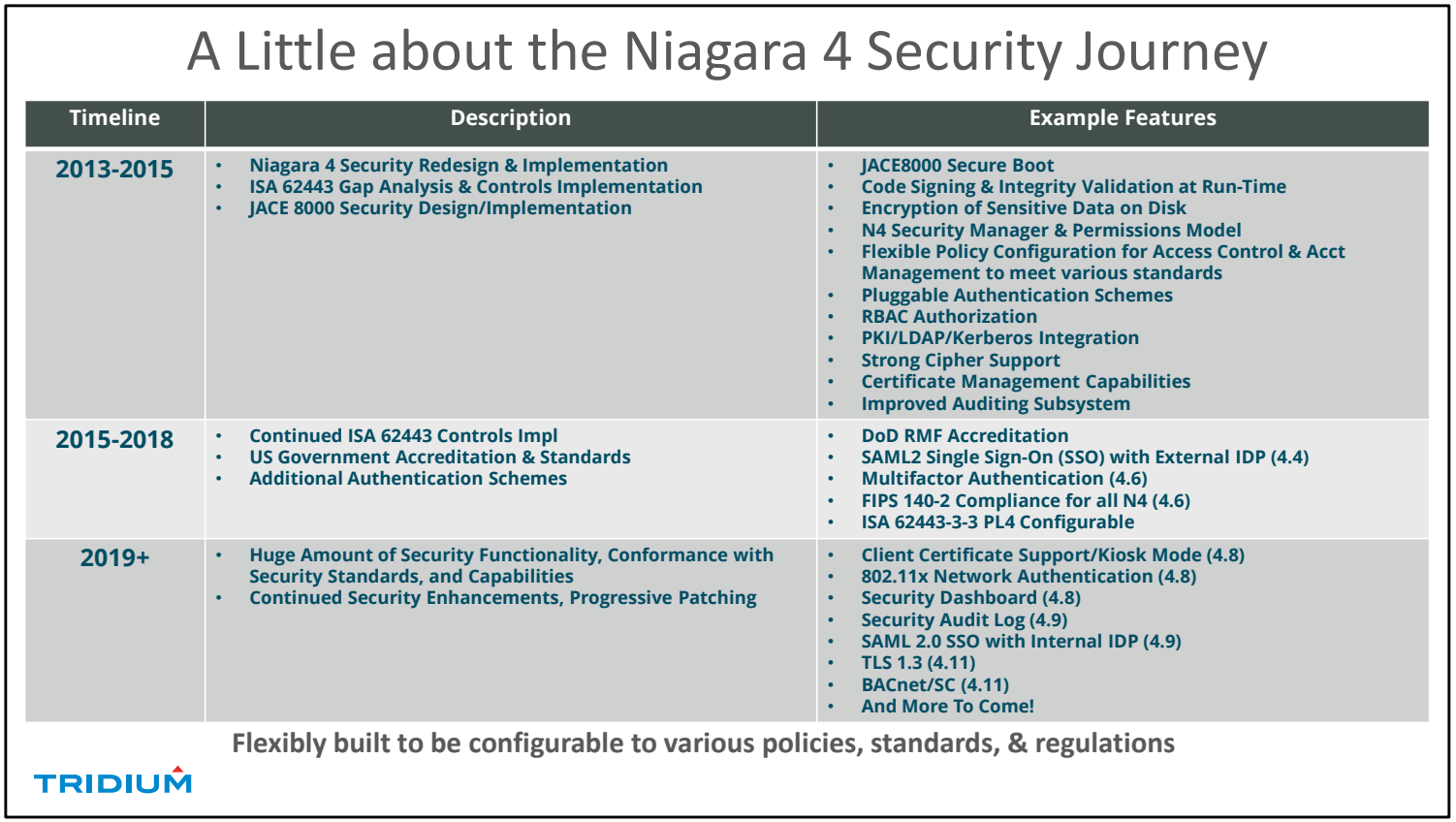
TRIDIUM

That slide that Fred just shared is really important for us to understand – all the roles that you have & the requirements based on how those groups are going to operate.

And as a specifier, you will have to understand the risk level of the organization – what "acceptable risk" is. This is going to help you narrow down various security requirements. The result of a risk assessment will show you, for example, that the security controls needed for a nuclear facility are going to be a lot different from the security controls needed for a school building. But understanding that is the result of having that risk conversation with the stakeholders. And also understanding the relevant security requirements from your domain. This will be different in the medical industry, the financial industry, and the US government, and they will most likely have standards you need to follow

Here's an example – within the DoD, there is a Unified Facilities Guide specification – for low and moderate impact facility control systems (this is according to that risk level I was talking about). It will have detailed requirements for setting up almost anything to be compliant to the DoD Risk Management Framework in those environments. For configuring our products, we have actually built the documentation that conforms with this spec – specific only to our product. But of course, you're going to have other products and other systems in that environment.

But the great thing about this is – depending on the industry that your building is in, any regulations & specs like this will make your life easier as a specifier – because you can really just refer to the spec. But of course, not all industries are like the DoD, so you may have to adopt some common-sense cybersecurity best practices to specify them. This is where working with security professionals & other stakeholders for the building will be helpful.
As specifier, it's critical that you pick products that are cybersecure and are compliant with the requirements that you'll need, and so I'll briefly discuss Tridium's journey related to this.



At Tridium, just about a decade ago, we looked to overhaul the cybersecurity posture of the Niagara Framework as we were planning the move from AX to N4, and as we were planning to release the JACE 8000. And so what we did at first is look at one of the security standards that Fred talked about – ISA 62443 – the gold standard of Industrial Control Systems security, and we asked – how can we meet those standards at the highest protection level?

Well, first of all, since Niagara is a framework & something that has to be configured out of the box, we had to change that question to "How can we make our product configurable to meet the security requirements of that standard?" So we did a gap analysis of what was possible with Niagara AX at the time, and what we needed to do to change. And we found a lot of gaps. And filling those gaps required a lot of work.

But the result of this journey for us is that our products not only meet this high standard, but along the way, customers from various industries with industry-specific security requirements asked us to include other options in order to be compliant. So security requirements specific to compliance in the Department of Defense, the healthcare and financial industries also became added to Niagara.

But what that means to you is – there are a lot of different options – and so as a specifier, you may have to specifically ask questions about *how* to configure Niagara – and of course, not just Niagara, but all of your security requirements.

Niagara Security Capabilities

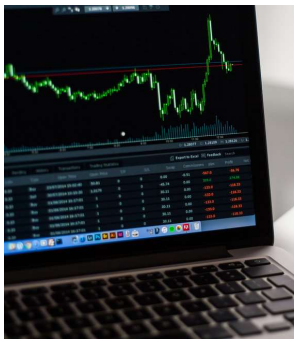
Authentication	Pluggable schemes provide flexibility; defaults are SCRAM-SHA; Multi-Factor Authentication (MFA); Digital certificate authentication (Kiosk Mode), 802.11x device network authentication, SAML 2 Single Sign-On, LDAP authentication, etc.
Identity infrastructure and PKI integration	Can integrate with any PKI infrastructure, LDAP directories, Kerberos, and SAML 2 Identity Providers for Single Sign-On; 802.11x device authentication to the network; SAML IDP integrated with Niagara
Role-Based Access Control	Provides access control for users by security role
Authorization at API level	Controls what individual software components can do
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; 3rd party module signing by default & provide visibility to administrator
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.)
Auditing of all user activity	User access is logged to customized levels Enhanced Security Audit Log & security facets
Security Situational Awareness	Security Dashboard provides an actional view into security posture of your systems & other connected Niagara systems on your network
Security Standards, Protocols, etc.	Integration: PKI, LDAP, Kerberos, SAML 2, BACnet/SC, Authentication: SCRAM-SHA (256/512 Bit Digest), WPA-PSK128, WPAPSK256, Google 2 Factor Auth, SAML 2.0; 802.11x Network Auth; Encryption Protocols: TLS 1.3/1.2; Encryption: AES GCM, AES 256 CBC, PBKDF2-HMAC-SHA256; Government Compliance: FIPS 140-2 Compliance, Federal Government DoD Risk Management Framework (RMF) Artifacts for Niagara4 available in SAFE

So for example – and I'm not going to read everything on this slide, but as a specifier, you can look at this slide & it will give you starting points in questions to ask. You're going to have to understand the risk level of the organization, and look at some of these rows, and you can ask questions like,

1. If you look at the first one - What should the authentication requirements be?
    - Highly-regulated industries with high risk levels might mandate Multi-Factor authentication.
    - A large company in the healthcare industry mandates 802.11x network authentication, so that every JACE has a digital certificate & must authenticate to their infrastructure before it gets an IP address – in that case, you'll have to specify that.
    - If it's a commercial building used for a large company, maybe it's – integrate with their Single-Sign-On infrastructure, or their LDAP infrastructure – something that's monitored.
    - Or they may be fine with the defaults (which is still SCRAM-SHA)

And you see the rest – and hopefully just looking at this slide will give you questions to ask as far as requirements. And when you look at things like "Role Based Access Control" on this slide, you should be thinking "What security roles should be set up for the systems in my building – what types of people should have what types of access?" These are really good conversation starters.

Niagara 4's 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 partners and customers to configure and manage Niagara correctly!

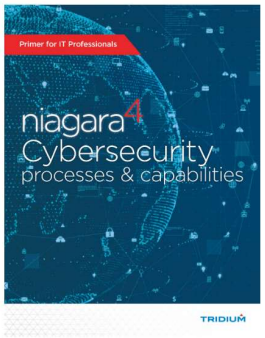
TRIDIUM

And that's not all. Because we know that integrators and contractors have to configure Niagara's security controls correctly, we designed Niagara 4 with the "Secure By Default" principle – we wanted to make it easy to configure Niagara securely, so we have all of our security configurations default to the most secure. So if someone accepts the defaults, it will be the most secure.

We also, with Niagara 4 introduced something that – at the time – nobody else did. At commissioning time, we force a strong password to be chosen, and it can't be the out-of-the-box default password. We also made certain things non-configurable so that operators and integrators wouldn't have an option – so things like validation of the software's integrity at run-time, sensitive data encrypted at rest, it was just done without operator involvement.

And we have embraced this since – and any capability we add, we still hold to this "secure by default philosophy"

Cybersecurity Documentation & Videos



Niagara Cybersecurity Processes & Capabilities

Niagara 4 Hardening Guide

Cybersecurity Best Practices TridiumTalk

White Paper - Cybersecurity and the IoT - Threats, Best Practices and Lessons Learned

BACnet Secure Connect & Niagara 4 Data Sheet

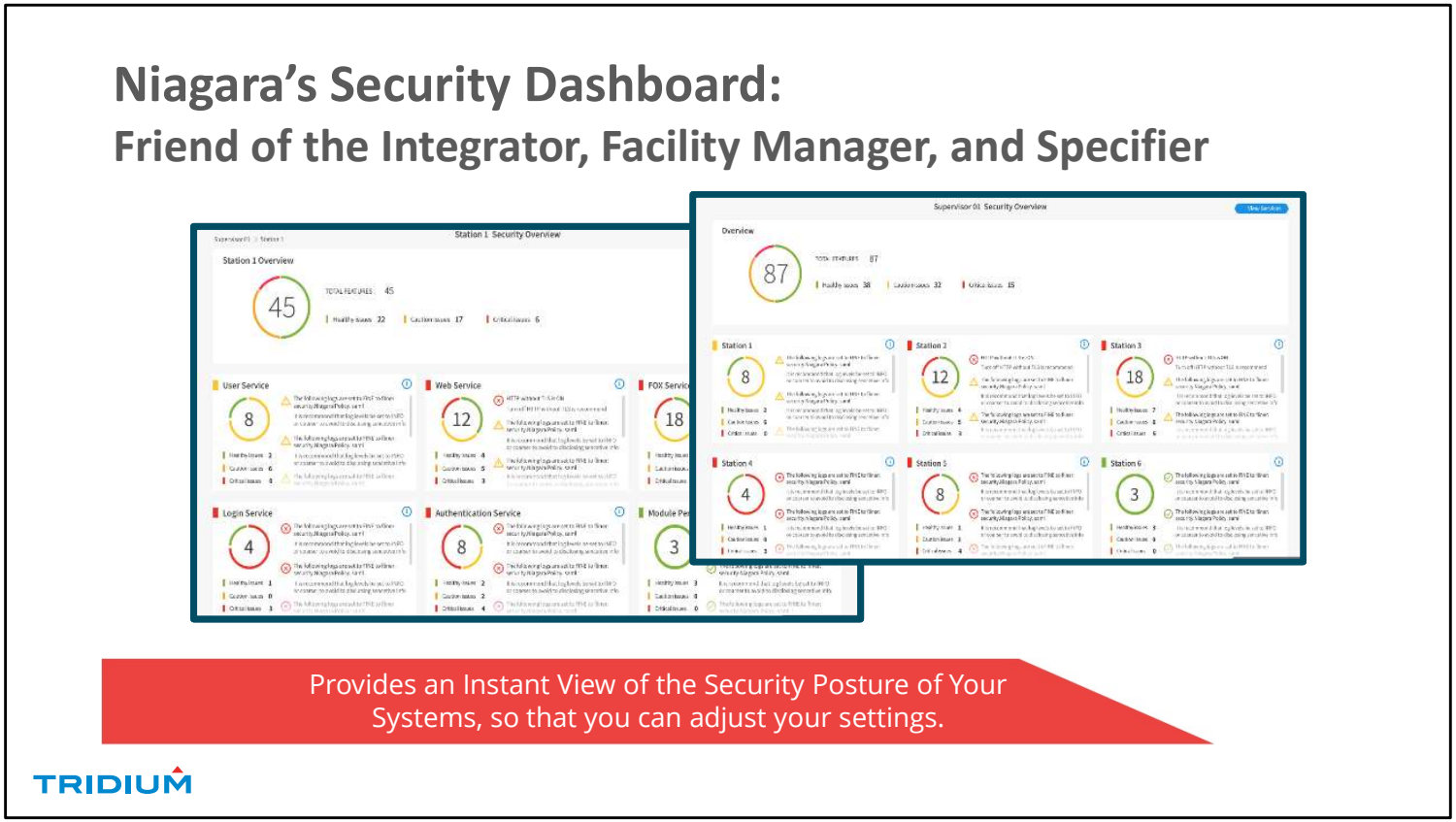
TRIDIUM

The other thing that we've done at Tridium – is try to educate our community on Cybersecurity. As you saw on the last few slides, we've built in lots of options, and there is a learning curve. Because of that, we have a lot of documentation and content. I'll call out a few in particular.

The first is the Niagara Hardening Guide – available on our web site. Ed Merwin used this as an example requirement in a specification that is useful. It is "Installation, set up and programming shall be in accordance with the latest revision of the Niagara Hardening Guide."

If you are specifying something for the US government, you probably want to see the youtube video on meeting cybersecurity requirements.

And Niagara supports Bacnet SecureConnect, which is the secure BACnet standard – and so as your specifying requirements for your building, this data sheet is going to be helpful to you. You can find them all on our web site or youtube channel.



Something that you will find useful as you write specifications can be found in the capabilities of Niagara's security dashboard.

Over the years, as we've been adding cyber capabilities to Niagara, we found that there is often a disconnect between what the Facility Manager (or Building Owner) thinks the security posture is – and what it actually is. We found this to also be the case with Niagara deployments. Meaning, someone builds the requirements for a job, an integrator comes in and does the job, but there was no EASY way for someone to check on the security posture of the Niagara deployment.

Certainly, you as a specifier should say that the configuration of Niagara shall conform to the Niagara hardening guide, but for someone to check compliance on that, it's a pretty tedious task.

So that's why we came up with the Security Dashboard and released it 4 years ago now – it shows you quickly how secure things are configured in all of the Niagara Systems on your network(using the colors red, yellow, and green), and gives you tips on how to fix them. This means that for a job, an integrator can use this to double-check his work to make sure the system is set up in a secure way. It also means that the facility manager can also demand a certain level of security, and check compliance with the dashboard. This is been so helpful for our community, we've even made it customizable, and we continue to make enhancements to it.

So – I really think that you should say that "For all Niagara Systems, the Security Dashboard shall be enabled." Depending on the level of acceptable risk, you might want to adjust how many red and yellow items there are, and specify that. That way, it will be easy to prove compliance at the end of the job.

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

TRIDIUM

Security processes are critical. When you are picking a vendor's product, certainly, you want to look at the security controls that it provides, but you also want to understand how they develop their product, test their product, and support their product.

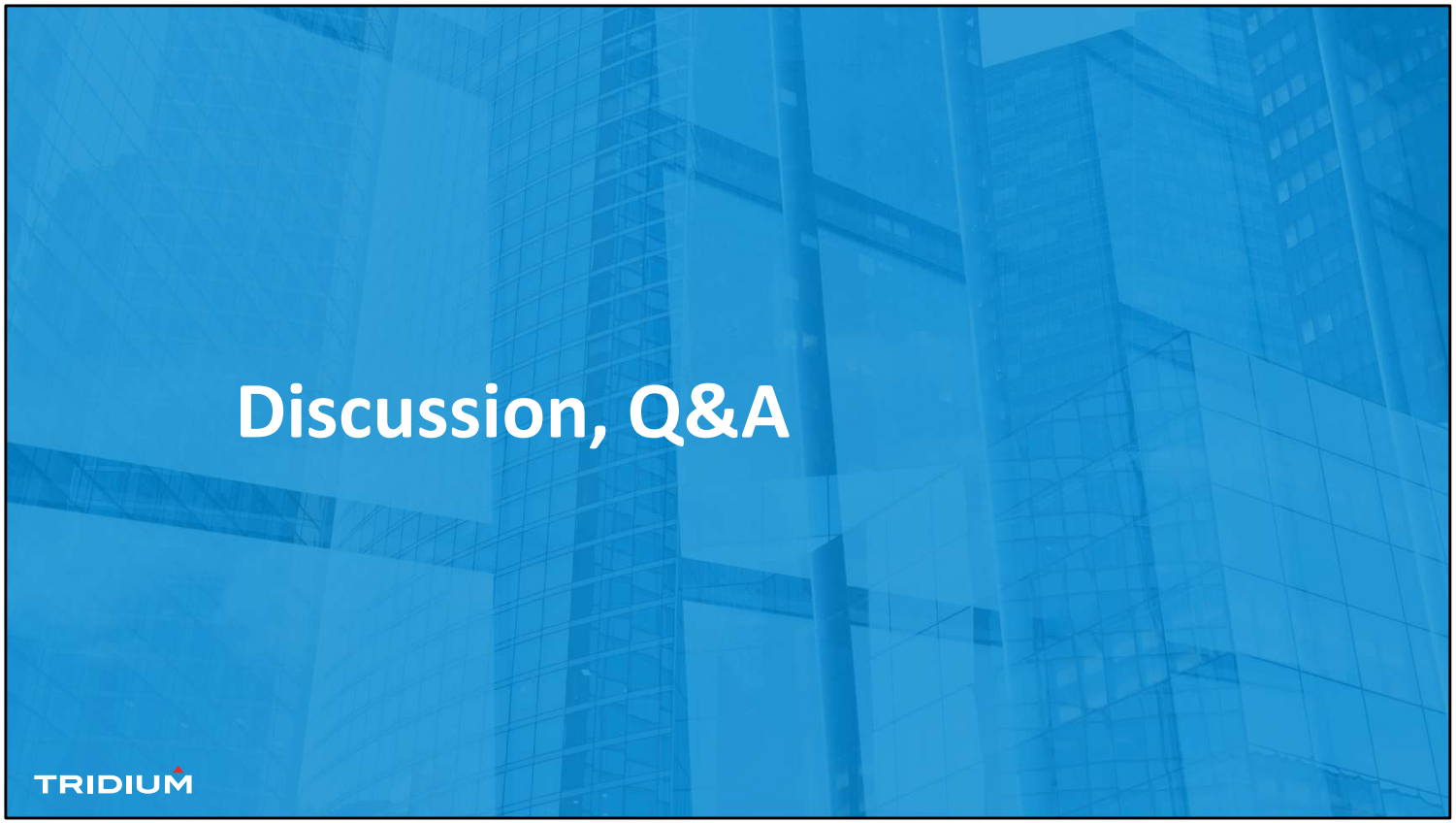
As a specifier, you may want to set standards for product vendors – they may need to provide a statement of how they will support their product and provide security updates, when they are found, at the very least.

Putting these all together (JUST an EXAMPLE)

Authentication	• "Niagara systems shall be configured to utilize the DigestScheme for authentication, in accordance with the latest Niagara 4 Hardening Guide" (Org-specific? May need to integrate with SSO or LDAP infrastructure, 802.11x, etc.)
Role-Based Access Control	• "Users will be assigned to Roles mapped to the appropriate permissions in the following categories: Admin, SignageReadOnly, LightingReadOnly, LightingControl, HVACControl, HVACReadOnly, ViewOnly.." (Work with stakeholders to define these roles – the more specific, the better!)
Security Standards, Protocols, etc.	• "All web-based or FOX-based transmissions between all systems shall be configured to use, at the very minimum, the TLS 1.2 protocol" • (For DoD)- All products shall be configured to support the Unified Facilities Guide Specification (Cybersecurity for Facility-Related Control Systems) May 2021"
Account Management	• Account management shall be configured according to "Station Account Management" & "Platform Account Management" sections of the latest version of the Niagara Hardening Guide." • "Concurrent login sessions shall be disabled." • "A super-user account (not named admin) shall be created, and the known admin account shall be disabled." • "Configure unique credentials for up to 25 users with the relevant roles and permissions provided by the owner" • "All account names, passwords, and passphrases for all systems shall be provided to the system owner upon the completion of the project"
Auditing of all user activity	• "Niagara shall be configured to generate alarms when an audit log reaches capacity and when audit processing failure occurs"
Security Situational Awareness	• "Niagara Security dashboard shall be enabled for all Niagara systems, and the security of all Niagara systems shall configured in such a way that no RED (insecure) items are shown."
Security Supported Products	• "Vendors of all products selected must have a process for security vulnerability mitigation & have documentation showing that they will release periodic security updates.."

So how do we bring this all together?

It can be a complex process that involves stakeholders, which means that for a successful specification, you're going to need to do some research and are going to have to have conversations with stakeholders. You may need to work with a security architect & you're definitely going to have to understand the risk level of the organization.. Here, I've thrown together just a few examples of things that might be in your specifications, and they may not apply to all systems.


Discussion, Q&A
TRIDIUM

Specification Resource – Cyber Security Dashboard

After determining the security requirements as described before (and in 62443), you can insert those into your cyber specification verbiage

The Niagara Security Dashboard can be used to monitor the system and validate compliance for operation. The spec language below should be modified with any specific details from your findings that are appropriate to your project

Niagara Cyber Security Dashboard Guide Specification

Implement a Niagara Security Dashboard as a centralized, easy-to-read and actionable view on the security posture of the entire Niagara infrastructure. The dashboard shall provide visual alerts in the event that any Niagara station in your network is set to allow non-secure connections. It shall display the status of required certificates for each station and shall identify whether running software modules and program objects are signed by their developers. Cyber dashboard shall present all the potential cyber issues at a glance and user shall be able to remediate them quickly for the protection of the Niagara network.

The Station View shall show individual services including User Service, Fox Service, Web Service, Login Service, Authentication Service, and Module Permissions. The Supervisor view shall show all JACEs on the Niagara network, so Niagara users can quickly identify issues and triage outliers.

Resources and Links

Tridium Website https://www.tridium.com/us/en

Intelligent Buildings https://www.intelligentbuildings.com/

Tridium Cybersecurity Page https://www.tridium.com/us/en/Products/niagara-cyber-defense

NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

IEC 62443 https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Page for Specifying Engineers https://www.tridium.com/us/en/Learn/by-role/specifying-engineer

Page for Cybersecurity Personnel https://www.tridium.com/us/en/Learn/by-role/cybersecurity

Search prior TridiumTalks on Cybersecurity https://www.tridium.com/us/en/services-support/events

Building Cyber Security https://buildingcybersecurity.org/

TRIDIUM

Resources and Links … *continued*

Edge10 https://www.tridium.com/us/en/Products/niagara/edge10

Niagara Analytics https://www.tridium.com/us/en/Products/niagara-analytics

Enterprise Security https://www.tridium.com/us/en/Products/niagara-enterprise-security

Niagara Drivers https://www.tridium.com/us/en/Products/niagara-drivers

Tridium University https://www.tridium.com/us/en/services-support/tridium-university

Marketplace https://www.tridium.com/us/en/services-support/niagara-marketplace

Pro Services https://www.tridium.com/us/en/services-support/professional-services

TRIDIUM