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.

bad actors to search for, discover and exploit Internet-connected devices. Specific to the IoT market, we saw the largest distributed denial-of-service attack of its kind in October 2016, when an estimated hundreds of thousands of IoT devices were attacked, infected with a virus and used in a coordinated effort to attack domain name system (DNS) servers, effectively bringing down a significant portion of the Internet.

A successful cybersecurity program encompasses far more than simply an approach that is asset-focused or revolves around only technology. A more holistic, defense-in-depth security approach is needed—one that involves people, processes and technology.

Over the past 15 years in the IoT space, Tridium has learned many lessons involving cybersecurity. We have been closely following the cyber threats that have continued to evolve and have been focused on continuously hardening our products. Because awareness about the threats is so critical, we also have been providing cybersecurity education for our customers, business partners and Niagara integrators.

One of the things that we have learned over the years is that while many organizations are taking approaches that revolve around technology and the security controls of their digital assets themselves (e.g., the target computer systems, devices and data), this alone is incomplete and ineffective. A successful cybersecurity program encompasses far more than simply an approach that is asset-focused or revolves around only technology. A more holistic, defense-in-depth security approach is needed—one that involves people, processes and technology.

PEOPLE, PROCESSES AND TECHNOLOGY

Certainly, technology is a part of the solution. At Tridium, cybersecurity is a top priority. We know that our products must be engineered with security in mind from the beginning, and we make every effort to make our products as secure as possible. At the same time, we also realize that security is a journey that we are on together with our business partners and product integrators. Out of the box, our products need to be securely configured. Once configured, the security of our products also depends on the security of the network. At the same time, the security of each device relies on the physical security of the organization where the device is placed. Finally, it's important to know that security involves not just technology but also people, who need training in processes, procedures and the proper use of IT.

People are sometimes the weakest link. A network engineer with a cybersecurity background may create a very secure infrastructure for his home—it may be protected by various firewalls and advanced intrusion detection systems—but if this engineer's spouse or child clicks on a rogue email attachment or a bad link, it could download malware that could infect the home network, rendering all those network security controls ineffective. In the same way, businesses need to train their employees on best practices involving the use of IT, including configuring smart devices to have the most secure settings. At the same time, general security awareness training that goes beyond IT is also important; for example, employees should be aware of "social engineering attacks," where someone may be able to ask enough questions (over the phone

or in person) to gather enough information to help infiltrate an organization's network. People need to be aware of the cybersecurity threats and the necessary steps to take to defend against them. What's more, people need to be aware of processes and procedures for protecting an organization's digital assets.

Organizational processes and procedures related to cybersecurity are critical, but it is also important that people know that these processes and procedures are to be taken seriously, and supported by management from the top down. There needs to be regular training related to these processes and procedures—otherwise, their development is a wasted exercise. These security policies must be specific to each organization, and, fortunately, many organizations have developed detailed guidelines and policies that can be tailored for any organization. *For example:*

The National Institute of Standards and Technology (NIST) has developed a significant amount of guidance that can be tailored to any organization. For example, NIST Special Publication (SP) 800-53 was developed for information systems in general and is effective for developing a security plan for any organization. Other NIST standards provide more detailed guidance; for example, NIST SP 800-82 provides security guidance specific to control systems, NIST SP 800-50 provides guidance for building an IT security awareness and training program and NIST SP 800-61 provides guidance for developing an incident management and response plan.[3]

The International Society of Automation (ISA) and International Electrotechnical Commission (IEC) have developed the ISA/IEC-62443 series of standards that define procedures for implementing secure control systems, and this guidance applies to end users, systems integrators, security personnel and control systems manufacturers involved in industrial control systems.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides excellent material for organizations managing and connecting control systems.[4] Reviewing these best practices will help you tailor your approach.

In many cases, there may actually be organization-specific best practices, guidelines or compliance standards for securing your systems that apply to your business domain. For example, the United States government has developed the Unified Facilities Criteria (UFC), which applies to any automation system deployed on U.S. government sites, and there are also standards related to HIPAA compliance for the security of information systems in the medical domain.[5] In cases in which no such guidance or standards exist, many of the standards referred to earlier in this section can be extremely helpful.

Organizational processes and procedures related to cybersecurity are critical, and it is also important that they are supported by management from the top down

Finally, **technology** is important. There are various approaches for applying security controls to networks and products. It's important that IT network professionals design organizational networks in a way that they are separated and segmented into various zones to provide defense-in-depth. Firewalls, intrusion-detection systems, intrusion-prevention systems and malware and virus prevention software are critical. Automated backups of systems and devices also can be critical to prevent data loss and device failure and as a means to recover from ransomware attacks. Technology products themselves also can be designed and developed with built-in security controls for making security easier and more effective.

[3] NIST Special Publications can be found at http://csrc.nist.gov/publications/PubsSPs.html.
[4] To see ICS-CERT's recommended practices, see https://ics-cert.us-cert.gov/Recommended-Practices.
[5] For more about the Unified Facilities Criteria, see https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc.

WHAT TRIDIUM IS DOING—DESIGNING SECURITY FOR OUR PRODUCTS

With people, processes and technology in mind, we at Tridium have developed an approach to cybersecurity that can be customized to the security policy of any organization. Our approach for doing this revolves around making it easier for our customers to secure our software, along with enforcing good "cyber behavior" through technology controls.

One of the principles that we used in the design of the security of Niagara 4 is "secure by default." Because the security of our products depends, in part, on the way that integrators configure them, we want their first option to be the most secure option. For this reason, we designed the user interface in Niagara 4 to make options default to the most secure configuration. For example, when users are added to a Niagara station, they default to a password policy where they are forced to choose strong passwords based on Open Web Application Security Project (OWASP) recommendations, and the strongest authentication schemes are used by default. Also, by default, all communications are encrypted. All this requires no configuration by the administrator.

Keeping with the "secure by default" principle, we provide security that does not need configuration at all. We force-change the default credentials immediately upon station commissioning, and we encrypt sensitive data at rest. Additionally, our code is digitally signed and validated for integrity and runtime, and our JACE® 8000 and Edge 10 controller are shipped with "secure boot"—all so that owners can have a non-repudiated assurance that the device and the core software that runs on it have not been manipulated or altered by malicious software.

NIAGARA 4	SECURITY CAPABILITIES
Authentication	Pluggable schemes provide flexibility; defaults are the most secure; supports 2-factor authentication
Identity infrastructure and PKI integration	Can integrate with any PKI infrastructure, SAML 2 Identity Providers for Single Sign-On, LDAP directories, and Kerberos
Role-based access control	Provide authorization for users by security role
Authorization at API level	Sandboxes code, controlling what individual software components can do (a grant/deny permission authorization model)
Encryption of all communications	All communications encrypted by default
Encryption at rest	Sensitive data is encrypted on disk
Digitally signed code, validated at runtime	Assures that core framework code can't be altered or manipulated
JACE 8000 and Edge 10 secure boot	Only boots our digitally signed trusted software, providing assurance against alteration
Common-sense user account management	Configure security mechanisms for attack prevention (lockouts, password strengths, etc.)
Auditing of all user activity	User access is logged to customized levels

OUR "SECURE BY DEFAULT" PRINCIPLE

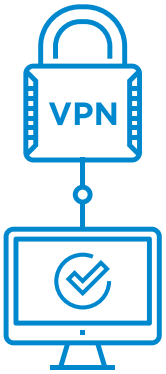
1. **Make security easier: default to the most secure configurations**
   - All transmissions encrypted
   - Users forced to have strong password strengths
   - Users set up with the strongest authentication mechanism
   - User lockouts upon consecutive bad logins
2. **Force administrators to do the 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 runtime
   - JACE® 8000 and Edge 10 secure boot: trusted software validation at boot-time
   - Device identity securely protected in Hardware Security Module on JACE 8000 and Edge 10
4. **Provide stronger configuration options based on the best practices**
   - Articles, documentation and TridiumTalks provide detailed guidance

Finally, we make security configurable so that all Niagara instances can be customized to adhere to organizational security policies related to user account management, public key infrastructure (PKI) and Lightweight Directory Access Protocol (LDAP) integration, password expiration policies and more. To make this as easy as possible, we created a document called the "Niagara 4 Hardening Guide," with step-by-step guidance for administrators to securely configure their systems and integrate them into computer networks in the most secure way. Additionally, we routinely give webinars and presentations to the Niagara community related to cybersecurity awareness, along with best practices for configuring Niagara systems.

As Tridium continues to build products beyond the Niagara Framework, the security of our products will continue to be based on the principle of "secure by default." As our product solutions will range from lightweight edge devices to cloud services that will enable new functionality for our products, cybersecurity will continue to be a critical factor in all our decisions. In doing this, we will continue to embrace open standards as well as closely follow emerging standards and best practices in IoT cybersecurity, focusing on such concepts as secure device identity, identity federation and delegated authorization, data encryption at rest and in transit, and much more.

BEST PRACTICES, BASED ON LESSONS LEARNED

Because of the cyber threats that are continuing to evolve, our company has been focused on cybersecurity education for our customers, business partners and integrators. Over the years, we have come up with some best practices that can be applied to any organization with control systems or IoT devices.



1. DON'T EXPOSE YOUR DEVICES ON THE INTERNET

In the past few years, there has been an increase in hacker tools and systems that crawl the Internet, probe connected devices and index metadata about those devices so that they can easily be searched. Using search engines like Shodan, Censys and others, hackers can make such queries as "connected routers with factory default usernames and passwords" and "vulnerable web cameras," for the purpose of attacking those devices. As we have continued to share at our events such as the Niagara Summit and the Niagara Forum over the last few years, organizations that have devices (and computers) that are directly connected to the Internet are exposed and vulnerable. Whenever you expose any device to the Internet, you are exposing the rest of your network to potential risk. This risk is something that can be remediated in the following ways:

a. If you don't need to connect your device to the Internet, don't. Just because it has an Ethernet connection doesn't mean that you absolutely need to connect it.

b. If your devices need Internet connectivity, make sure that you use network security best practices to isolate your internal devices in such a way that they are not exposed to the Internet. Remember, just because your device is "cloud-enabled" and requires communications *to* the Internet cloud doesn't mean that you need to open up your organization to get incoming connections *from* the cloud. This is a bad practice and exposes your entire network to security risk. At the same time, if you need to provide remote access to devices within your organization, there are many factors to consider, and we recommend ICS-CERT's "Configuring and Managing Remote Access for Industrial Control Systems" as a guide for doing so.[6]

c. Setting up your devices behind a virtual private network (VPN) can offer protection, especially if the devices require remote access or remote administration. For example, many organizations set up a security gateway/VPN router in a DMZ to protect our devices in an isolated control system network, where an authenticated remote user can administer those devices over an encrypted VPN tunnel. This protects the devices behind it from being directly exposed on the Internet. At the same time, this can be one piece of your network security puzzle, which brings us to our next recommendation.

[6] Department of Homeland Security, "Configuring and Managing Remote Access for Industrial Control Systems," https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf.

2. USE A DEFENSE-IN-DEPTH NETWORK SECURITY STRATEGY

Work with your IT department to make sure that you are defending against cyber threats effectively from a network level. Any successful organization should have a well-thought-out defense-in-depth enterprise security strategy that includes a secure network infrastructure with added security controls. This may include firewalls, intrusion detection and prevention systems, VPN solutions, malware detection/remediation technology, continuous network monitoring software and more. An effective strategy that we recommend is isolating your network into separate, protected "zones." This separation is critical, because if one area of your network is breached, it is important to have further protection for other areas. For more information and details on how this can be done, we recommend the paper from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) called "Recommended Practice: Improving Industrial Control System Cyber Security with Defense-In-Depth Strategies."[7]

3. CHANGE "FACTORY DEFAULT" CREDENTIALS

One of the most popular searches on the Shodan site is for various devices with the factory default username and password. Many devices, such as routers and web cameras, ship with default credentials, and users are urged to change them. Sadly, many are not changed, and owners often fall victim to attacks into their networks through these easily hijacked devices. For this reason, in our releases since Niagara 4, we force our users to change the factory default credentials immediately upon commissioning. Many other products do not make such a requirement, and if you are using any product that has default credentials, it is important that you immediately change those credentials—otherwise having that device on your network becomes a liability and an attack avenue into your entire network.

4. PATCH YOUR SYSTEMS

Every day, researchers and organizations such as US-CERT and ICS-CERT publish a slew of new reports of vulnerabilities in Internet protocols and products, along with where to go for patches. This may apply to your computer systems, control systems or device firmware. It is critical that you have someone in your organization tasked with making sure that all systems are up to date. To do otherwise would be to expose systems on your network to cybersecurity risk. At Tridium, we release patches and security releases periodically. When security advisories are released about vulnerabilities in Internet protocols and software upon which Niagara depends, we work quickly to make available a patch or a security release of our software to limit the exposure. For publicly disclosed vulnerabilities and security releases of our products, we issue security bulletins to our OEMs and post them on our website at http://www.tridium.com/en/resources/library.

[7] ICS-CERT, "Recommended Practice: Improving Industrial Control System Cyber Security with Defense-in-Depth Strategies," https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

5. PROTECT YOURSELF FROM RANSOMWARE ATTACKS

Over the last few years, incidents of ransomware attacks have risen incredibly; in these cases malicious software encrypts data on the systems in your network, asking for a "ransom." A recent example was the "WannaCry" ransomware attack that occurred in May 2017, when a cryptoworm infected an estimated 230,000 computers in over 150 countries within one day.[8] This was not limited to computers; hospitals in England and Scotland reported that other equipment affected were MRI scanners, blood storage refrigerators and other mission-critical systems.[9] According to Verizon's 2018 Data Breach Investigations Report that covered security incidents from the previous year, ransomware is the top variety of all malware, and their reports over the past few years have seen a substantial rise in ransomware security incidents.[10] A similar report, done by Symantec Corporation, found that the number of new ransomware families more than tripled in the last year, signaling that more and more attackers are creating new ransomware malware.[11]

For the most part, they are introduced into a network by viruses arising from (a) malicious email attachments in phishing schemes, (b) links clicked on through a web browser or (c) physical media (typically USB drives). It is also possible that ransomware could be introduced into your network via an attack on an IoT device.

Effective ways for protecting yourself are:

a. Educate your people on the safe use of IT assets and the dangers of ransomware.

b. Use anti-virus software on your systems and keep them up to date.

c. Do periodic, scheduled backups of your systems.

d. If you have a supervisory system, such as a Niagara Supervisor, which oversees multiple control systems, treat it as mission-critical infrastructure. This means it should not be used for surfing the web or checking email, as these are potential attack avenues for viruses and malware.

Ransomware is a billion-dollar industry for cybercriminals, and incidents continue to rise at an alarming rate.

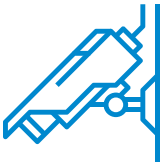
6. ALWAYS USE ENCRYPTED COMMUNICATIONS

Although this seems to be common sense, it needs to be said. If you are using a system in which encryption in communications is optional, don't be tempted to turn it off for any reason. If an adversary has access to a network where your system is installed and you are running unencrypted communications, you will be unprotected from attacks on confidentiality (where your adversary may be able to view sensitive information, such as passwords) or various other attacks, such as impersonation, session hijacking and countless other risks.

[8] BBC News, "Cyber-attack: Europol says it was unprecedented in scale," 13 May 2017, http://www.bbc.com/news/world-europe-39907965.
[9] Jon Ungoed-Thomas, Robin Henry, Gadher Dipesh, "Cyber-attack guides promoted on YouTube," *The Sunday Times*, (14 May 2017).
[10] Verizon, "2018 Data Breach Investigations Report," https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.
[11] Symantec, "Internet Security Threat Report," April 2017, https://www.symantec.com/security-center/threat-report.

7. ALWAYS FOLLOW DOCUMENTED BEST PRACTICES FOR SECURING YOUR DEVICES AND SYSTEMS

Every IoT device and every system you use should have a "security best practices" guide that will give you step-by-step directions. At Tridium, in addition to our security guide that comes with our product, we also release "hardening guides" for our products that show best practices for configuring our systems securely.[12] In the same way, other companies release security best practices. It is important that you read and follow them.



8. DON'T FORGET PHYSICAL SECURITY

Often overlooked as an afterthought, physical security is crucial. It doesn't matter how secure your device is or how securely you have configured it if it is vulnerable to a "sledgehammer" denial-of-service attack or a USB malware attack, which requires physical access.

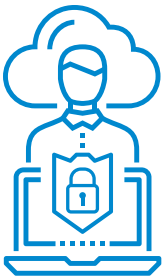
9. UNDERGO FORMAL THREAT AND RISK ASSESSMENTS

Building a cybersecurity approach for your organization revolves around understanding and managing your risks. Formal threat and risk assessments of your operational assets (networks, computers, controllers, etc.) are helpful for determining gaps and vulnerabilities in your cyber defense approach, and this process provides input into how you will manage cybersecurity risk in your organization. Prior to any assessment activity, it is important for your organization to define a risk threshold score that will serve as a determining factor for making mitigation decisions. Typically, risks are scored using the Common Vulnerability Scoring System (CVSS), and each organization determines the score threshold for which mitigations will always occur.

Before any assessment, your organization will identify the assets that you wish to protect and document the security requirements for those assets revolving around confidentiality, integrity and availability. A formal threat and risk assessment can then be done by internal security experts or by a third-party organization trained for that purpose, and the assessment will address the risks to the operational environment. Results of this assessment will all include scored threats and risks discovered, and this report will need to be reviewed by key management stakeholders. For identified threats that have been scored above your organization's risk threshold, your organization will then need to determine how and when to mitigate them with security controls. Remember that this effort shouldn't be a one-time process; because your network assets, devices, system configurations and security requirements change over time, formal threat and risk assessments should be done on a periodic basis.

Because your network assets, devices, system configurations and security requirements change over time, formal threat and risk assessments should be done on a periodic basis.

[12] Our Niagara AX and Niagara 4 hardening guides can be found at http://tridium.com/resources/library.



10. DON'T FORGET ABOUT "PEOPLE, PROCESSES AND TECHNOLOGY"

Although security technical controls are a key part of the solution, the weakest links in cybersecurity are often undefined (or not-well-defined) processes and the people who need to follow them. There need to be defined security policies and procedures in your organization that revolve around the use of IT, patching software, incident response, security technologies and much more. There are so many resources available, especially the publications created by NIST and ICS-CERT (mentioned earlier in this paper) that contain policies and best practices that can be customized for your organization. These policies need to be relevant (and revisited over time to make sure they are), and they need to be enforced. Training and security education are critical; the people in your organization to whom these policies apply need to be educated to understand and follow them.

The IoT cybersecurity landscape is populated with a range of threats, requiring that each of us be prepared, vigilant and continually assessing and refining our security approach. We hope that the guidance for defending against those threats is helpful and gives you a foundation for developing your own strategy. At Tridium, we realize that the cybersecurity process is a journey—one that we share with our customers and other community stakeholders. As we continue this journey, we will focus on not only the security of our products, but also our commitment to continue to share best practices that can be used in our community and beyond.

TRIDIUM

tridium.com

Locations and customer support, worldwide

Headquarters
North America
1 804 747 4771

Support
North America & Latin America
1 877 305 1745

Europe, Middle East & Africa
44 1403 740290

Asia Pacific
8610 5669 7148

2019-0002