IT Security for OT Systems – Best Practices

Version 1.0

REAL ESTATE CYBER CONSORTIUM (RECC)

REAL ESTATE
CYBER CONSORTIUM

IT SECURITY FOR OT SYSTEMS

Building Operational Technology (OT), considered a subset of Internet of Things (IoT) technology, broadly refers to systems used to control and monitor critical physical processes within buildings. Unique aspects of OT systems and devices demand modified approaches to minimizing cyber security risk. This best practice list serves as a summarization of industry best practice by corporate, commercial, educational and governmental real estate professionals focused on the design, installation, commissioning, operations, and maintenance of next generation Building Operational Technology.

The list of best practices addresses topics intended for:

- Traditional IT staff, who may not be familiar with the unique environment of building operational technology;
- Building operators, who may not be experienced with IT and IS lifecycle management best practice and operational frameworks; and
- Industry service providers and solution manufacturers, who must focus on alignment of product offerings with increasing cyber security scrutiny

Best practices are categorized into the following groups:

- Technical: Device specific and system-wide considerations for access control, configuration, capabilities, etc.
- Policy & Process: Incorporation of OT into existing IT lifecycle management practices
- People: Ensuring proper knowledge and experts are in place to support OT

Last Modified
5/28/2019

REAL ESTATE
CYBER CONSORTIUM

TECHNICAL (DEVICE SPECIFIC AND SYSTEM-WIDE)

RECC Best Practice Discipline Area	Sub-category	Best Practice	Justification and clarification
Technical (device specific and system-wide)	Access Control	Multi-factor authentication	Ensure two-factor authentication practices are in place (especially, or at minimum for administrator accounts) to reduce unauthorized account access
		Complex user account passwords or "pass-phrases"	Ensure the use of stronger passwords to minimize "brute-force" password guessing
		Disable or rename default user accounts	As many OT devices ship with default administrative or configuration user settings, be sure to disabled or rename these settings
		Limit administrative level account permissions to a well-known group of resources	Limiting the administrative access to those who have a need to know will strengthen your access control process
		Provide "least-privilege" account permissions to all users with device and system accounts	Ensuring no user has the capability to do more than what their role entails will limit security incidents and help with audit logging
		Use only named accounts for one-to-one, person-to-account credentials	The use of general user accounts results in credential sharing which increases the chance of unauthorized access
		Reduce remote access to devices and systems	Filtering access to device management consoles by IP will reduce the chance of unauthorized access
		No hard-coded password	OT device code or programming should not use hard-coded passwords. Contact OEM for alternate solutions
		Periodic review of user accounts	Certify user accounts should still be active in systems to avoid active account to those who no longer require
	Device and System Configuration	Devices are patchable via properly authenticated mechanism	Security is an on-going process and IT/OT devices must be remediated/patched per corporate standards
		Device uses trusted update mechanism to accept patches	Ensure there is a managed/trusted process to push patches to all devices that is controlled by your security officer
		Standard device configurations are developed, deployed and tracked for variance	Creation of a standard settings list for common devices will aid in quick remediation efforts in addition to ensuring uniform secure baselines
		If capable, disable or configure to meet organization security standards: - Bluetooth - Wireless - NTP - SMTP - FTP - Telnet - SSH - Remote Logging - Non-essential device services	Ensure the device configurations limit the use of services based on the functions required by the IoT device
		Configure devices and systems to perform minimum required services and duties for which they are intended for	Ensure the device configurations limit the use of services based on the functions required by the IoT device. Common example: Prevent email and internet access from device management consoles

TECHNICAL (DEVICE SPECIFIC AND SYSTEM-WIDE)

RECC Best Practice Discipline Area	Sub-category	Best Practice	Justification and clarification
Technical (device specific and system-wide)	System Architectures	Develop and maintain a technical target architecture	Consider implementation of architectural review board to obtain alignment across IT and OT disciplines; Target architecture should include data-flow diagrams
		System communication architectures leverage segmented networks, micro-segmentation and other cyber security techniques, such as: - Application whitelisting - Layered network architectures - Firewalls, access control lists or unified threat management devices	Ensure co-mingling of building assets with network/corporate assets are kept at a minimum; Segmentation: Logically or physically segment your IoT assets from your corporate assets (or at least limit integrating or connecting systems); Consider leveraging separate production and non-production environments helping facilitate proper change management techniques
		Cloud integration and/or hosting is configured to enforce encryption (in transit and at rest) and implements appropriate separation within the cloud environment.	Ensure co-mingling of building and device data within a shared/multi-tenant environment is appropriately separated and encrypted in order to prevent unauthorized access and/or sharing of information between cloud tenants; Encrypting critical data will minimize compromise and use of your data assets; Review of device functionality, data flows and configuration for assets communicating with the cloud should be included as a part of the technical target architecture documentation and the device/system approval process
	Physical and Cyber Protections and Capabilities	Devices use industry-standard protocols for communications between devices	The use of standard communication protocols will strengthen authentication, improve error detection, and ensure data transmission quality
		Devices use industry-standard protocols for encryption of data in transit and at rest; This includes associated system file and databases	Encrypting critical data will minimize compromise and use of your data assets
		Deploy physical security techniques	Ensuring key IT/OT devices are physically secured with access controlled to those resources who have a need to know will prevent unauthorized access
		Add to existing IT intrusion prevention techniques	As IoT become more and more common, consideration should be given to augment your intrusion prevention to check for abnormal behavior of IoT devices
	Device Data	Perform data classification activities to aid in proper architectures	An understanding of the overall IoT data architecture will assist with the identification of the proper security controls to be assessed
		Perform data retention analysis on devices	Minimize or eliminate IoT data hoarding – keep/collect what you need/require and ensure regular back-ups of data and system to allow for recovery
		Add to existing IT data loss prevention techniques	As IoT becomes more common, consideration should be given to augment your data loss prevention to monitor for unauthorized data leakage associated with IoT devices; Specifically, in cloud architectures: 1) If edge-to-cloud is cloud orchestrated, leverage secure device protocols enabling easy-to-push change at scale in a zero day risk scenario 2) If edge-to-cloud cannot be cloud orchestrated, tunnel device traffic so that any zero day risk in the device protocol is encapsulated allowing for better management at scale
	Coding Standards	Ensure OT supplier leverages proper coding standards, such as Open Web Application Security Project (OWASP)	Ensuring security is "baked" into the product/vendor during the design/development of the IoT device will improve overall security posture

POLICY & PROCESS

RECC Best Practice Discipline Area	Sub-category	Best Practice	Justification and clarification
Policy & Process	Vulnerability & Incident Management	Implement and maintain written policy covering OT	Operational technology, in contrast to traditional information technology, has important differences impacting the ability to meet traditional IT policy; Development of OT specific policies will ensure proper protections are in place for the OT environment and reduce cycles required to manage traditional IT policy exceptions and violations
		Provide contractual language to account for disclosure of potential vulnerabilities	Reference the "RECC Vendor Language for Cyber"
		Identify and track vulnerabilities of assets in inventory	Use manufacturer and other industry (ICS-CERT) vulnerability databases to assess inventory cyber-vulnerability exposure
		Develop incident response policies for OT	The physical-to-digital nature of OT devices result in incident response practices differing from typical cyber and IT incident response
		Ensure timely remediation of discovered vulnerabilities	Ensure OT policy and process are designed to meet the capabilities of the real estate portfolio support staff and industry in order to remediate exposure as quickly as possible
	Acquisition	Provide contractual language to have OT provider (seller) produce certification of vulnerable-free devices	Reference the "RECC Vendor Language for Cyber"
		Develop, monitor and practice a controlled acquisition process for OT and OT systems	Controlled acquisition is a key element of managing inventory
	Inventory	Maintain an inventory of OT assets	This includes development of processes accounting for controlled acquisition and disposition and change and maintenance records
	Maintenance	Perform patching of all OT assets	IoT devices (where appropriate) must be patched through the stack OS, middleware, and application including related modules on a regular basis as defined by your corporate security guidelines
	Assessments & Audits	Conduct an end-to-end assessment of building and IoT systems as described by RECC Best Practices Assessment	Reference the "RECC Best Practices Assessment - Building and IoT Cyber Risk Management Framework" for an in-depth listing of Assessment and Audit components
		Perform automated device audits to validate asset inventory, patch levels, configurations	
		Perform vulnerability assessments (pen tests, etc.)	
		Conduct regular risk assessments of cyber programs	
		Conduct regular risk assessments on OT vendors	
	Contracts & Legal	Third party vendor contracts	Ensure contract arrangements align to enterprise cybersecurity policies and dictate specific operational requirements; Review RECC Vendor Language Best Practices for details
	Technology Currency	Address end of life systems (including firmware, software and embedded modules) through a risk assessment	Ensure leadership both understands and responds to risks (remediate, avoid, transfer, accept, etc.)

RECC Best Practice Discipline Area	Sub-category	Best Practice	Justification and clarification
People	Training	Properly train staff on OT vulnerabilities	Different threat vectors and risks are present with potential impact to equipment damage, occupant comfort and potentially safety; Properly trained staff who understand these differences provide increased level of awareness on how vulnerabilities impact the real estate environment
	Staffing	Ensure technical staff are properly qualified to address uniqueness of OT industry	OT equipment and system profiles vary widely across OT categories; Qualified staff help develop solid cyber security profiles
	Third party services & contracts	Provide contractual language for seller to notify buyer of any known security vulnerabilities for the duration of the contract	Breach Notification (specify time period), including physical breach, as well as loss of mobile media, and must cooperate with Owner (including notification duties if requested)
		Provide contractual language for seller to provide anticipated timeline for ending security support for devices	
		Provide contractual language for seller to provide formal notification when security support ends	
		Provide contractual language for seller to maintain and enforce retention policies for any and all reports, logs, audit trails and any other documentation that provides evidence of security, systems, and audit processes and procedures	
		Provide contractual language for [seller] to notify [buyer] of a security incident within 24 hours of becoming aware of a security incident impacting the [buyer]. In the event that [seller] notifies [buyer] of a security incident or the [seller] is notified by the [buyer] or any third party of a security incident, [seller] shall cause its authorized users and subcontractors to: (a) Fully cooperate with [buyer] and its third-party advisors in investigating and resolving the vulnerability giving rise to the Security Incident; (b) Provide [buyer] with information regarding the Security Incident, including but not limited to the steps taken to contain the Security Incident and to mitigate any harm to [buyer] and any remedial actions taken to prevent further occurrences of the Security Incident; and (c) Fully cooperate with [buyer] with respect to any investigation, reporting and notification requirements, including those required by Law	Reference the RECC "Guiding Principles to Improve Cyber Security Protection for Property Owners and Managers", which addresses risks introduced by service providers and items such as legal precedence for agreement breaches, ability of user organization to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault and how international boundaries may affect the issues
		Provide contractual language for seller to notify buyer in writing within 24 hours of: an employee's or contractor's departure from the [seller]; or an employee or contractor no longer needing remote access to [buyer's network]; or [seller] determining the need to cancel such user's access to [buyer's network] for any reason; or any remote access user accounts that are no longer needed by [seller]	
		Provide contractual language that defines the obligation of [sellers] to restore the application or services in accordance with established SLA's for expected recovery	

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

Real Estate Cyber Consortium (RECC) ("Consortium") standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While the Consortium administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

The Consortium is a volunteer professional organization with no regulatory, licensing or enforcement power over its members or anyone else. The Consortium does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public because its works are not obligatory and because it does not monitor the use of them.

The Consortium disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. The Consortium disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. The Consortium does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, the Consortium is not undertaking to render professional or other services for or on behalf of any person or entity, nor is the Consortium undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

The Consortium has no power, nor does it undertake to police or enforce compliance with the contents of this document. The Consortium has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. The Consortium does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document should not be attributable to the Consortium and is solely the responsibility of the certifier or maker of the statement.

PRIVILEGED AND CONFIDENTIAL

Real Estate Cyber Consortium (RECC) ("Consortium") board members and contributor members ("Participants") are expected to ensure their participation and communications serve the procompetitive objectives identified by Consortium and do not violate the antitrust laws. Participants should focus discussions on Consortium's statement of articulated objectives.

This means that no activity or discussion at our meetings or other functions, or independent of our Consortium activities, may be engaged in for the purpose of bringing about any understanding or agreement among the Participants' activities that affects competition among the Participants including any of the following: (a) raising, stabilizing, or setting prices for products and/or services of the Participants; (b) regulating the nature or volume of products or services offered by the Participants; (c) allocating geographic markets or customers served by the Participant; (d) encouraging boycotts or unreasonably seeking to exclude specific entities and/or third-party vendors from the Consortium; or (e) otherwise restricting competition among the Participants and/or among third-party vendors.

In addition, Participants must not discuss or reveal any individual Participant's competitively-sensitive proprietary information, including any Participant's prices, margins, discounts, costs, capacity, inventory, sales, customer lists/customer contacts, future business plans, or bids for contracts.