

Cybersecurity Guidance for Data Center Power and Cooling Infrastructure Systems

White Paper 216

Version 1

by Patrick Donovan and Katie Hargraves

Executive summary

Monitoring data center physical infrastructure systems with management software means connecting power, cooling, environmental and security monitoring devices to IP networks. These networks often extend to remote servers, corporate IT systems, mobile devices, and 3rd party cloud services. These connections offer potential avenues of attack for hackers. Mitigating these cyber security risks requires continuous action from both vendors and those involved in the design, installation, operation, and maintenance of the data center. This paper describes what to expect from vendors and presents user best practices for each phase of the lifecycle of the site. NOTE: This white paper is not a detailed, step-by-step guide for your actual, specific installation. Rather, it is meant to be an overview guide or checklist to assist in developing a detailed strategy.

RATE THIS PAPER



Introduction

Network-connected, data center physical infrastructure equipment¹ – i.e., the power, cooling, and environmental/security-monitoring devices found in the IT space - are necessary for ensuring availability and making operation of the data center efficient. However, these network connections, particularly if poorly designed and implemented, could be used by cyber criminals as an attack surface. A typical installation is composed of widely distributed, network-connected hardware devices communicating to network gateways, firewalls, and on-premise or remote infrastructure management (DCIM) servers. These connections may extend to mobile devices, corporate IT and facility management systems, and 3rd party cloud services. **Figure 1** shows a simplified block diagram of an example data center to highlight the many potential cyber-attack vectors on power and cooling infrastructure that is network connected to potentially a wide variety of devices, users, and monitoring systems. The arrows represent data flow and network connectedness.

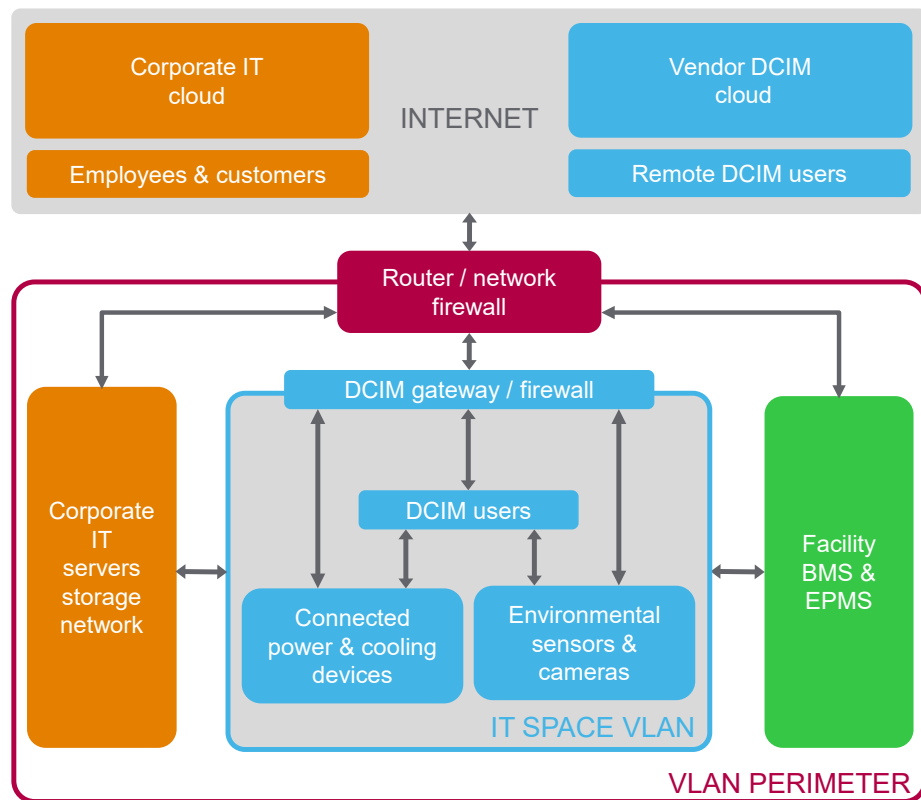


Figure 1

This simplified block diagram of an example data center and its devices' network connections to other devices, networks, and management platforms illustrates the need to be diligent with cybersecurity best practices throughout the site's lifecycle.

Despite the continuous threat and concern, power and cooling devices and their management platforms can be “hardened” (i.e., made more secure) thereby greatly reducing cyber risks by following the best practices described in this paper. An effective protection plan requires constant vigilance and evolving defense tactics since cyber threats are ever changing and striving to beat whatever current defense measures exist now. **It is a common mistake to put much of your effort and focus on design, but not enough on on-going vigilance and maintenance to keep protection measures and technology up to date.** This requires operational discipline and executive management support.

As with any corporate IT network, **cybersecurity of the power and cooling infrastructure and its management networks must be a consideration at every phase of the data center lifecycle.** This begins with choosing device and management software vendors who are proactive and prioritize cybersecurity in the development,

¹ Sometimes referred to as operations technology (OT)

support, and maintenance of their offers. Security should be a main driver of all their actions, and they should be transparent about it with the public. This paper will explain what to expect from the vendor and what characteristics to look for in their offers. It will then describe cybersecurity best practices for IT space power and cooling infrastructure design, installation/setup, and the operations & maintenance phases of the site's lifecycle. A complete security strategy would cover people and processes, physical security, as well as network and device hardening. This paper focuses on the hardening and protection of connected data center infrastructure devices and their networks across their lifecycle.

NOTE: This white paper is not a detailed, step-by-step guide for hardening your actual, specific installation. Rather, it is meant to be an overview guide or checklist to assist in developing a specific cybersecurity strategy.

For those who are managing a portfolio of smaller, highly distributed edge IT sites, see Schneider Electric White Paper 12, [“An Overview of Cybersecurity Best Practices for Edge Computing”](#).

The cybersecurity guidance covered in this white paper will be explained in the context of the data center lifecycle as shown in **Figure 2**.

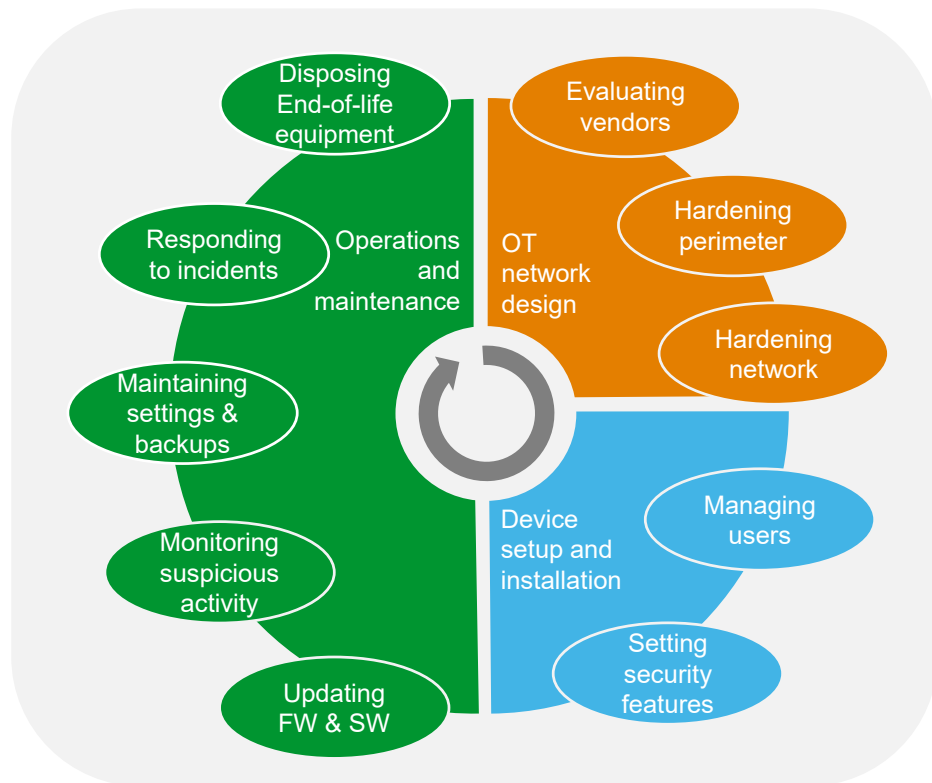


Figure 2

Shows the topics of cybersecurity guidance given in this paper in the context and flow of the data center lifecycle starting from the initial design of the network, to device installation and setup, and on through the long operations and maintenance

Vendor evaluation criteria

Manufacturers of data center power, cooling, environmental monitoring infrastructure devices, and their management software suites play a critical role in your cybersecurity strategy. The degree to which a vendor prioritizes security in the design, development, and support of their products should be a key decision factor in which solutions you choose. Always choose to work with security-conscious vendors who are proactive, open, and transparent. Doing so will make it less likely for a breach to occur since there should be less vulnerabilities by design and any that do emerge should be detected and addressed sooner than they would otherwise.

Evaluating a vendor’s cybersecurity acumen comes down to interviewing them and reading their documentation that [convey how they manage cybersecurity risks](#) through their design and development practices, as well as how they support their products once deployed in the field. The following sub-sections are a list of attributes and best practices to ensure your chosen vendor has or follows. Embracing these indicates the vendor has a “security-first” corporate culture that impacts everything from staff hiring and training, as well as product design, testing, and technical support.

Follows secure development lifecycle (SDL) process

SDL is a process by which security is considered and evaluated throughout the development lifecycle of hardware and software products. It was originally developed and proposed by Microsoft². The use of an SDL process to govern design, development, deployment, and operation of a device or management software application is good evidence that the vendor is taking the appropriate measures to ensure security and regulatory compliance. The SDL process spans many aspects of the development lifecycle including internal staff training, security documentation, the use of design best practices, handling of source code, 3rd party intrusion testing, and post-sales, incident response support, etc. The vendor should be using a process that is either certified [ISA/IEC62443-4-1](#), or that is consistent with ISO 27034³. Schneider Electric White Paper 239, [Addressing Cyber Security Concerns of Data Center Remote Monitoring Platforms](#), describes an effective SDL process in more detail.

Relies on independent technology validation

Whether developed internally or via a 3rd party, the vendor’s software and device cybersecurity features should be assessed by a cybersecurity-accredited assessment body. [CREST](#) accreditation and IEC 62443-4-2/-3-3 certifications are an example. They are an international not-for-profit providing internationally recognized accreditations for organizations, products, systems, and professional-level certifications for individuals.

Operates under an information security policy

The vendor and all of their 3rd party contractors and suppliers should operate under and adhere to a policy that insures customers and their device data are handled, stored, and safeguarded from unauthorized access and use according to broadly recognized standards and regulations including [ISO27001](#), [NIST](#), [ISA/IEC62443](#), and [GDPR](#).

Monitors and assesses cybersecurity capabilities regularly

Mature vendors will regularly review their capabilities through accredited labs and by using the support of external independent entities such as consultants, auditors, and [pen-testers](#). By seeking continuous improvement in mitigating risks in this way, the vendor will improve its ability to detect potential vulnerabilities, control weaknesses, identify potential attack vectors, and assess potential impact of new threats on their customers and partners.

Manages product vulnerabilities openly and timely

Vendors should have a process for managing vulnerabilities in their products that should be based on [ISO30111](#). A DevOps team should be established, well-staffed

² https://en.wikipedia.org/wiki/Microsoft_Security_Development_Lifecycle

³ <http://www.iso27001security.com/html/27034.html>

and outfitted with the ability to continuously detect and mitigate any vulnerabilities. They should also be responsible for responding quickly to any vulnerability discovered and/or reported by 3rd parties or cybersecurity researchers via an established (by the vendor) [online portal](#) for reporting. In this way, vendors can demonstrate a willingness to work transparently and collaboratively with researchers, cyber emergency response teams, and device operators to ensure that accurate vulnerability mitigation and remediation information is provided.

OT network design and configuration best practices

This section applies not only to new data center builds, but also to retrofits and expansion projects where new devices are being added and networked to management software platforms. The operations technology (OT) network refers to the (typically) IP-based network used by the data center power, cooling, and environmental monitoring devices to communicate with their software management platforms such as data center infrastructure management (DCIM) and building management systems (BMS).

Defense-in-depth

Since malicious cyber-attacks use computer networks to access, change, steal, or destroy information, focusing on the network (used for infrastructure device monitoring) design is critical in managing this risk. While security and network administration policies (outside the scope of this paper) are a key foundation for developing robust network security, this section will focus most on some key guidance for ensuring the power and cooling infrastructure management network is well designed for security. **A secure network begins with adopting a “defense in depth” (DiD) strategy for the network design.** Figure 3 illustrates the layers of defense (i.e., hardening) involved in this white paper.

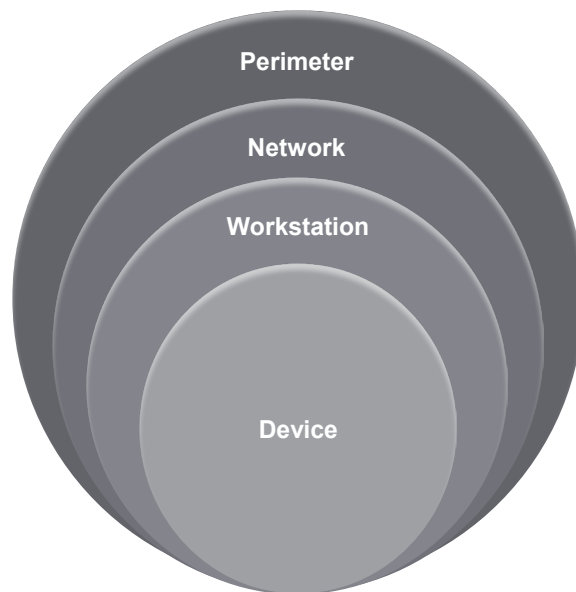


Figure 3

Defense-in-depth involves a layering of security hardening tactics to limit the impact of any one cyber breach.

DiD involves a layering of multiple, independent security technologies and processes to provide security redundancy and to limit the impact of any one cyber breach. Before providing design/selection guidance for each layer of the OT network’s defense-in-depth design approach, it is first worth noting two important caveats:

- OT network design should be **developed with inputs from all relevant stakeholders** including:
 - IT network management
 - Facility operators
 - System integrators and/or managed service providers (MSPs)
 - Security consultants
 - Device vendors

- **Good cybersecurity starts with effective physical security** to prevent unauthorized access to monitored devices and network physical and virtual infrastructure (cabling, servers, routers, firewalls, gateways, etc). Schneider Electric White Paper 82, "[Physical Security in Mission Critical Facilities](#)" and White Paper 102, "[Monitoring Physical Threats in Data Centers](#)", provides more information on this topic.

The following sub-sections were derived from content from Schneider Electric's overview guide titled, "[Read This First: Recommended Cybersecurity Best Practices](#)". Note that workstation and device hardening are discussed in the next section on setup and installation.

Perimeter hardening

Building a highly protected network perimeter that helps prevent outside access is the most critical line of defense against cyberattacks. The use of network [firewalls](#) contributes to security by controlling the flow of information into and out of network entry points. Using a set of user-defined configuration rules, a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. We recommend that you follow these general guidelines related to the use of firewalls:

- Always place network-connected power and cooling devices behind firewalls and other security protection appliances⁴ that limit access to only authorized remote connections.
- Limit access to the networks on which power and cooling devices are connected through careful setup of user access policies within the firewall.
- Do not allow unsecured devices that face the public internet to minimize exposure to attackers by employing network scanning tools that will identify internet-accessible OT devices.
- Continually monitor for events that might indicate attempted unauthorized access.

Some best practices for configuring network firewalls include⁵:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic. A typical approach is:
 - Create rules that explicitly deny access
 - Add rules to permit only the required access
 - Add a broad-based rule to deny access to all remaining traffic

⁴ Examples: antivirus scanning devices, content filtering devices, intrusion detection system (IDS)

⁵ [Best Practices for Securing an Intelligent Building Management System \(iBMS\)](#)

- Confirm that the firewall can detect TCP “SYN-flood” attacks by tracking the state of a TCP handshake.
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.

Network hardening

- Logically (virtually) separate the OT network from other corporate, guest, or public networks and implement secure network access controls

The OT devices in the data center should connect to a network that is separate from other corporate networks. A recommended way to do this is through the use of [VLANs \(virtual local access networks\)](#). VLANs enable the OT network to utilize the same physical network (i.e., cabling and network appliances) used by other corporate networks while logically separating and isolating the network at the data layer of the [OSI model](#). This virtual separation provides some degree of security. OT network security is further enhanced through the design and implementation of firewalls as described above. Together, this helps protect data center operations from cyber threats that might have breached business or other corporate backend systems and vice versa. This segmentation and isolation, in effect, limits the potential impact of a breach. A separate VLAN-based network that exists behind a well-configured firewall ensures that data center power and cooling device data, including broadcasts to all nodes, remains within the logical boundary established by the design. In some environments, it may be preferable to use zones and conduits. Refer to IEC 62443-3-2 for detailed information on zones and conduits.

Think carefully before granting outside access. Each network entry and exit point must be secured. By granting access only when a valid reason exists, you can minimize risk and keep security costs down. So, reduce the pathways into and within your networks. Implement security protocols on existing pathways (e.g., VPN) to make it more difficult for a threat to enter and move around your system. Strong segmentation helps prevent an attacker that enters one part of the network from gaining access to other areas. Utilize multifactor authentication where available. Sanitize laptops and systems that were connected to any other network by fully updating software programs and using antivirus protection. Also, require all remote users to connect and authenticate through a single, managed interface before conducting software upgrades, maintenance, and other system support activities

- Design in measures for detecting compromises

Minimize the chances of compromise by designing in anomaly detection. This is the capability to continuously monitor and audit system events. Use network security tools such as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), antivirus software, and network usage logs to help detect compromises as early as possible. Note these anomaly detection tools are available as a service from qualified vendors. Include a [trusted time server](#) such as [NTP \(Network Time Protocol\)](#) to synchronize the clocks for all devices in your network. This helps ensure that your device data logs provide accurate data about the time of any breach that can then be easily correlated to other devices at the site.

- Use DCIM monitoring tool or network scanning solution to create an asset inventory and network map

A detailed inventory of your assets and a map of your infrastructure can help increase awareness of components that may require patching and backup. We recommend following these basic guidelines:

Installation & setup best practices for devices and workstations

- Inventory all devices with an IP address, including their software and firmware versions.
- Include removable media and spare equipment.
- Identify all communication protocols used across the network.
- Catalog external connections to and from the OT networks, including vendor, third-party, and other remote access.
- Implement alerting to notify you when new devices are added your network

This section covers the workstation and device hardening layers of the DiD strategy as shown in **Figure 3** above. Installation and setup include user account management and the configuration of security features of each system component including configuring network firewalls (as described above), hardening network-connected infrastructure devices, configuring user accounts for devices and management software, and enabling threat detection as mentioned above. This section focuses on the devices, management software, and the workstations/mobile devices used to access them.

Data center power and cooling infrastructure systems communicate to software management platforms through built-in network ports or added network communication modules, also known as network management cards (NMCs). When devices are first installed and setup, it is important to configure the NMC network communication and user-access parameters to maximize security. During the initial installation and setup process, the devices and management software might be more vulnerable to attack. During this process, temporarily isolate the system from the outside world until all aspects of your security strategy are in place.

Prior to going “live” with an installation, be sure that all devices and management software servers/gateways have the latest firmware available. It is also important to review any security bulletins that might exist for the products being used. Contact the vendor if you’re not sure. Schneider Electric keeps new and updated security bulletins at its [Schneider Electric Security Bulletins web page](#).

By securing individual devices and software management servers/gateways, you not only reduce the risk of an internal attack to control or shut down that device and interrupt connected loads, but it also reduces the chances of it being used as a point of access into the larger software management system and network. The specific step-by-step process to harden will vary depending on the make/model/manufacturer and whether it’s an NMC-based device or the physical or virtual machine hosting the management software (e.g., DCIM server). However, the general best practices should apply to all and can be grouped in two categories: user management and security features and settings.

User management

Devices and their management software platforms control access to their data, in part, through user accounts. Vendors will provide multiple user types defined by their level of access and rights to view and/or edit (i.e., read/write). Best practices related to user account setup include:

- Replace all default vendor passwords with strong alternatives, and if possible, utilize an authentication server to centralize authentication, authorization and accounting management; Strong passwords should be eight characters minimum with a mix of letters, numbers, and symbols; enforce the number of failed

login attempts before locking the account. Implement multifactor authentication wherever supported.

- Likewise, remove all default logins (i.e., administrator) and system IDs.
- Disable every user's access to the system by default and add permissions only as required.
- Restrict each group of users to the lowest level of privileges necessary to perform their role.
- Require the use of a password manager.

For much more detailed guidance on digital identity management, see [NIST Special Publication 800-63](#) and [NIST Appendix A on Strength of Memorized Secrets](#).

Security features and settings

Enabling and configuring security-related features or settings in the device NMC and management software platform is obviously a critical aspect of setup and installation. Best practices related to these features or settings are described below.

Protection of passwords and passphrases

Ensure that device-stored passwords passphrases are hashed or encrypted; and not stored as plain text. Vendor device cybersecurity documentation should have this information. Here is [an example](#) of such documentation for Schneider Electric's Network Management Card 3.

Device access methods, authentication, and their use of encryption

Evaluate each device to determine what network ports and access methods are available, and whenever possible, use a non-standard port and disable any that do not have a planned use. Note that port scanning applications can help expedite the identification process. Be sure to disable ports and access methods that were used temporarily for device commissioning but won't be needed during operation. Here is a list of common device access methods with a note about their preferred method of use.

- Remote access through command line interface – Do not use Telnet, but rather use [Secure Shell Protocol \(SSH\)](#).
- Simple Network Management Protocol (SNMP) – Use SNMPv3 with the strongest authentication and encryption enabled and not SNMPv1 or SNMPv2c; SNMPv3 offers enhanced cybersecurity features including an authentication passphrase and encryption of data in transit.
- File transfers – Use [Secure Copy Protocol \(SCP\)](#) and not File Transfer Protocol (FTP).
- Web server – Use [Hypertext Transfer Protocol Secure \(HTTPS\)](#) instead of HTTP, since HTTPS uses [Transport Layer Security \(TLS\)](#), a cryptographic protocol designed to provide security for data transmitted over IT networks.

More secure-conscious vendors will, by default, disable the less secure methods. Basic authentication, however, is typically accomplished through network port access, usernames, passwords, and IP addresses without using encryption. For enhanced protection, use the more secure, encryption algorithm-based methods of access as described above, and ensure the other less secure methods are disabled.

Some vendors may also support additional authentication features to further enhance security such as...

- Network-based port access via [extensible authentication protocol over LAN \(EAPoL\)](#); this enables a request for network access at the individual port level via the network's switch or router (where applicable) which the device network management card is connected.
- Centralized authentication, authorization, and accounting management through [Remote Authentication Dial-in Users Service \(RADIUS\)](#).
- Use of [digital certificates](#) (also known as public key certificates) with TLS protocol to authenticate the network-connected device or its embedded web server to the web browser (the TLS client) used to access the device or server.

Device firewalls

Device network management cards with web servers will offer firewall functionality. For enhanced security, make sure this is enabled and configured. Review the policy rules and make sure to edit existing rules or add/delete new ones as required for your installation.

Also, configure your device (and network) firewalls to allow network-based scanning by Information Security (IS) vulnerability scanners. IS should scan hosts on the network and determine if hosts are vulnerable to common network threats, or if a system appears to have been compromised.

Automatic updates

It is recommended to allow or enable automatic updates of device firmware, management software or server/gateway patches to help ensure infrastructure and its management software remain secure against evolving threats.

Workstations/laptops/mobile devices used for accessing devices and management servers/gateways

Every device used to access the OT network management software (e.g., DCIM, BMS, etc) and its network-connected devices needs to be as safe as possible. Scan any devices used to exchange data, such as external hard drives or USB drives, before using them in any node connected to the network. Remove unnecessary programs and services from workstations and store sensitive data on a server. Regularly back up data from hard drives. Finally, require all users to lock their screens when they aren't in use.

Consider stronger authentication methods for critical host devices such as:

- Biometric Authentication limits access based on a physical or behavioral characteristic such as a fingerprint.
- Two-Factor Authentication limits access to users with both a password and a physical or soft token.

Operations & maintenance best practices

Data center power and cooling infrastructure devices, their software management tools, and the network they run on all need to be monitored and maintained from a security perspective. While there are tools available to help with this task, it still takes operational discipline to be consistent, thorough, and persistent. Vigilance is critical as cyber threats are constantly evolving and system firmware and software evolve over time potentially opening new vulnerabilities for hackers and cyber criminals. For guidance on improving your overall data center facility operations and maintenance program beyond just security, see Schneider Electric White Paper 196, "[Essential Elements of Data Center Facility Operations](#)" and White Paper 197, "[Facility Operations Maturity Model for Data Centers](#)".

At a fundamental level, there are five principal tasks for the operations team responsible for cybersecurity of the infrastructure once it is operational:

- Keeping firmware and software updated
- Maintaining security settings and data backups
- Monitoring for suspicious activity
- Responding to a breach
- Disposing of end-of-life devices and servers

Some guidance to operations teams for each task is given below.

Keeping firmware and software updated

All OT network-connected devices, appliances, gateways, and servers must always be kept up to date with the latest firmware or software patches. Note that a network-connected infrastructure device contains both device firmware and network management card firmware and/or software. It is important that both are kept up to date. Cyber criminals are constantly working to find vulnerabilities in existing code in order to hijack the device to steal data, control devices, cause outages, etc. New firmware and software patches not only fix bugs and provide additional performance enhancements, but they often address known security vulnerabilities. These code updates should be installed or applied as soon as they become available from the vendor. This requires on-going discipline from the operations team. Here are a few related tips:

- Enable auto updates when possible.
- Check for and use mass configuration/update features sometimes found in device management software platforms to accelerate the application of new code to multiple devices at once.
- If testing and validation of new firmware/software is required, employ a patch monitoring and management tool to prioritize devices/appliances and available patch updates, verify patch source and integrity through digital signatures, and facilitate the change management process.
- Use a DCIM monitoring tool that includes a security assessment function (**Figure 4** shows an example) that provides a report on which devices need an update or have compromised security settings in their network management card.

Maintaining security settings and data backups

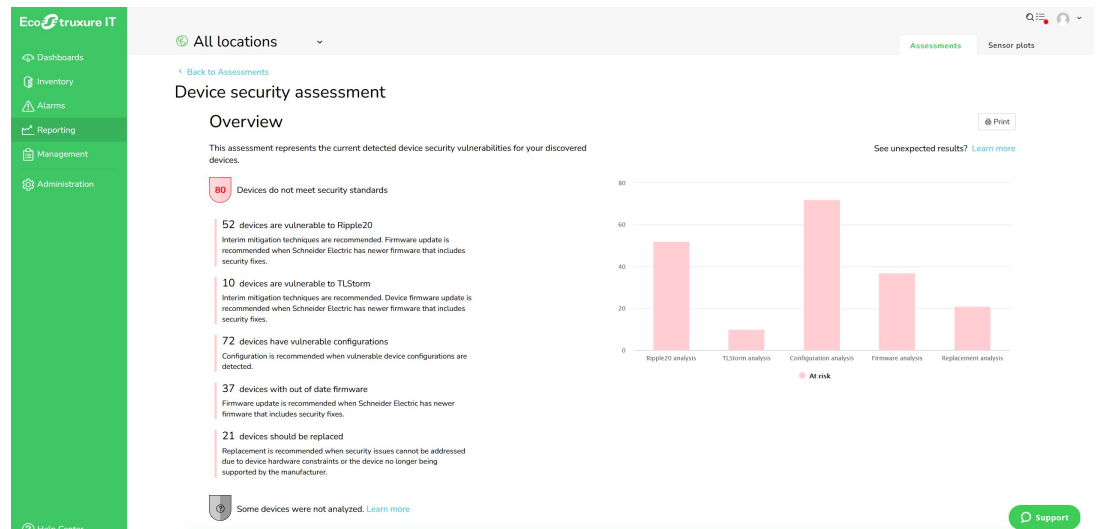
The security features and settings that were enabled and configured during the initial setup and installation, need to be maintained throughout the life of the infrastructure device, network appliance, or management server/gateway. By minimizing the number of users with the ability to change these settings, you reduce the chances of unintended or non-permitted changes being made. Beyond that, these settings should be checked regularly to ensure they remain set properly over time. DCIM tools with a security assessment feature as shown in **Figure 4** can simplify this work significantly, at least, for power and cooling infrastructure devices. Also, as new devices are added, the change management process needs to properly account for the user account creation and the devices' security settings and features as described previously.

Also, back up all critical resources off the network and keep a copy in a secure, tamper-proof, or offline environment. Ensure that you have multiple backups over

time, so you can restore from a version that predates any infection. Remember to test backups regularly

Figure 4

This screenshot shows an example of a DCIM security assessment feature from Schneider Electric's EcoStruxure Data Center IT Expert software tool. The feature assesses which devices are not meeting security standards in terms of firmware being up to date and whether there are any vulnerable configurations.



Monitoring for suspicious activity

Assuming network security tools like intrusion detection and prevention systems (IDSs and IPSs) are in use for the OT network, operations teams must provide the time and staff resources to regularly monitor system logs (e.g., firewall activity logs) and promptly respond to alerts. These efforts should include ensuring this data along with OT device and workstation logs are sent to security information and event management system (SIEM), if in use. Effective use of these tools can block malware, stop attacks in progress, and be used to review data to identify a past attack that might have gone unnoticed. These lessons learned should lead to adjustments in security settings and policies to improve preparedness for future cyber events. As with any monitoring software tool, it is important for the operations team to be well trained and familiarized with the tools' settings and functions.

Responding to an attack/data breach

In the facility operations and maintenance (O&M) realm, a cyber-attack or data breach represents a crisis; an urgent, critical event or situation that, if not responded to properly, will eventually result in system interruption and/or loss of business. Therefore, it is important for O&M teams to have an overarching Crisis Management Plan (CMP) which should include an Incident Response Plan (IRP), also known as an Emergency Operating Procedure (EOP) for cyber-attacks/data breaches. CMP deals with preparing for, detecting, mitigating, and post event analysis of a crisis. The IRP is used for the immediate response to a crisis as it is developing in the hopes of stopping or containing the attack to limit its impact. Schneider Electric White Paper 217, "[How to Prepare and Respond to Data Center Emergencies](#)" goes into the elements of an effective CMP in detail.

A well-designed and executed IRP should stabilize the situation, provide clarity as to what has happened, guide operator actions to stop and/or limit the attack, and initiate processes to issue communications and resume or restore business operations. It should provide step-by-step instructions to ensure all activities are carried out in a safe and deliberate manner. This is done to prevent further (or wider) service interruption or loss of data. These negative effects result from performing work in an uncontrolled manner. So, it is important for all operations staff to review the plan and be trained in its execution, ideally through the use of regular drills. The

plan should exist as a document and preferably maintained through a computerized document management system (CDMS). Another key guidance is to ensure the plan is clear about who does what and to have a very clear escalation path. Otherwise, operational paralysis can occur particularly in the midst of a stressful crisis.

There are good examples of incident response plans online that can be used to form the basis for your plan. The University of California Berkley offers a detailed explanation and catalog of the elements of an IRP [here](#).

Note, you should consider implementing an Incident Response Retainer (IRR) to ensure there is the resources and expertise required to quickly mitigate the impacts of a cyber breach.

Disposing end-of-life equipment

To ensure user, device, log files, and configuration data does not fall into the wrong hands, consult vendor documentation to understand how to erase this data before the product is disposed of and/or recycled. For power and cooling infrastructure devices, these instructions are typically contained in the device hardening guide.

Considering cybersecurity services

For those data centers who either do not have the resources or who wish to have 3rd party expert support and validation, there are vendors, like [Schneider Electric](#), who offer cybersecurity services. These solutions can run the gambit from consulting services (e.g., gap analysis, policy & procedure development), to network design, device hardening, training of operations teams, as well as monitoring and maintenance services (e.g., firewall & device monitoring, OT security information and event management).

Conclusion

How to mitigate cybersecurity risks associated with data center power and cooling infrastructure and its management networks must be a consideration at every phase of the data center lifecycle. This begins with choosing device and management software vendors who are proactive and prioritize cybersecurity in the development, support, and maintenance of their offers. Security should be a main driver of all their actions, and they should be transparent about it with the public. Data center operators must adopt a defense-in-depth approach, as described in this paper, to the design and implementation of the OT network, the devices, and its software management systems. And finally, throughout the long operations and maintenance phase of the data center, operators must constantly remain vigilant and active in monitoring for suspicious activity, maintaining security settings and data backups, updating device/appliance firmware, and being well trained and prepared for responding to cybersecurity incidents if they occur.

Disclaimer

IN NO EVENT SHALL SCHNEIDER ELECTRIC IT CORPORATION, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC IT CORPORATION OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC IT CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC IT CORPORATION RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

About the authors

Patrick Donovan is a Senior Research Analyst for the Energy Management Research Center at Schneider Electric. He has over 27 years of experience developing and supporting critical power and cooling systems for Schneider Electric's Secure Power Business unit including several award-winning power protection, efficiency, and availability solutions. An author of numerous white papers, industry articles, and technology assessments, Patrick's research on data center physical infrastructure technologies and markets offers guidance and advice on best practices for planning, designing, and operation of data center facilities.


Katie Hargraves is a Cybersecurity Advisor with over 24 years of experience assuring quality and cybersecurity for critical power and cooling systems at Schneider Electric. As a Certified Secure Software Lifecycle Professional (CSSLP), she works to incorporate security practices into each phase of the software development lifecycle (SDLC) for Schneider Electric's Secure Power Business unit's software and embedded firmware offers.

RATE THIS PAPER






 [An Overview of Cybersecurity Best Practices for Edge Computing](#)
White Paper 12

 [Addressing Cybersecurity Concerns of Data Center Remote Monitoring Platforms](#)
White Paper 239


 [Physical Security in Mission-Critical Facilities](#)
White Paper 82


 [Monitoring Physical Threats in Data Centers](#)
White Paper 102


 [Essential Elements of Data Center Facility Operations](#)
White Paper 196

 [Facility Operations Maturity Model for Data Centers](#)
White Paper 197

 [How to Prepare and Respond to Data Center Emergencies](#)
White Paper 217

 [Browse all white papers](#)
whitepapers.apc.com

 [Browse all TradeOff Tools™](#)
tools.apc.com

 [Learn more about the next evolution of DCIM](#)
se.com/dcim

Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
dcsc@schneider-electric.com

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at
www.apc.com/support/contact/index.cfm