Life Is On Schneider Electric

Cybersecurity Guidance for Data Center Power and Cooling Infrastructure Systems

White Paper 216
Version 2.1

Data Center Research & Strategy

by Patrick Donovan
Katie Hargraves
Maria A. Torres Arango

Executive summary

Connecting power, cooling, environmental, and security systems to IP networks brings efficiency but also creates new vulnerabilities. These networks often touch remote servers, corporate IT, mobile devices, and cloud services. They create potential entry points for cyber attacks. Managing this risk requires constant vigilance from vendors and all parties involved in designing, installing, and operating the data center. This paper outlines what to expect from vendors and offers a clear checklist to help you build a strong, actionable cybersecurity strategy.

RATE THIS PAPER ★★★★★

Key takeaways

1. **The interconnected nature of physical infrastructure equipment in data centers poses significant cybersecurity risks that can be mitigated with appropriate cybersecurity best practices**. Network design, device installation and setup, plus operations and maintenance, constitute the lifecycle phases of the cybersecurity framework for data center equipment.

2. **We present a framework for vendor evaluation and provide guidance on physical infrastructure equipment integration.** It is based on *defense-in-depth* and *zero trust* cybersecurity strategies and leverages the synergy between "secure by design" and "secure by operation" philosophies.

3. **Factors to evaluate equipment vendors on their security maturity include their development processes, independent security certifications, and information security policies.** Transparency is a primary attribute to consider. **A reputable vendor will be transparent about their security practices and have a clear process for managing and disclosing product vulnerabilities.**

4. **Device management network design must include inputs from all relevant stakeholders.** This includes IT managers, facility operators, system integrators, security experts, and device providers.

5. **Layered network segments, with distinct domains and explicit verification policies, helps block intrusions and limit the damage if a breach occurs.**

6. **During the installation and setup, it is crucial to secure every component.** Every device and piece of software at a workstation is a potential attack vector. Securing these involves managing user accounts, configuring firewalls, and hardening devices to protect against potential threats.

7. **The operations & maintenance phase is the longest, therefore it has the highest risk. T**hroughout this phase, it is vital to keep all device firmware and management software tools updated, maintain their security settings and backups, and continuously monitor for suspicious activity. Also, having clear procedures to respond to breaches – and preparing for such events – can help mitigate the impacts of any cybersecurity incidents.

8. **Use of third-party cybersecurity services can be helpful especially when lacking expertise or staff bandwidth is limited.** Different service tiers are often available, depending on the data center's needs and the maturity level of its cybersecurity operations.

Introduction

Network-connected, data center physical infrastructure equipment – i.e., the power, cooling, and environmental/security-monitoring devices found in the IT space – is necessary for keeping a data center available, resilient, and efficient. However, these network connections, particularly if poorly designed and implemented, can be exploited by cybercriminals as attack surfaces.

A typical installation features widely distributed, network-connected hardware devices communicating with 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 displays a simplified data center, highlighting the numerous power and cooling infrastructure components subject to a potential cyber-attack vectors. These are network-connected to a wide variety of devices, users, and monitoring systems.

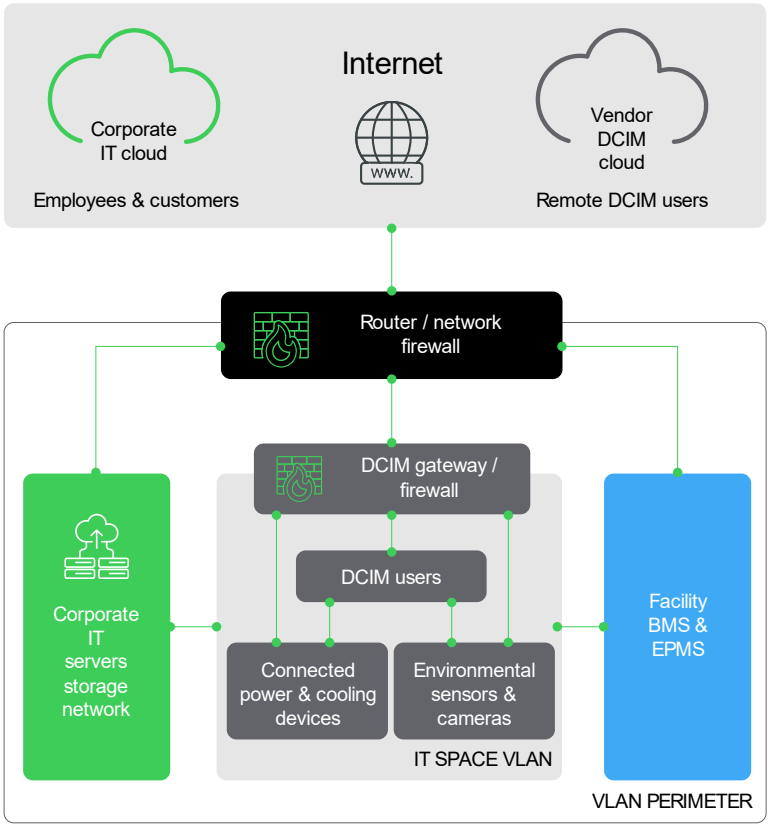


Figure 1

Simplified diagram of an example data center and its devices' network connections to other devices, networks, and management platforms.

Diligence with cybersecurity best practices throughout the site's lifecycle becomes essential for reliable and efficient data center operation.

Despite the continuous threat and concern, power and cooling devices, along with their management platforms, can be "hardened" (i.e., made more secure) by following the best practices described in this paper, significantly reducing cyber risks. An effective protection plan requires constant vigilance and evolving defense tactics, as cyber threats are ever-changing. Cyber-criminals will continually strive to evade current defense measures.

It is a common mistake to devote too much effort and focus to design, but not enough to ongoing vigilance and maintenance, which are essential for keeping protection measures and technology up to date. This requires operational discipline and executive management support. These best practices can be implemented in stages, depending on the maturity of your operations, covering cybersecurity needs incrementally in a more cost-effective manner. Cybersecurity cash flows have often been regarded as costs. Yet, the reality is that these are

increasingly being viewed as an investment, considering the escalating risks and potential costs associated with a cybersecurity incident in the evolving, interconnected data center space. An OT cybersecurity breach could not only result in downtime, but also cause environmental incidents leading to fines, bans, and loss of business.

As with any corporate IT network, **cybersecurity of the power and cooling infrastructure, as well as its management networks, must be a consideration at every phase of the data center lifecycle.** This begins with choosing devices and management software vendors who are proactive and prioritize cybersecurity in the development, support, and maintenance of their offerings. **Security should be the primary driver of all vendors' actions, and they should be transparent about it with the public**.

This paper explains what to expect from vendors and what characteristics to look for in their products and services. We 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 should 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, where two approaches act in concert: *Secure by Design* and *Secure by Operation*[1].

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

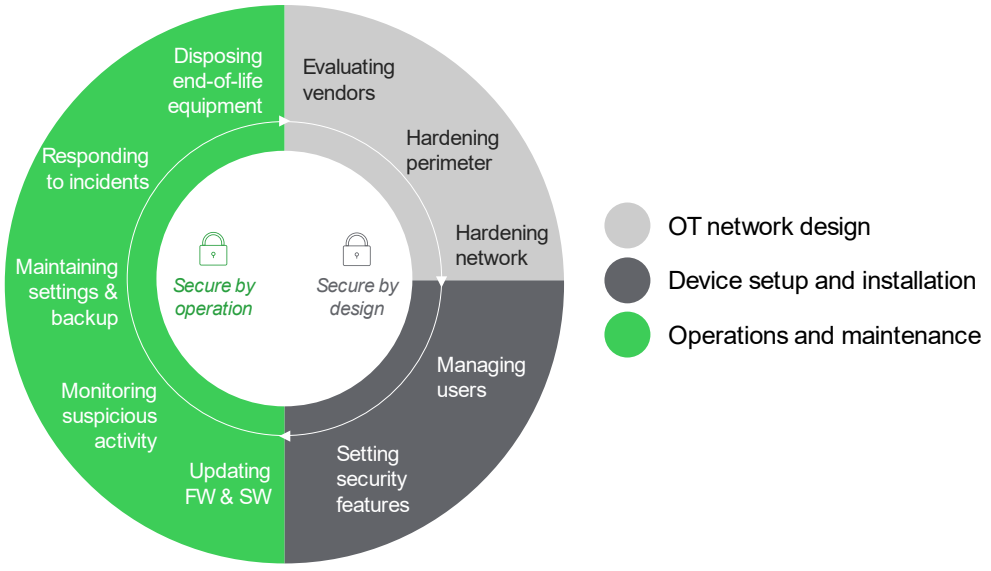
For those who are managing a portfolio of smaller, highly distributed edge IT sites, see Schneider Electric White Paper 12, *"An Overview of Cybersecurity Best Practices for Edge Computing"*.

The cybersecurity guidance presented in this white paper is provided within the context of the data center lifecycle, as illustrated in **Figure 2**.

Figure 2

Topics of cybersecurity guidance provided in this paper in the context and flow of the data center lifecycle. We start from the OT network design, move to device setup & installation, and on through the operations & maintenance phase.

This cybersecurity framework leverages the synergy between the Secure by Design and Secure by Operation philosophies.



[1] Operations team and design teams work together to deploy systems that meets the cybersecurity design requirements set by both product vendors and the OT network designers. Integrators play a critical role in setting and maintaining a resilient cybersecure installation.

Vendor evaluation criteria

Manufacturers providing 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 security-conscious vendors who are proactive, open, and transparent. Doing so makes a breach less likely to occur since there should be fewer vulnerabilities by design, and any that do emerge should be detected and addressed sooner than they would otherwise.

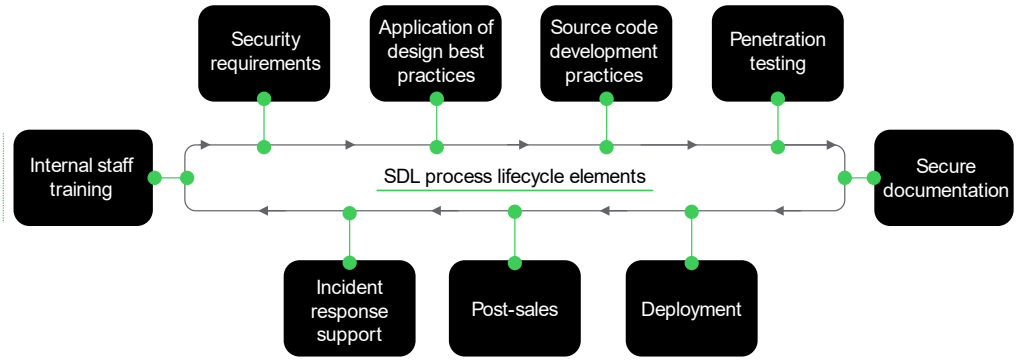
Evaluating a vendor's cybersecurity acumen comes down to interviewing them and reading documentation conveying how they manage cybersecurity risks. This details their design and development practices, as well as how they support their products once deployed in the field. Next, independent testing of vendors' offerings and components can validate your assessment of their cybersecurity compliance and management practices. The following subsections outline the attributes and best practices that your chosen vendor should possess or adhere to. Embracing these practices indicates the vendor has a "security-first" corporate culture, impacting everything from human resources (hiring and training) to assets and software (product design, testing, and technical support).

Follows secure development lifecycle (SDL) process

The SDL process considers and evaluates hardware and software throughout the entire development lifecycle. Initially proposed and developed by Microsoft[2], the use of an SDL process is good evidence that the vendor is taking the appropriate measures to deliver security and regulatory compliance. Such SDL process should govern design, development, deployment, and operation of a device or management software application. Figure 3 shows main elements in the SDL process that impact the development lifecycle.

Figure 3

Elements of the SDL process lifecycle that enable vendors to implement and maintain a more secure cyber posture.



The vendor should use a process that is either certified to ISA/IEC 62443-4-1 or is consistent with ISO 27034[3] Schneider Electric White Paper 239, *Addressing Cyber Security Concerns of Data Center Remote Monitoring Platforms*, describes an effective SDL process in more detail. Our SDL certification can be found here.

Relies on independent technology validation

Whether developed internally or through a third-party vendor, the software and device cybersecurity features of the vendor's products should be assessed by a cybersecurity-accredited assessment body. CREST accreditation and IEC 62443-4-2 and IEC 62443-3-3 certifications are examples. These are international not-for-

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

[3] http://www.iso27001security.com/html/27034.html

profits providing internationally recognized accreditations for organizations, products, systems, and professional-level certifications for individuals.

Operates under an information security policy

The vendor, along with all their third-party contractors and suppliers, should operate under and adhere to policies that protect customers; handling, storing, and safeguarding their device data from unauthorized access. It must also provide that usage is in accordance with broadly recognized standards and regulations. These include ISO 27001, NIST, ISA/IEC 62443, and GDPR. While adhering to regulations is a legal requirement, alignment with recognized standards is often the baseline for a secure posture. Vendors with a secure focus implement best practices that go beyond regulatory alignment.[4]

Monitors and assesses cybersecurity capabilities regularly

Mature vendors will regularly review their capabilities through accredited labs and utilize the support of external, independent entities such as consultants, auditors, and penetration testers. By seeking continuous improvement in threat prevention and risk mitigation, the vendor will improve its ability to detect latent vulnerabilities, control weaknesses, identify evolving attack vectors, and assess the impact of threats on their customers and partners. Moreover, such vendors will maintain open communication lines with their customers and efficient subscription to security bulletins and security alerting channels.

Manages product vulnerabilities in an open and timely manner

Vendors should have a process for managing vulnerabilities in their products that is based on ISO30111. A DevOps team should be established, well-staffed, 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 parties or cybersecurity researchers via an established (by the vendor) online portal for reporting. This is referred to as **responsible disclosure**. In this way, vendors can demonstrate a willingness to work transparently and collaboratively with researchers, cyber emergency response teams, and device operators to provide accurate vulnerability mitigation and remediation information.

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 typically to the IP-based network used by the data center. This includes power, cooling, and environmental monitoring devices that communicate with software management platforms, such as data center infrastructure management (DCIM) and building management systems (BMS). The guidance provided here is based on the implementation of *Defense-in-Depth* and *Zero Trust* cybersecurity strategies.

Defense-in-depth

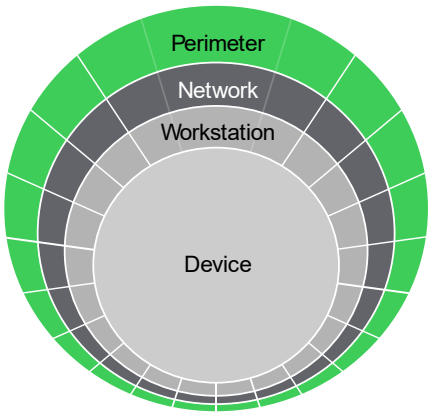
Since malicious cyber-attacks use computer networks to access, change, steal, or destroy information, focusing on the network (used for infrastructure device monitoring) design is critical in managing this risk. Security and network administration policies are outside the scope of this paper. However, they are a key foundation for developing robust network security. This section focuses on providing well-designed security guidance for the power and cooling infrastructure management network. **A secure network begins with adopting a** "defense in

[4] See Schneider Electric's approach to digital policy implementation: *NIS2 Directive* and *Cyber Resilience Act (CRA)*

depth" (DiD) strategy for the network design. Figure 4 illustrates the layers of defense (i.e., hardening) involved in this white paper.

Figure 4

Defense-in-depth involves a layering of security hardening tactics to limit the impact of any one cyber breach phase. Zero trust involves use of least privilege access and strict verification to access domains of data and devices, under the assumption of a compromised network to limit the impact of a 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.

Zero trust

Zero trust is a cybersecurity strategy that requires strict identity verification for any user and device attempting to access resources, even if they are within the network perimeter. [5] Three main zero trust pillars inform best practices at the different stages of the data center lifecycle. These include:

- Never trust, always verify – Access to data and devices is not granted by default but should be authorized and validated at every instance.
- Use least privilege access – Access is granted for limited periods of time and limited amounts of data to mitigate the impact of a cybersecurity incident.
- Assume there's a breach - By treating your network as if it were compromised, the impact of a potential intrusion is mitigated. Monitoring and analysis of risk are implemented continuously.

Before providing design/selection guidance for each layer of the OT network, 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*, provide more information on this topic

[5] See the *CIO Federal Zero Trust Data Security Guide* for further information on this topic.

Note that workstation and device hardening are discussed in the next section on setup and installation.

Perimeter hardening

Building a well-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 appliances[6], limiting 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 access the networks. This minimizes 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 include:[7]

- 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.
- 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 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 area 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[8]. This virtual separation provides some degree of security. OT network security is further enhanced through the design and implementation

[6] Examples: antivirus scanning devices, content filtering devices, intrusion detection system (IDS)

[7] *Best Practices for Securing an Intelligent Building Management System (iBMS)*

[8] OSI refers to Open Systems Interconnection model developed by the International Organization for Standardization ISO

of firewalls as described above. Together, these help 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, limit the potential impact of a breach. A separate VLAN-based network that exists behind a well-configured firewall protects data center power and cooling device data, including broadcasts to all nodes, keeping it 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 who 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 provide accurate device data logs about the time of any breach that can then be easily correlated to other devices at the site.

- Use a 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:

- 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 to your network.

Installation & setup best practices for devices and workstations

This section covers the workstation and device hardening layers of the DiD strategy, as shown in Figure 4 above. Installation and setup include:

- user account management,
- 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,
- enabling threat detection as mentioned above.

This section focuses on the devices, management software, and workstations or 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 set up, it is essential 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 reduce the risk of an internal attack to control or shut down that device and interrupt connected loads. Moreover, you also reduce the chances of devices 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 is 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 into 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 & 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

Make certain that device-stored passwords and passphrases are hashed, 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 standard device access methods with notes about their preferred method of use.

- Remote access through command line interface – Use Secure Shell Protocol (SSH) as it provides encryption capabilities, strong authentication, and secure device communication and control over insecure channels like the internet. Legacy protocols like Telnet must be avoided as these are not secure and could pose serious threats to your data and physical infrastructure.
- Simple Network Management Protocol (SNMP) – Use SNMPv3 with the strongest authentication and encryption enabled; 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 security-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 disable less secure methods that may also be available.

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) to 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 any vulnerabilities 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 keep infrastructure and its management software 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 requires organizations to have operational discipline – to be consistent, thorough, and persistent.

Vigilance is critical as cyber threats are constantly evolving, and system firmware and software also evolve, 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. Both must be kept up to date.

Cyber criminals are constantly working to find vulnerabilities in existing code 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 ongoing 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.
- Leverage only certified tools and field services provided by legitimate vendors to perform updates to the local datacenter infrastructure.
- 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.

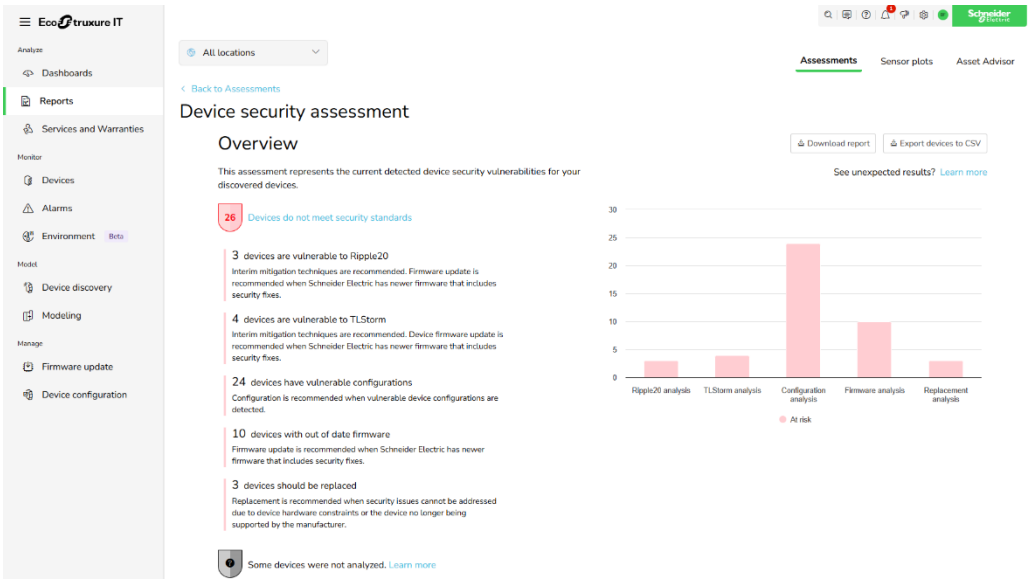
Maintaining security settings and data backups

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 validate they remain set properly over time. DCIM tools with a security assessment feature, as shown in Figure 5, 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, whenever possible, back up all critical resources and store the backup off the network. Maintain multiple backups over time, so you can restore from a version that predates any infection. Remember to test backups regularly.

Figure 5

This screenshot shows an example of a DCIM security assessment feature from Schneider Electric's EcoStruxure™ 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 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 enabling this data, along with OT device and workstation logs, are sent to the 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, the operations team needs to be well-trained and familiarized with the tool's 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 appropriately, 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 situation as it is developing, with an aim toward 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, which include contacting local authorities and informing vendors and customers in a controlled fashion by order of dependency of the supply chain.

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
- initiate processes to issue communications
- resume or restore business operations.

The IRP should provide step-by-step instructions, so all activities are carried out safely and deliberately. 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 is that the plan is clear about responsibilities: who does what, and with a very clear, precise 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 provide additional resources and expertise if required to quickly mitigate the impacts of a cyber breach.

Disposing end-of-life equipment

To prevent user, device, log files, and configuration data from falling 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 that either do not have the resources or who wish to have 3rd third-party expert support and validation, there are vendors, like Schneider Electric, who offer cybersecurity services.

Using third-party support allows data centers to focus on other aspects of their business while maintaining a secure position. Similarly, for organizations facing cybersecurity staffing challenges or a lack of cybersecurity experience, managed security services represent a route to obtain their desired cybersecurity maturity level. Figure 6 provides a summary of the services a cybersecurity vendor can provide.

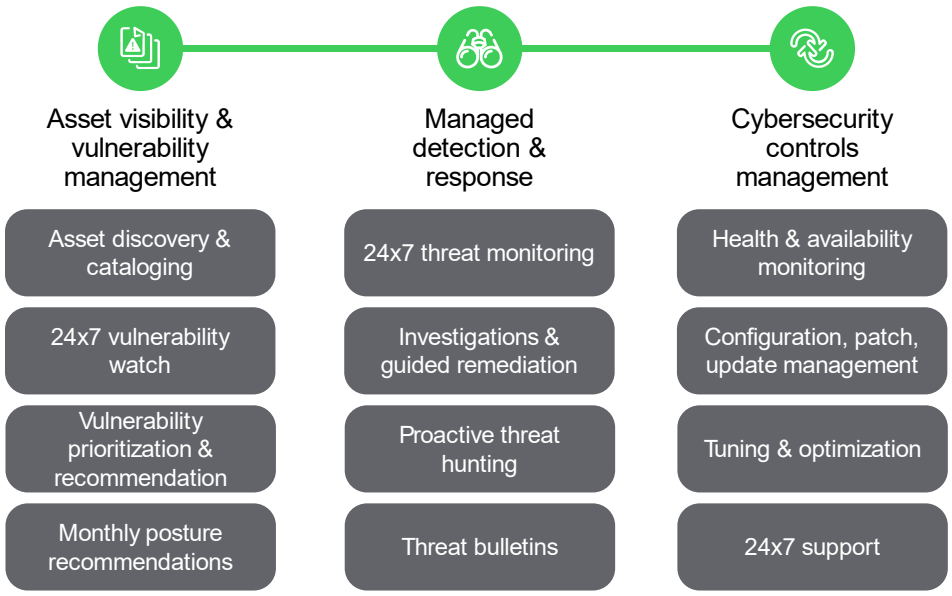


Figure 6

Managed security services offered by Schneider Electric

Different services coverage is available allowing operators to scale based on their cybersecurity maturity, staffing, and risk tolerance

AI and cybersecurity in infrastructure systems

As AI becomes part of the operational fabric of data centers, it both strengthens and tests resilience. The same intelligence predicting load, balancing power, and optimizing cooling now shapes how systems and people defend together against incursions. Cybersecurity is no longer a separate control layer; it is built into the data center itself, governing how intelligence, energy, and human action stay in sync.

AI as protection

AI enhances protection when applied to infrastructure telemetry and operational behavior. Models trained on baseline patterns can detect deviations in power use, network traffic, or user activity. These often precede faults or intrusions. By learning from both system data and human operations, AI supports decision-making, reduces alert fatigue, and prevents errors caused by oversight or workload. It also strengthens the human layer through operator training and procedural compliance. This can turn insight into consistent action. Integrated with Schneider Electric's OT/IT cybersecurity frameworks, AI accelerates detection, shortens response, and reinforces segmentation and access policies. This allows operational data to become an active defense layer: continuous, adaptive, and auditable.

AI as threat

While AI is a benefit to cybersecurity, it also expands the attack surface. Adversaries and cybercriminals use similar tools to exploit data, mislead models, or imitate authorized user behavior. Safeguards must now extend from code to conduct: linking encrypted telemetry, zero-trust identity management and validation of models, access points, and operator behavior. Every part of the system must continue to perform as expected, but to validate its integrity under real-world conditions. Software and procedures must co-evolve to deliver appropriate protections. Vigilance in both is critical.

As AI becomes integral to both protection and performance, managing this duality requires shared accountability. Collaborative cybersecurity services (built around verified telemetry, lifecycle validation, and disciplined human practice), now define operational maturity. Data centers must evaluate if they have the capabilities to do this on their own or should consider additional support.

Next steps

Mitigating cybersecurity risks associated with data center power and cooling infrastructure and its management networks must be considered at every phase of the data center lifecycle. We provide a framework to evaluate power and cooling infrastructure vendors and to integrate this equipment in the data center. We recommend you take these next steps:

1. **Choose device and management software vendors who are proactive and prioritize cybersecurity in the development, support, and maintenance of their products and services**. Security should be the main driver of all their actions, and they should be transparent about it with the public.
2. **Adopt a defense-in-depth approach to the design and implementation of the OT network, the devices, and its software management systems**. Strengthen this approach using **zero trust** principles to prevent intrusions and mitigate the impact of breaches.
3. **Remain vigilant and active throughout the long operations and maintenance phase of the data center.** This includes 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.
4. **Benefit from the experience of third-party security service providers** to build your cybersecurity expertise and maximize the reliability and efficiency of your data center. Even for mature organizations, these services provide a calibration point to maintain a proactive approach and a secure position.

About the authors

Patrick Donovan is a Senior Research Analyst for the Energy Management Research Center at Schneider Electric. He has over 30 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 27 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.

Dr. Maria A. Torres Arango is a Research Analyst in Schneider Electric's Data Center Research & Strategy group. She investigates technology, materials and infrastructure to guide data center strategies. She also examines market forces driving technology advancement and participates in developing tools that highlight tradeoffs or selection in critical data center decisions. Maria's former expertise involves materials design and optimization; and fundamental studies on materials synthesis processes using X-ray characterization at the National Synchrotron Light Source II, Brookhaven National Laboratory. A lifelong learner, Maria holds a BS in aeronautical engineering from Universidad Pontificia Bolivariana, Colombia; and a MSc in aerospace engineering and a PhD in materials science and engineering from West Virginia University.

Acknowledgements

Special thanks to **Dee Kimata,** Cybersecurity Though Leadership Director**;** and **Kreshnik Musaraj,** Cybersecurity Officer Data Center Business; for peer reviewing this white paper.

Resources

An Overview of Cybersecurity best Practices for Edge Computing
White Paper 12

Addressing Cyber Security 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

DCIM Monitoring Value Calculator for Distributed IT
TradeOff Tool 29

Browse all TradeOff Tools™
tools.apc.com

Note: Internet links can become obsolete over time. The referenced links were available at the time this paper was written but may no longer be available now.

Contact us

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

Schneider Electric Data Center Research & Strategy
dcsc@se.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