How Modern DCIM Addresses CIO Management Challenges within Distributed, Hybrid IT Environments

White Paper 281

Version 3

by Patrick Donovan

Executive summary

The role of today's CIO is expanding and becoming more challenging. The days of managing a single enterprise data center are over. Business requirements are forcing CIOs to hybridize their data center and IT portfolio architecture by placing IT capacity in colocation facilities and building out capacity at the local edge – sometimes in a big way. In addition to managing and maintaining resilient and secure operations at all these sites, they are now being asked to report on the sustainability of their IT operations. Software management tools need to evolve in order for CIOs to do their jobs effectively. Through examples, the paper explains how modern DCIM platforms are a critical tool for making hybrid enterprise IT more resilient, secure, and sustainable.

RATE THIS PAPER ★★★★★

Introduction

It is widely reported[1,2] that the role of a Chief Information Officer (CIO) is experiencing a sea change. IT is now at the center of business strategy as digital technologies power and sustain the global economy. The criticality of IT in every aspect of business has driven CIOs from just filling the tactical role of deploying, operating, and maintaining IT to also focusing on business strategy. CIOs increasingly have a leading role in driving business innovation, aligning IT projects with business goals, digitalizing business operations, and leading corporate organization change programs, for example. This role expansion has made their job more critical and complex.

What has not been as widely reported, however, is that the traditional CIO role of IT service delivery has become more critical and complex as well. After all, a CIO's impact on business strategy and execution depends on continuous IT service delivery. As shown in **Figure 1**, the success of a CIO is ultimately rooted in a solid foundation of maintaining resilient, secure, and sustainable IT operations. But, in an environment of highly distributed hybrid IT, this becomes harder to do.

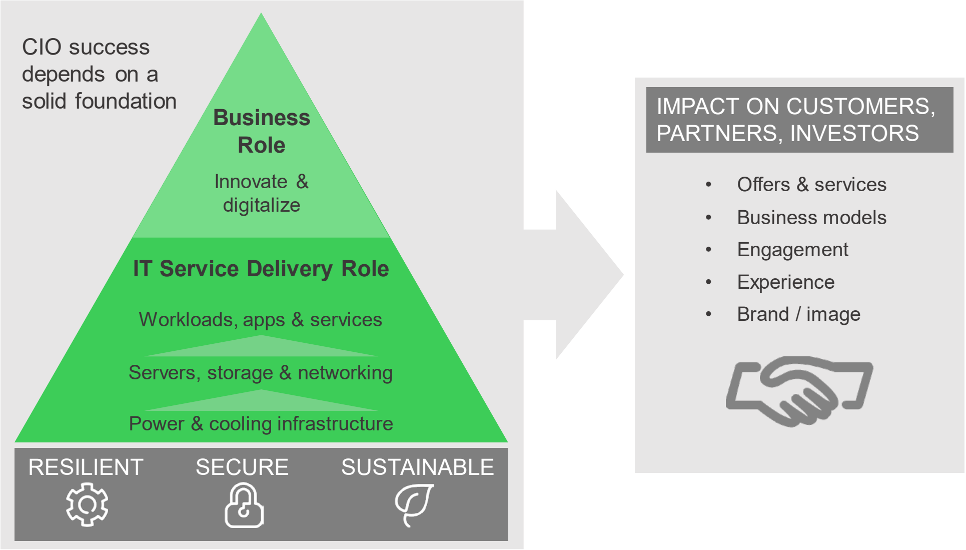

CIO success depends on a solid foundation
Business Role
Innovate & digitalize
IT Service Delivery Role
Workloads, apps & services
Servers, storage & networking
Power & cooling infrastructure
RESILIENT
SECURE
SUSTAINABLE
IMPACT ON CUSTOMERS, PARTNERS, INVESTORS
Offers & services
Business models
Engagement
Experience
Brand / image

Figure 1

CIO success in both their business and traditional roles of IT service delivery are dependent on maintaining resilient, secure, and sustainable IT operations. DCIM is a critical tool for building and sustaining that foundation.

Modern data center infrastructure management (DCIM) software, optimized for distributed environments, plays an important role in maintaining this foundation for hybrid data center environments with distributed IT infrastructure. In this paper, we first describe the evolution of enterprise IT portfolios and the management challenges that result. We then explain how DCIM software has also evolved and provide real-world examples to demonstrate how DCIM improves resiliency, enhances both physical and cybersecurity, and drives progress on environmental sustainability goals.

Evolution of enterprise data center and IT portfolios

From centralized, on-premise to distributed, hybrid IT

From the 1990s through the early 2000s, for a given enterprise corporation, IT portfolios tended to be contained in a few centralized, on-premise data centers. This changed, of course, when cloud computing and data center colocation providers emerged and became widespread. Today enterprises increasingly have both

[1] https://www.digital-adoption.com/cio-role/

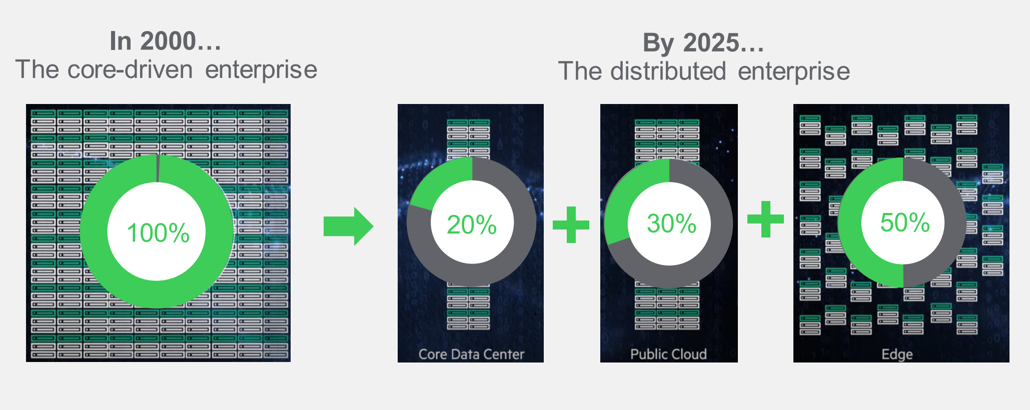
[2] https://mitsloan.mit.edu/ideas-made-to-matter/cio-role-changing-heres-whats-horizon

owned and leased IT physical and virtual assets spread across many more locations. This is referred to as "hybrid IT" or "hybrid computing environments". This growing sophistication complicates operations and maintenance by making it more difficult for CIOs and their operations teams to maintain visibility and control over all assets and view them in aggregate.

This geographic distribution of IT infrastructure and assets is further intensifying due to the growth of critical IT deployments at the edge of networks. Digitalization, the need to reduce network latency, and the desire to reduce network bandwidth costs, are working together to drive more enterprise IT compute and storage capacity deployments at the ends of the network, closer to users. White Paper 226, The Drivers and Benefits of Edge Computing, delves further into this. These edge computing deployments are being done by cloud and colocation providers, as well as by enterprises themselves. Hewlett Packard Enterprise (HPE) predicts (see **Figure 2**) that by 2025, 50% of enterprise compute will be at the edge of the network with only 20% in core, on-premise data centers and the rest in the public cloud[3]. This means the typical enterprise now exists in a very complex hybrid IT environment with power & cooling infrastructure systems and IT assets highly distributed across an increasing number of sites, many of which are small, unstaffed, and operated in a "lights out" fashion.

Figure 2

HPE predicts a highly distributed, hybrid IT environment for enterprises



Note, all of this is further complicated, of course, by the fact that CIOs must also keep track of and manage IT assets increasingly used for work-from-home (WFH) and other remote work scenarios. Although this is generally outside the scope of data center infrastructure management (DCIM) software tools today, and so is outside the scope of this paper, some more advanced residential UPSs are able to collect and report energy information that could be used for sustainability metrics across the WFH population. The additional complication of managing widely distributed WFH IT makes effective software management tools more of an imperative since good tools simplify and automate management tasks.

This complex environment creates unique management challenges for your IT infrastructure management team. **Table 1** lists some of the more common difficulties that arise.

[3] https://www.youtube.com/watch?v=IouhGfmHSZE

Table 1

Common management challenges that result from complex hybrid IT environments that include multiple local edge sites

Challenge	Description & impact
Visibility of multiple, geographically dispersed sites	Inability to see all assets in aggregate and remain situationally aware of what is happening particularly with adds, moves, changes, and security patch/firmware updates. Not knowing aggregate environmental sustainability impact or security status of infrastructure assets.
Lacking on-site staff	Lack of on-site visibility and an inability to respond to problems; Being unaware of who might be accessing equipment. Increased likelihood of unplanned downtime, cost to maintain, and time to resolve issues.
Receiving large numbers of alarms and status change notifications	The need for “eyes and ears” at all locations means potentially thousands of environmental and device sensors are reporting status and alarm notifications. The alarm “storms” can overwhelm users and result in missed critical notifications and wasted effort.
Maintaining a large fleet of dispersed equipment and software	The distributed, “lights out” nature of the smaller sites makes cost-effective maintenance a challenge as it is likely not practical to have trained staff at every site with replacement parts.

These challenges can present themselves in many ways. Here are some examples we have heard…

- Having to calculate the carbon footprint of IT operations
- Trying to remotely troubleshoot a problem with a store clerk or security guard
- Making sense of a storm of “UPS on battery” – “UPS online” alarms
- Getting a call that “something” is beeping or flashing its lights
- Figuring out how to deploy security patch updates to dozens or hundreds of sites
- Servers unexpectedly rebooting at a site while service personnel perform maintenance, but no way to know for sure if they caused it
- Trying to forecast power capacity needs during budget cycle time
- Wondering who is accessing remote IT installations
- Having enough IT staffing resources to manage all these tasks (without software management tools)
- Having visibility into IT infrastructure at colocation sites

Evolution of CIO focus in their traditional role of IT service delivery

There has been a shift in CIO focus and in the management priorities of their operations teams. New management priorities and responsibilities in turn, places new requirements on DCIM software tools today. CIOs must focus more on maintaining resiliency and security in more places, as well as tracking and improving environmental sustainability of IT operations overall. It is not that these topics were unknown or unimportant before, but the complex, distributed nature of hybrid IT along with the enterprise’s increasing dependence on all IT make these tasks more challenging and imperative today.

“Boundaryless data centers” drives need for resiliency everywhere

“The traditional four walls and a ceiling no longer contain the datacenter. The logical datacenter construct now extends to cloud providers, colocation facilities, edge devices, and edge computing. Today’s datacenter exists without clear boundaries, creating growing complexity. The new hybrid computing environment is now much harder to operate as performance, reliability, compliance, and security are all more difficult to manage[4].”

As stated by the quote shown above from CIO.com, as traditional data center boundaries break down, IT operations are occurring everywhere now essentially. And this means that IT infrastructure, *wherever* it is located, needs to be treated more as a traditional data center power and cooling infrastructure would be treated, i.e., as mission critical. As more and more IT service delivery is driven remotely from the edge, the reliability and uptime of those distributed assets becomes more critical to the business. This is not to say, of course, that all IT infrastructure, applications, and workloads have the same level of criticality. But, in general, IT installations found outside the traditional “brick n’ mortar” data centers are just as critical today and, therefore, require improved infrastructure and management practices.

As explained in Schneider Electric white paper 256, “Why Cloud Computing is Requiring Us to Rethink Resiliency at the Edge”, small, remote on-premise IT installations have commonly been seen lacking security and redundancy, with unorganized IT enclosures or racks, and typically run without dedicated cooling or DCIM monitoring. Since any one of these conditions presents a threat to availability, CIOs must address these conditions where they exist. A best practice for mitigating these risks is to deploy IT at the edge using micro data centers. These all-in-one enclosures securely contain servers, networking, and storage along with an uninterruptable power supply (UPS), rack power distribution, cooling, environmental monitoring, and DCIM monitoring. How DCIM itself helps ensure IT resiliency is explained in the next section.

Distributed IT makes security a top concern

Obviously, if critical IT assets are widely deployed outside the confines of tightly controlled and staffed data centers, security is going to be a serious concern. A 2020 IDC survey[5] confirms that it is a top concern for CIOs (**Figure 3**). This worry spans both physical and cyber security. The Allianz Risk Barometer report published in 2022 ranked “cyber incidents” as the top business risk for enterprises today with “business interruption” ranked closely behind in second place.

[4] CIO.com, Don’t be left behind. Dramatic change is impacting datacenters and people

[5] Source: IDC White Paper, Succeeding at Connected Operations with Edge Computing

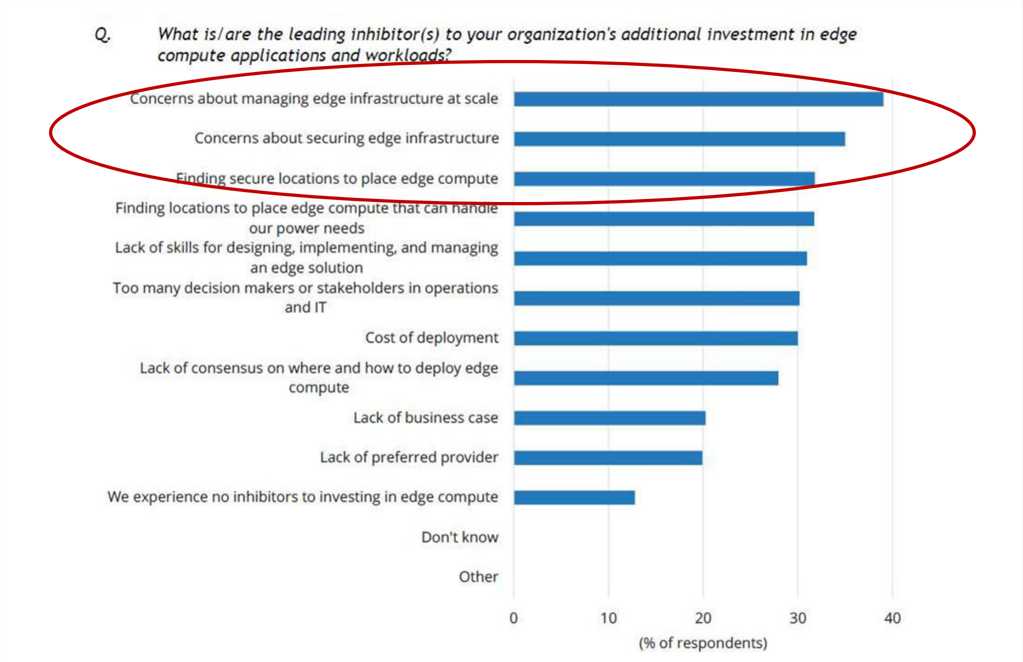


Figure 3

A 2020 IDC survey shows that security of edge IT installations is a top concern for CIOs and IT operations teams.

Compared to highly controlled purpose-built data centers, remote unstaffed IT installations are naturally going to be more vulnerable to having unauthorized people access the installation either intentionally or unintentionally (e.g., cleaning crew plugging vacuum in to a rack plug strip) that leads to business interruptions. So, finding and implementing a secure location for every installation is a challenge.

Also because of hybrid IT, protecting against cybersecurity threats becomes a greater challenge. Larger numbers of network connections that result from decentralized IT installations provide cyber criminals with larger numbers of attack vectors to exploit. The more outside network connections there are, the more security monitoring that must be done, and the greater the likelihood of a human error occurring that exposes a system vulnerability. Security software tools, including DCIM, are required to remotely monitor and automate security best practices as much as possible.

CIOs increasingly asked to track environmental impact of IT

While CIOs and their operations teams are struggling to maintain resiliency and security of their expanding universe of IT, there is growing pressure to track, measure, report, and reduce the environmental impact of their enterprise IT operations. This pressure is coming from governments, investors, customers, and internally, perhaps, out of a sense of having a shared responsibility to address climate change. Schneider Electric white paper 64, Why Data Centers Must Prioritize Environmental Sustainability: Four Key Drivers, explains in detail why CIOs will have to focus much more on this in the future.

However, CIOs are struggling today to answer even the fundamental sustainability questions such as, how much energy does my IT consume and what is the carbon footprint? What can the IT department do alone to reduce emissions? For IT outsourced to the cloud or located in colocation providers, the onus can, to some degree, be put on the vendor to provide data for the relevant metrics. For on-premise IT, however, the CIO will be tasked with collecting the disparate data. While perhaps for some enterprises, this portion might be very small and seemingly inconsequential, for many, CIO owned on-premise IT assets represents a much larger portion of their overall portfolio. A Schneider Electric analysis[6] (**Figure 4**) shows how the share of energy consumed by IT will shift over time illustrating clearly that distributed IT is going to be a bigger sustainability challenge than traditional core data centers (which includes centralized large cloud and colocation data center energy).

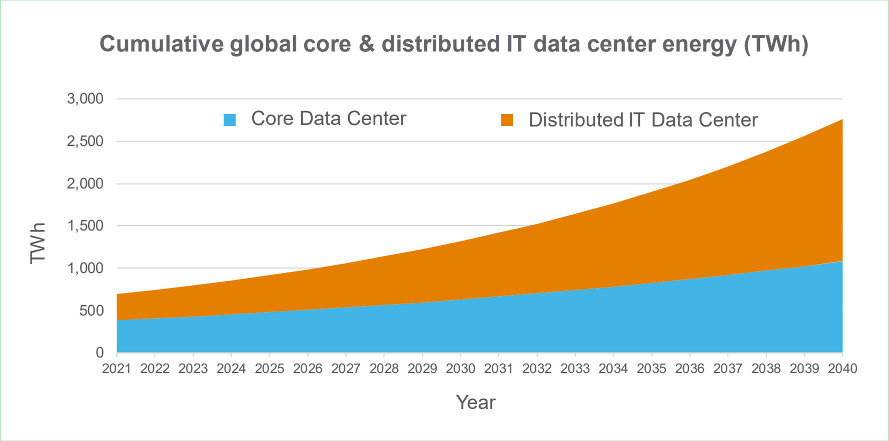


Figure 4

Schneider Electric TradeOff Tool 28, Data Center and Edge Global Energy Forecast, shows what the share of energy consumed by IT could be between core data centers and edge computing sites over time.

How DCIM makes hybrid IT more resilient

Data Center Infrastructure Management (DCIM) software tools communicate with power, cooling, environmental monitoring devices, as well as with other facility and IT management software. DCIM has been fundamentally used to maximize the efficient use of power, cooling, and space resources. Well-implemented, DCIM improves the availability and resiliency of physical infrastructure systems and the IT workloads they support. Most DCIM suites offer 2 core functions:

- **Monitoring & device management** – awareness of device/environmental health and security status changes, trends, and alarms
- **Planning & modeling** – simulating adds, moves, changes; risk analysis, capacity optimization

Both functions work to improve and sustain resiliency of the IT.

How monitoring & device management improves resiliency

Operation of IT equipment – either in a core data center or a remote edge IT site - depends on stable electrical power, sufficient ventilation (or active cooling), as well as a secure location that is safe from unauthorized access or exposure to other physical and environmental threats. These dependencies mean that a highly resilient IT installation requires monitoring and management of the infrastructure equipment with DCIM software tools. This is particularly so for remote, unstaffed sites. You cannot effectively manage something that cannot be seen, after all. Waiting too long to discover there's a problem with the supporting power and cooling infrastructure will lead to business interruption. **DCIM software provides that remote visibility and early warning in conjunction with device and environmental sensors and cameras**. These are summarized in **Table 2** below. White Paper 280, Practical Guide to Ensuring Availability at Edge Computing Sites, goes beyond the DCIM system and describes specific actions to take to improve availability of the power and cooling systems that support small, remote IT installations.

[6] Source: Core & Distributed IT Data Center Global Energy Forecast TradeOff Tool

Table 2

Resiliency benefits of DCIM monitoring and device management functions

Function	Description	Resiliency impact
Device & environmental monitoring	Provides a “read only” connection to all critical infrastructure devices (e.g., UPS, rack PDU, cooling, etc.) – regardless of vendor – to monitor status, access & alarms in real time.	Awareness of status changes, trends, and alarms prevents issues from becoming critical incidents that could lead to IT service interruptions. Monitoring for unauthorized access to equipment reduce physical security risks.
Device management	Provides a means by which infrastructure devices can be configured (e.g., alarm thresholds, communication settings) and their firmware updated.	Configuration & updates ensures equipment performs as expected and helps secure the overall system from cyber security threats.
Asset tracking	Provides a holistic view of all assets, including their location, name, status, etc.	IT resiliency requires having an asset inventory and understanding their attributes and resource dependencies, particularly when conducting maintenance activities.
Data analytics & visualization	Presents useful and actionable information on device status, alarms, and the health of the infrastructure systems and their environment through simple dashboards and reports.	Raw device data, frequent status change notifications, and “alarm storms” can overwhelm users; analytics and clear visualization of data makes DCIM use simpler and more effective to ensure critical alerts do NOT go unnoticed. Predict battery failures ahead of time to avoid unplanned outages.
3rd party platform integration	Allows DCIM data to be shared with a remote monitoring and management (RMM) tool or building management system (BMS) using application programming interfaces (APIs) or an SNMP management information base (MIB).	Managed service providers (MSPs) commonly manage edge computing IT and use their own management platforms; sharing DCIM data with these tools solves “lack of staff” challenge by enabling trusted partners to manage it for you. Ensures visibility even when you do not have the staff to do it.

Particularly with highly distributed IT portfolios, resiliency depends first on using DCIM to monitor critical power and cooling systems and the environmental monitoring sensors that support the IT. Next, we show how DCIM planning and modeling functions improve resiliency to sustain business operations.

How planning & modeling improves resiliency

Hybrid IT environments make for a challenging operations environment given their criticality to business operations. Careful coordination and planning are required between facilities and IT when it comes to adds, moves, and changes. The potential impact on system availability can be so severe that each operational task must be carefully evaluated in terms of its net effect on availability. DCIM planning and modeling modules provide the means to do this careful evaluation.

This function begins with creating and maintaining an accurate map of all infrastructure assets and IT equipment along with their interdependencies with each other. Once setup, the software will map a given virtual machine (VM) to a specific:

- Physical host server and network port
- U space
- IT rack
- Power path(s) (i.e., path A and/or B showing Rack PDU, UPS, PDU, switchgear)
- Cooling units

In 2D and 3D views, DCIM planning & modeling modules will show real-time capacities of all resources (e.g., power, cooling, rack space, network switches, and cabling). Policies can be set down to the workload level to ensure workloads receive the required level of criticality (e.g., the VM can only reside on a host with 2N power redundancy or a UPS with xx minutes of runtime).

By creating, in effect, a "digital twin" (in both 2D and 3D, typically) of your portfolio of data centers and edge IT sites, this DCIM function simulates adds, moves, and changes so that operators understand the potential impacts *before* real action is taken. By first performing actions virtually, the risk of an unplanned interruption in IT service, as maintenance is performed, is minimized. Particularly when there's no on-site IT staff, having this digital visualization of all assets and their interdependencies is important. Note, with all assets fully documented (type, serial number, rack location, network port, power path, etc.) and mapped to each other, this information could also serve as a basis for a disaster recovery (DR) plan.

Imagine needing to "swap and replace" all your remotely located UPSs. With DCIM planning and modeling functionality, you would understand – without being on site - which physical servers, virtual workloads, and applications were dependent on each of the UPSs. Turning the UPS off and switching to a redundant power path could be simulated to understand what the impact would be on connected workloads and applications. Affected critical workloads could be identified and safely migrated to another server or site before the UPS replacement takes place. This information and the ability to run simulations makes it easier to plan and execute the actual transition while reducing the chances of an unexpected outage.

The following bullets summarize some example ways that DCIM planning and modeling functions can improve resiliency of the IT:

- Prevent VMs or physical servers from being moved or added to locations with insufficient power and cooling capacities that could otherwise result in system downtime.
- Be alerted to an unexpected change in power capacity to avoid a sudden outage when the circuit becomes overloaded and trips a breaker.
- Reduce risk of human error during maintenance activities through fault simulations.
- Integrate with virtual machine management software to initiate VM migration once the UPS reaches a low battery state or fault condition to avoid an unintended loss of service.
- Use work order management tools to better ensure critical maintenance is properly scheduled, assigned, defined, and carried through before a failure occurs.
- Simulate a replacement of a UPS to understand what workloads would be affected during the changeover so that they can be moved proactively to a location that meets its requirements.

How DCIM improves security

As mentioned previously, widely distributed, hybrid IT means an increase in the number of networked devices and in overall network connections to the outside world. This increase provides more opportunity for cybercriminals to attempt to breach security measures to access the IT and/or the physical infrastructure systems that support them. In recent years, according to the CyberEdge Group's recent Cyberthreat Defense Report, there has been a 40% increase (over 7 years) in companies that have been compromised by a cyber-attack, going from 61.9% to

86.2% of surveyed enterprise companies[7]. Choosing cybersecurity-conscious vendors, implementing, and maintaining the right technologies and network architecture, along with constant vigilance by the operations team is an imperative today. White Paper 216, Cybersecurity Guidance for Data Center Power and Cooling Infrastructure Systems provides an in-depth framework for preventing the supporting infrastructure managed by DCIM software from becoming a successful target for cyber-attacks.

It is often said that cybersecurity begins with physical security. Particularly for remote, unstaffed edge computing sites, maintaining physical security can also be a challenge without having the right software tools. Given the criticality of the IT, it is imperative for operations teams to secure and control access to the IT enclosures, if not also to the rooms that they are housed in and have remote visibility to the locations where the IT is housed through security cameras.

DCIM software has not traditionally been the tool to turn to for either cyber or physical security functionality. With the development of hybrid IT and edge computing, however, modern, and effective DCIM solutions evolved to incorporate these capabilities. The next two sub-sections explain what those capabilities are.

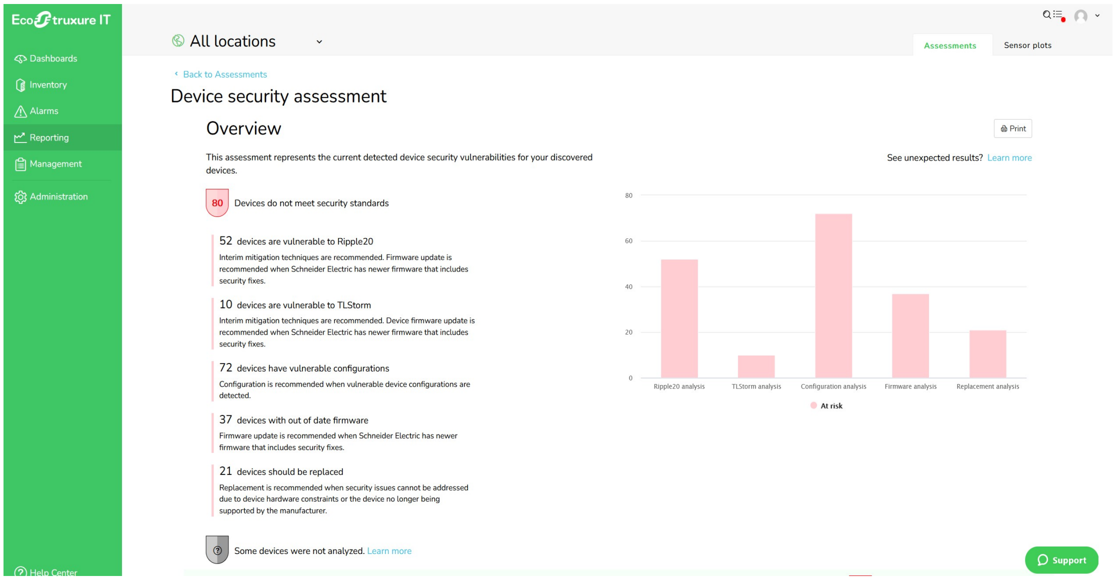
How DCIM reduces cybersecurity risks

Devices monitored by DCIM – ie, Rack PDUs, UPSs, cooling units, and environmental monitoring appliances, etc. - all have built-in network management cards that enable the device to communicate on the network. All of these devices, as well as the DCIM server and gateway 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 devices 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.

The security features and settings that were enabled and configured during the initial setup and installation, also 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 5** can simplify all of this work described above significantly, at least, for power and cooling infrastructure devices. These assessments will scan all connected devices across the entire IT portfolio to provide a report highlighting out of date firmware and compromised security settings. Some DCIM tools will also automate the updating of firmware and provide a means to perform mass configurations of security settings across multiple devices at once to greatly simplify the process.

[7] https://cyber-edge.com/cdr/



‹ Back to Assessments

Device security assessment

Overview

This assessment represents the current detected device security vulnerabilities for your discovered devices.

See unexpected results? Learn more

80 Devices do not meet security standards

52 devices are vulnerable to Ripple20
Interim mitigation techniques are recommended. Firmware update is recommended when Schneider Electric has newer firmware that includes security fixes.

10 devices are vulnerable to TLStorm
Interim mitigation techniques are recommended. Device firmware update is recommended when Schneider Electric has newer firmware that includes security fixes.

72 devices have vulnerable configurations
Configuration is recommended when vulnerable device configurations are detected.

37 devices with out of date firmware
Firmware update is recommended when Schneider Electric has newer firmware that includes security fixes.

21 devices should be replaced
Replacement is recommended when security issues cannot be addressed due to device hardware constraints or the device no longer being supported by the manufacturer.

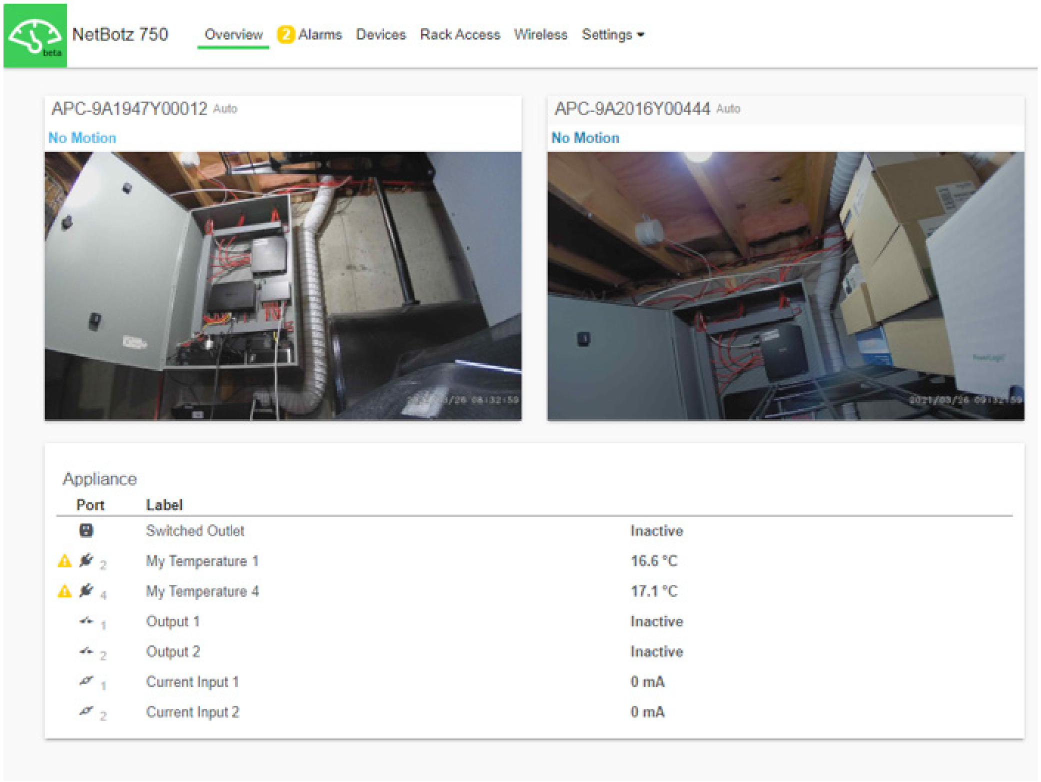
Some devices were not analyzed. Learn more

Figure 5

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 any vulnerable configurations.

How DCIM reduces physical security risks

Data center environmental monitoring appliances can be used to not just detect/track temperature, humidity, fluid leaks, smoke, and vibration, but they also typically integrate with security cameras, door sensors, and access cards. Monitored and controlled through DCIM software, these appliances help remote operations teams monitor and track human activity around critical IT as well as environmental conditions that could equally threaten the resiliency of business operations. **Figure 6** shows an example environmental monitoring appliance and camera system interface as part of an overall DCIM implementation.



Appliance

Port	Label	
	Switched Outlet	Inactive
⚠ 2	My Temperature 1	16.6 °C
⚠ 4	My Temperature 4	17.1 °C
1	Output 1	Inactive
2	Output 2	Inactive
1	Current Input 1	0 mA
2	Current Input 2	0 mA

Figure 6

This is a screenshot of a Schneider Electric NetBotz 750, an example environmental monitoring appliance and camera system, to show how devices like this can be used to monitor and track unmanned distributed sites.

How DCIM helps achieve sustainability goals

Throughout much of the 2010s, the data center industry was very focused on energy efficiency centered around the power usage effectiveness (PUE) metric. Most traditional DCIM solutions offer the ability to report PUE. Although widely adopted, PUE is fundamentally only an energy efficiency measurement of the supporting power and cooling infrastructure for the IT. It does not address greenhouse gas (GHG) emissions, total energy consumed, or anything to do with circularity or land use. A similar metric was developed for water use, called WUE, that has had more limited traction in the industry.

Now that there has been a global shift in awareness and focus on addressing climate change more broadly and with a sense of urgency, the data center and IT industry is responding by making its products more sustainable. This means less embodied carbon, higher energy efficiency, and greater circularity and recyclability of its products and solutions. For enterprise CIOs who are under growing pressure to track and show progress on corporate sustainability goals, this also means that industry vendors should be providing the product information and data CIOs need for tracking and reporting sustainability metrics. Schneider Electric white paper 67, Guide to Environmental Sustainability Metrics for Data Centers, defines a range of metrics for data center and distributed IT owners to strive to measure depending on whether you consider yourself to be “a beginner”, “advanced”, or a “leading” organization in terms of operational maturity.

Referred to as Environmental Sustainability Management (ESM) software, enterprise-level platforms exist for collecting data and reporting virtually all environmental sustainability metrics across an enterprise including energy, GHG (including Scope 1, 2 and 3 emissions), water, waste, and land & biodiversity metrics. These systems rely on data collected from meters, sensors, invoices, and via APIs, from other management software tools, such as DCIM. ESM software then aggregates, normalizes, and presents the data and metrics for reporting and goal-tracking purposes. Effective solutions ensure accurate, auditable, and transparent non-financial reporting of environmental sustainability data and metrics at an overall, global enterprise level.

Metrics and reporting

But for CIOs who are trying to get a grasp of the basics for their domain of on premises data centers, colocation assets, and edge computing sites, modern DCIM software tools can help. Some DCIM (“out of the box”) offers today will collect data and report for individual sites and in aggregate:

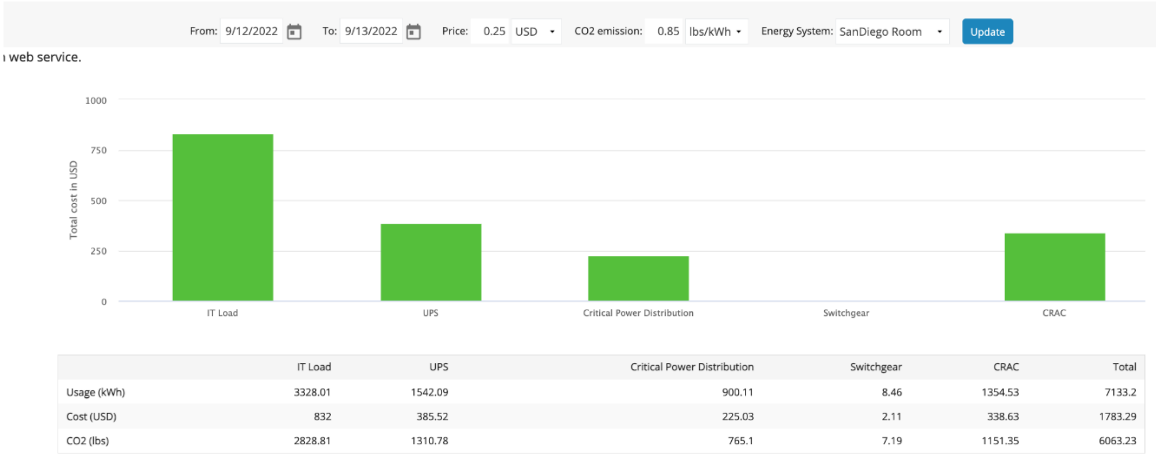
- PUE: current and historical
- Energy consumption: usage at sub-system level to show in both real-time and historical trends of total consumption, IT consumption, and power losses
- Carbon footprint (scope 2 emissions) based on local carbon emissions factors in total and by subsystem including IT, power, and cooling.

For these metrics to be meaningful, of course, it is important for the DCIM software to be able to communicate with and normalize data from all power and cooling infrastructure devices, regardless of make or model. This ensures a complete picture of environmental impact. So DCIM tools and infrastructure devices that embrace common, open protocols (e.g., SNMPv3) and that accommodate the use of APIs/web services should be used.

For CIOs required to track their Scope 3 emissions of the enterprise IT, which is largely the embodied carbon in the IT and supporting infrastructure, DCIM can also help. The first step is to take inventory of what is installed at all sites. DCIM's asset management functionality can be used to map out all devices in data centers or edge IT installations including the IT, networking, storage, power distribution and cooling infrastructure. Embodied carbon data obtained from device manufacturers can be stored as attributes of the devices in the DCIM asset management tool. DCIM can be used to track equipment age to differentiate between new equipment and existing to assist with Scope 3 emissions accounting, as well. Note, some DCIM tools can integrate with IT discovery and inventory software tools (IT asset management, or ITAM) and configuration management database (CMDB) systems which potentially could be used in a similar way to track embodied carbon of all physical assets, including those devices monitored by DCIM.

At the time of this writing, DCIM is in the early phase of its evolution towards becoming an environmental sustainability reporting management tool for data center white space and edge computing, in addition to being a tool for improving resiliency and security. We can foresee DCIM providing the means to collect and report on more of the metrics that are summarized in **Table 2** of Schneider Electric White Paper 67 referenced above. Embodied carbon data of the infrastructure hardware that is documented in an environmental declaration form or product environmental profile (PEP) file could be autoloaded into the DCIM software as new devices are added to the network so that their scope 3 emissions can be properly accounted for more easily. Data related to product end-of-life such as recyclability could also be stored and presented by DCIM software in the future to help with improving circularity.

While standard offers are limited today, some vendors offer engineering services to customize the output of a DCIM system and/or integrate the DCIM software with other data sources (e.g., emissions factor libraries) or platforms (e.g., ESM, ITAM, CMDB software) to address environmental sustainability reporting needs. **Figures 7 and 8** show examples of custom dashboards made to show energy consumption, cost, carbon emissions, PUE, power losses and capacity utilization. And for those enterprises who are using an ESM platform, energy data from your on-premise data centers and edge computing IT sites can be sent from your DCIM software to the ESM tool via an API to provide enterprise sustainability teams with a consolidated view of the impact of your on-premise IT portfolio, for example.



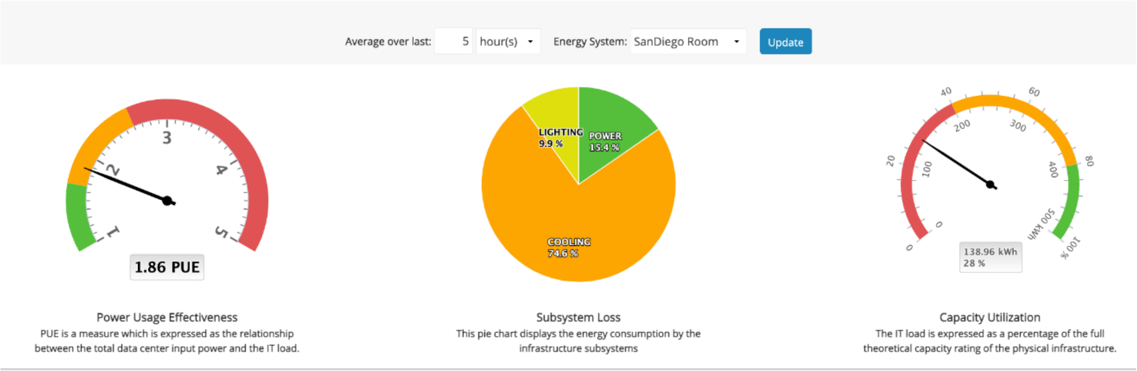
From: 9/12/2022 To: 9/13/2022 Price: 0.25 USD CO2 emission: 0.85 lbs/kWh Energy System: SanDiego Room

ı web service.

	IT Load	UPS	Critical Power Distribution	Switchgear	CRAC	Total
Usage (kWh)	3328.01	1542.09	900.11	8.46	1354.53	7133.2
Cost (USD)	832	385.52	225.03	2.11	338.63	1783.29
CO2 (lbs)	2828.81	1310.78	765.1	7.19	1151.35	6063.23

Figure 7

This screenshot shows an example custom dashboard from Schneider Electric's IT Advisor planning and modeling software that shows energy consumption, cost, and carbon emissions for various infrastructure systems of a data center.



Average over last: 5 hour(s) Energy System: SanDiego Room

Power Usage Effectiveness
PUE is a measure which is expressed as the relationship between the total data center input power and the IT load.

Subsystem Loss
This pie chart displays the energy consumption by the infrastructure subsystems

Capacity Utilization
The IT load is expressed as a percentage of the full theoretical capacity rating of the physical infrastructure.

Figure 8

This screenshot shows an example custom dashboard from Schneider Electric's IT Advisor planning and modeling software that shows the current, real-time PUE, power losses by subsystem and capacity utilization.

Reducing emissions

The use of DCIM in your day-to-day operations can directly serve to reduce energy consumption and, thereby, lower your emissions today. The following bullets list some of the ways this can be done. Note, not all DCIM offers are capable of performing these actions.

- Design energy-efficient floor layouts for expansion/consolidation projects that optimize airflows and ventilation pathways to minimize cooling energy.
- Use built-in computational fluid dynamics (CFD) analysis tools to reduce cooling energy by testing increasing temperature set points, enabling economizer mode, and changing other cooling parameters.
- Take advantage of IT optimization tools in DCIM that monitors server utilization and power consumption at a rack and individual server level to help reduce overall IT energy consumption by avoiding overprovisioning and underutilization.
- Use built-in CRAC/CRAH AI-based optimization tools in DCIM to automatically regulate unit airflow speeds or turn off cooling units when cooling energy is overprovisioned.
- Use DCIM energy consumption data (via rack PDUs) as a department chargeback mechanism to drive more energy efficient behavior.

Put more simply, DCIM functions can be used to better match power consumption to the IT load by turning down or turning off idle infrastructure resources. Or by consolidating the IT load to reduce both IT energy consumption as well as power losses from the supporting infrastructure.

Conclusion

As the role of enterprise CIOs expands to driving business strategy, digitalization, and innovation, their traditional role of IT service delivery remains critical. However, this has become much more challenging as IT portfolios have become more distributed geographically and spread between cloud, colocation, and the edge. IT resiliency and security must be constantly monitored and maintained across their entire portfolio of IT assets. At the same time, there's growing urgency and pressure to track, report on, and improve environmental sustainability. The distributed nature of Hybrid IT portfolios today makes all this challenging to do. Modern DCIM software tools designed for distributed IT environments help address these management challenges. This paper has described in detail how DCIM monitoring & alarming as well as planning & modeling functions serve to make Hybrid IT more resilient, secure, and sustainable.

About the author

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.

Resources

The Drivers and Benefits of Edge Computing
White Paper 226

Why Cloud Computing is Requiring Us to Rethink Resiliency at the Edge
White Paper 256

Why Data Centers Must Prioritize Environmental Sustainability: Four Key Drivers
White Paper 64

Practical Guide to Ensuring Availability at Edge Computing Sites
White Paper 280

Cybersecurity Guidance for Data Center Power and Cooling Infrastructure Systems
White Paper 216

Guide to Environmental Sustainability Metrics for Data Centers
White Paper 67

Browse all white papers
whitepapers.apc.com

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 Energy Management Research 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