BCS

DATA CENTER OPERATIONS

How People, Processes and Technology are Redefining Data Center Operations

By John Hevey

Contents

Reasons Data Center Owners May Not Be Sleeping At Night ... 3
Is the service provider 100% focused on operating data centers? ... 3
Is there a single point of accountability? ... 3
How do they deliver excellence? ... 4
Is the service provider willing and able to show its work? ... 4
How does the service operator impact my bottom-line? ... 4
Strategic Solutions That Will Safeguard Next-Generation Mission Critical Infrastructure ... 5
Strategy 1: Monitor infrastructure using real-time, eyes-on-glass capability ... 5
Strategy 2: Measure for success ... 6
Strategy 3: Manage based on predictive methodologies ... 6
Plan for Eliminating Critical Human Error in Critical Facility Operations ... 7
Can we talk? ... 7
Root causes ... 7
Looking ahead: 5-point plan ... 7
What Every Risk Officer Should Think About in 2021 ... 9
Change of state is predictable failure – capture it and respond swiftly ... 9
Get ahead of future events rather than react to them ... 10

Reasons Data Center Owners May Not Be Sleeping At Night

Published June 29, 2020, Data Center Frontier (datacenterfrontier.com)

The data center industry is on the cusp of the next cycle in its maturation as a business sector. Infusion of capital, a push towards outsourcing, higher density and peaking utilization rates, the disruptive nature of hyperscale companies and further advancement of edge computing are a few of the dynamics that are shaping our industry.

But while business is trending favorably for the data center sector, data center owners are questioning how these changes influence how they can, or more importantly, how they should operate their critical facilities. Paramount of them: What is the primary motivation and mission of my critical facility management provider? Is it protecting and operating my most critical assets, or winning a contract and chasing a financial goal?

According to Uptime Institute's 2019 Data Center Industry Survey, one-third of data centers experienced a service outage in the past year. Gartner has reported the average cost of data center downtime is $5,600 per minute, with another study reporting 70% of all data center and critical facility downtime being attributed to human error. Delta Airlines is still haunted by their 2016 data center outage that grounded over 2,000 flights, cost the company over $150 million and tarnished Delta's image and brand.

In an industry where 100% uptime is the expectation, how do these situations occur and what can owners do to proactively de-risk their data center operations and protect their company? Based on our team's decades of experience both operating data centers on behalf of enterprises and serving as data center operators ourselves, we propose these five questions data center owners should be asking operators to ensure that service provider goals are consistent with their own.

1 Is the service provider 100% focused on operating data centers?

Most data center service providers run multi-faceted businesses, with critical facility management being just one of their offerings. This creates a lack of focus and at times, competing business interests. A service provider who attempts to balance multiple business interests are much more likely to fall short of expectations. The service provider should be dedicated and laser-focused on a single mission: operating and protecting your critical infrastructure. Nothing else should matter.

2 Is there a single point of accountability?

Most critical infrastructure service providers utilize multiple vendors to perform both critical and ongoing operations and maintenance. The result can be a lack of accountability and at times, finger-pointing among providers. A service model that puts subject matter experts (SMEs) as first responders that self-perform the majority of the preventative, corrective and emergency maintenance; optimizes the efficiency of mission-critical facilities. Critical facility management, IT service management, physical security, risk assessments, program audits and professional services should be performed by a single partner using their own trained and certified employees. In essence, a critical facility service partner should operate your data center as if it was its own.

One-third of data centers experienced a service outage in the past year. In an industry where 100% uptime is the expectation, how do these situations occur?

3 How do they deliver excellence?

The constant care and attention required to operate a 7x24x365 mission-critical facility is prompting data center owners to seek long-term partnerships; not just service providers looking to survive the next contract renewal. Ask to see the written playbook that guides processes for administration, operations, reliability centered maintenance, IT service management and physical security. Data center owners should meet not just with salespeople but with the people who will be charged with operating and protecting their mission-critical infrastructure. Data center owners should assess the confidence, passion and dedication to quality that the team brings to the partnership. Do they love what they do? Are they experts in their discipline? Do they understand your goals and are they fully committed to helping you achieve them?

> The best qualified service providers will allow owners to peek behind the curtain to gain total transparency into the people, programs, processes and technology that's used to operate and protect their critical facilities.

4 Is the service provider willing and able to show its work?

Data center owners deserve to be fully aware of the level of care, attention and detail that goes into the operations of their critical facility. The best qualified service providers will allow owners to peek behind the curtain to gain total transparency into the people, programs, processes and technology that's used to operate and protect their critical facilities as well as how those resources are applied to benefit the customer. The customer should be able to drop in and inspect operations at any time for any reason. The service provider should be able to explain what it is doing to proactively deliver higher performance and additional efficiencies.

5 How does the service operator impact my bottom-line?

Data center owners that rely on multiple vendors to manage and operate their critical facilities can have a direct impact on the owner's bottom line and overall cost of ownership. Margin-stacking, mark-ups on outsourced services and inefficient use of staffing can impact operational costs by over twenty percent. A service provider should be motivated to improve total cost of ownership and take a performance-based approach. The service provider should be able to set fixed operational costs that enable the facility owner to meet forecasted operational costs and budgets without sacrificing service delivery.

The mission-critical facility operations model is at an inflexion point. Data center owners are in a position to take the lead on influencing where the industry goes next. Data center owners can sleep well at night knowing that their critical facilities are in good hands. But it starts with asking the right questions.

Strategic Solutions That Will Safeguard Next-Generation Mission Critical Infrastructure

Published August 5, 2020, Data Center Frontier (datacenterfrontier.com)

In a COVID-19 world, most companies in America are constantly challenged to rethink their business models and operate in new ways. A search for normalcy may be avoiding the realities of the situation. The "next normal" will be much different from anything we have seen or experienced.

Mission-critical infrastructure is not immune to this reality. Uptime Institute's 2020 global data center survey highlights factors showing the urgency of rethinking data center operations and looking at how and who is operating and protecting your critical infrastructure. Chief factors include:

- 78% of survey respondents cite having a power outage in the past 12 months. Of that group, 75% stated the resulting downtime was within their power to have prevented.
- Hardware refresh cycles are getting longer, putting increased pressure on asset management, maintenance methods and staff capabilities.
- Critical facility management of resiliency, business continuity and downtime varies widely, pointing to the need for rapid adoption of industry best practices.

So, what is a data center owner to do? BCS recommends three strategies that create a framework for critical facility operations in uncertain times.

Strategy 1: Monitor – Develop and execute systems and methods to provide active, real-time monitoring of critical infrastructure.

Strategy 2: Measure – Establish a business intelligence ecosystem that measures key performance indicators that drive efficiency, resiliency and overall performance of your critical infrastructure.

Strategy 3: Manage – Rethink your current management program to move beyond the traditional preventative mindset, to one that is more predictive.

Following are descriptions of these strategic solutions along with practical approaches owners can take to mitigate risk, decrease total cost of ownership (TCO) and chart a positive course for their critical facilities and infrastructure.

Strategy 1: Monitor infrastructure using real-time, eyes-on-glass capability

Effective monitoring starts with situational awareness of the diverse systems, physical infrastructure and human resources that align with operating and protecting your data centers. The best monitoring solution combines trusted people, proven processes and leading technology into one integrated approach, creating both top-down visibility and bottom-up real-time awareness.

Too often, what is intended as a lights-out critical facility, does not have the advanced telemetry or a remote visibility in place to protect it against loss of customer service, credibility and reputation.

Best industry practices for effective monitoring use purpose-built, business intelligence systems, combined with deploying tactical, eyes-on-glass, remote monitoring capability for maximum visibility and 24/7, real-time operational incident management.

Too often, what is intended as a lights-out critical facility, does not have the advanced telemetry or a remote visibility in place to protect it against loss of customer service, loss of credibility and loss of reputation. Here's a case in point:

The Company: A large telecommunications provider serving a Top 5 metropolitan city.

The Incident: A transformer serving a hub aggregation facility failed during a thunderstorm on a Friday evening. Back-up systems responded as designed, moving to an onsite generator to assume the critical load without interruption.

The Problem: No one knew the generator had assumed critical load until it ran out of fuel on Sunday, instantly shutting down video, voice and data services for hundreds of thousands of customers — right before kickoff on the NFL's opening weekend!

The Recommended Solution: Within minutes of losing utility power, a tactical response could have been initiated using eyes-on-glass, active monitoring of site telemetry. The site outage could have been prevented.

Measuring key aspects of your critical infrastructure starts with a clear, concise understanding of the key performance metrics that most impact the tactical operations of your facility.

Strategy 2: Measure for success

Since you "can't manage what you don't measure", you need to focus on what — and how often — to measure key aspects of your critical infrastructure. This starts with a clear, concise understanding of the key performance metrics that most impact the tactical operations of your facility.

Once key metrics have been established and measurement systems are put in place, owners and operators need to benchmark current performance against each metric and develop operating levels that will govern future management of the facility.

Similar to monitoring, there are several industry best practices, including instituting a metrics-based approach that allows an operator to move to a structured, predictive maintenance strategy and decrease a reliance on reactive-based, corrective practices.

Strategy 3: Manage based on predictive methodologies

To go beyond prevention toward adopting an effective critical facility management program based on predictive methodologies requires four steps:

1. **Ensuring transparency around the measurement of key metrics.**
2. **Conducting regular and open dialogue among key stakeholders using a monthly business review showing metrics performance against stated goals.**
3. **Detailing specific actions required to continue proper performance and impact areas of improvement.**
4. **Prioritizing those actions and identifying individuals accountable for them with an expected timeline for completion.**

Instituting critical facility monitoring, measurement and management will create a framework and a roadmap for data center owners and operators to follow that will lead to certain success in these uncertain times

Plan for Eliminating Critical Human Error in Critical Facility Operations

Published August 26, 2020, Data Center Frontier (datacenterfrontier.com)

Can we talk?

Once again, Uptime Institute's Global Data Center Survey reports the high likelihood, disturbing frequency, and increased damage caused by data center outages. Findings from 2020 show that 78% of organizations say they had an IT-related outage in the past three years. 75% of organizations say their most recent incident could have been prevented with better management or improved processes, making the vast majority of outages a result of human error.

Let that sink in. Three-quarters of the outages that took place over the last 12-months could have been prevented, yet we're not talking about it. We seem to accept that number.

To put this in perspective, what if the commercial airline industry had a 75% human error failure rate? Thankfully, this is not the case. The aviation industry promotes strict discipline, engineered process, a checklist regimen, and a predictive and preventative approach as a foundation for operational rigor.

The mission-critical industry is accountable for operating and protecting some of the world's most vital workloads in some of the most complex critical facilities in the data center ecosystem. 100% availability of critical IT applications is the de facto performance standard.

Yet, Uptime Institute reports that the industry achieves this less than 25% of the time, with most failures associated with human actions and behaviors. It's time for a paradigm shift for the mission-critical industry — one that changes the human error statistics.

Root causes

Why do critical facility outages still happen, and why have human error failure rates remained flat? This article is not an assault on hard-working, intelligent, and dedicated data center engineers. Failure analysis routinely exposes underinvestment in people, processes and technology necessary to operate mission-critical facilities in the manner in which they were designed.

Key Findings

- More significant outages are becoming more painful
- Operators admit that most outages are their fault
- Power problems are still the most significant cause of major outages

Disasters do happen; (most) outages, however, should not. On the surface, outages look the same, affecting access and availability of applications, systems, and services. However, if we look behind the curtain, we can see areas where we can prevent outages and increase overall availability. At BCS, we believe the path forward lies in closing gaps in process, training, and resources.

Organizations should adopt and embrace a playbook as the foundation of their operations program model; one that is site-specific and able to scale based on changing business demands and infrastructure needs.

Looking ahead: 5-point plan

1 **Create and improve operational procedures and documentation.**

Despite the broad availability of established standards and best practices from Uptime Institute, NFPA, ISO, IEEE, and OSHA, many people accountable for the reliability of mission-critical environments are not applying them in a unifying framework.

Organizations should adopt and embrace a playbook as the foundation of their operations program model; one that is site-specific and able to scale based on changing business demands and infrastructure needs. Doing so will introduce a strict, operational discipline that will help eliminate human errors.

2 Institute training as part of operational DNA.

Data center operators have historically struggled with training. Some operators talk about it, few actually do it, and even fewer do it well. Comprehensive training must be a foundational element of any good critical facility operations program.

Critical facility training best practices include:

- Develop training programs that apply to specific, site-level assets and systems
- Institute a skills assessment program that identifies gaps in skill and knowledge
- Increase team preparedness through the continuous execution of drills using site-specific emergency operating procedures (EOPs)
- Leverage a variety of industry accreditation and certification programs

3 Establish continuous improvement and risk mitigation programs that target human behaviors.

Next-generation operators have developed programs designed to infuse a continuous improvement rigor to proactively eliminate operational risks. Program examples include:

- Find anomalies, flush out what drives the anomaly and engineer plans to fix the anomaly before it becomes intrusive to normal operations. A Find, Flush, and Fix program approach is a systematic method of identifying deficiencies to systems issues before they become problematic.
- A Near-Miss Program encourages transparent reporting and open discussion about incidents that could have happened but were identified and remedied before they did. The ability to debrief as a team and talk about a near-miss is the height of program maturity.

> Most owners are moving towards working with a dedicated, single-source operations provider that is committed to self-performance of maintenance and operations.

4 Consolidate operations into a single-source, self-performance operations model.

Original Equipment Manufacturers (OEMs) complement any good mission-critical program and add value for their proprietary knowledge, firmware updates, and annual required preventative maintenance. However, OEMSs are not invested in the day-to-day success or long-term performance of your facility, especially those which lack the formal training and discipline to work in mission-critical environments.

A reliance on numerous vendors creates operational risk. Most owners are moving towards working with a dedicated, single-source operations provider that is committed to self-performance of maintenance and operations.

5 Operators must adopt a stewardship mindset.

Data center owners entrust their critical IT environment, assets, and services to individuals. These individuals must adopt a stewardship mindset that puts the operation and protection of the critical environment and the services delivered as their top priority.

What Every Risk Officer Should Think About in 2021

Published December 28, 2020, Data Center Frontier (datacenterfrontier.com)

This year's global pandemic has forced organizations to challenge conventional wisdom, alter business practices, and try to define a new normal. The data center and critical infrastructure industry is no exception. COVID-19 and its impact on our work forces and communities has motivated data center owners and operators to dust off their business continuity and contingency capabilities to test their effectiveness. Let's be honest — no one was fully prepared for what 2020 had to offer!

To date, real time operational reviews and tweaks have minimized risks for many operators. But what lies ahead, may prove to be a larger challenge and more threatening. In fact, circumstances are converging to create a period of increased operational risk — a perfect storm that needs to be prioritized and addressed with the correct risk mitigation strategy.

On a macro-level, the environment for this approaching storm is influenced by an increased reliance on outsourcing to cloud solutions, increases in digital and mobile technologies, increased workloads, and the rapidly changing complexity of today's data center infrastructure.

Is your organization susceptible to this perfect storm? If you are a Risk Officer, ask yourself these questions:

- Is your organization seeing large increases in capacity utilization?
- Do you have tech debt or heavily leveraged, aging infrastructure?
- Have you deferred preventative or corrective maintenance, or planned infrastructure CAPEX improvements?
- Have you experienced employee attrition, or been asked to reduce staffing levels in the last 12-months?
- Is your strategy to shift toward lights-out management?
- If you experience a workload outage, do seconds and minutes make a difference — versus hours?

If you answered 'yes' to any combination of these questions, I encourage you to continue reading. If you've answered 'no' to these questions, are you assuming too much good? Out of sight and lack of visibility to a site's risks should never be out of mind.

Change of state is predictable failure – capture it and respond swiftly

Change of State is a core tenant of our physical world. For the human body, change of state is essential to our existence (e.g. our ability to convert oxygen into our blood system) and a warning sign of something that needs our immediate attention (e.g. a spiked temperature). When systems work well — life (literally) is good. When systems fail, things can go very bad rather quickly.

Most traditional data center operations do not have centralized resources and systems dedicated to the detection, reaction, triage, response and timely mitigation for reporting on operational changes of state.

Most organizations manage and prioritize change of state when it comes to applications and digital environments. It's our experience, however, that most organizations don't place the same level of scrutiny, rigor and discipline around the data center physical environment where their most critical workload assets and applications reside.

Today's critical infrastructure is an increasingly complex and sophisticated environment comprised of interconnected systems. While traditional data center operations have some disparate systems to report on operational changes of state; most do not have centralized resources and systems dedicated to the detection, reaction, triage, response and timely mitigation of such anomalies. A proven approach that can immediately identify and respond to a change of state, is often referred to as eyes on glass.

Case in point, a nightshift Data Center Engineer is performing maintenance at 1:00 am. At the same time, a critical failure within the heat-rejection system occurs, triggering an email alert. The Engineering Team doesn't immediately see the email (and may not until much later in the shift) resulting in cascading thermal concerns within the data center environment. What required immediate attention and response, didn't get it.

> What is missing in our industry — and within most distributed organizations — is centralized command-and-control to see the big interconnected picture and the potential for cascading failures.

Let's look at a non-data center analogy. The pilot of a commercial airliner flying at 39,000 feet has the ability to fly, control and monitor waypoints between Kansas City and Dallas. An air traffic controller sees that the aircraft has unexpectedly changed altitude. The change (of state) doesn't correspond with the flight plan or the last instructions from Air-Traffic Control. An anomaly has occurred and triage and action are required to respond and resolve the anomaly and return things to normal. What is missing in our industry — and within most distributed organizations — is centralized command-and-control to see the big interconnected picture and the potential for cascading failures.

Get ahead of future events rather than react to them

Today's data center owners and operators need to see the approaching storm, quickly respond to rapidly changing conditions, and address gaps in incident management when changes of state occur within the critical facility. What's needed are solutions that extend detection and response capabilities by aggregating telemetry and correlating multiple data points in real-time to enable timely and effective incident response.

Next-generation operators (BCS Data Center Operations included) combine people, processes and technology through a centralized, single-source deployment solution that leverage:

- Centralized, 7x24x365, eyes-on-glass visibility into critical facilities and physical operations
- Trained surveillance and ITIL certified analysts that constantly monitor critical environments, looking for and analyzing change of state data
- Purpose-built, computerized maintenance management systems and business intelligence capabilities
- An extensive operational playbook to guide real-time incident response actions, communications, root-cause analysis, post-incident action and reporting

With this approach, data center owners and operators can mitigate known (and unknown) operations risks at their data center, with their workloads, and their businesses.

About the Author

John Hevey, CTDC, CTIA, CDCP, DCIS; Vice President, Corporate Technical Service at BCS Data Center Operations

John has spent his entire professional career operating, protecting and servicing mission-critical facilities, including leading the operations division for BCS; being responsible for enterprise data center facility operations for a leading financial services company, and heading critical infrastructure and strategy for 207 Time Warner Cable critical facilities. See more on LinkedIn.

About BCS Data Center Operations

BCS is an enterprise-level critical facilities operations company focusing exclusively on data centers. The BCS solutions portfolio includes facility management, IT services, physical security and a range of value-added professional services through one fully integrated self-performance model. BCS serves the needs of Fortune 500 companies, including three of the nation's leading financial service providers.

For more information visit bcsdatacenteroperations.com or follow BCS on LinkedIn.

BCS
DATA CENTER OPERATIONS