Plan for Eliminating Critical Human Error in Critical Facility Operations

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.

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