

What Every Risk Officer Should Think About in 2021

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.

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.

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.

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 bcsgroup.com/data-center-operations or follow BCS on [LinkedIn](#).