DATA CENTER BRIEF

Your Monitoring System may be Failing You

Many data center monitoring systems are not as effective as they could be typically due to how they were deployed and/or the lack of on-going governance.

How long ago was your monitoring system installed? Was it thoroughly commissioned post installation? When was the last time you audited it? Are you getting the best use out of it? As the vital view of your data center's health, this is one of the most important tools to support data center resiliency. Here are some aspects to consider.

What do you have, and has it kept up?

Is the current state of your system documented? Do you have a points list for each critical system? Are the points sufficiently described? With respect to your generator(s), are there monitoring points for fuel level and battery health? Is your ATS not in auto transfer mode? [Remember your service tech puts it in manual during every PM]. Are there new systems that have been installed that are not monitored? Are there systems that have never been monitored but should be? How about monitoring the handholes on your property so you know when the telecommunications provider accesses them?

Single source of truth during incident reconstruction!

Incidents typically involve more than one system. Reconstructing what happened when there were various times on each systems' clock is challenging. [check each system's clock and you will see the variety]. If all systems report to a single monitoring system, alarms will report in the sequence they occurred. This could save hours reporting results as well as increase your confidence level.

Single pane of glass

There have been significant improvements enabling systems to communicate with each other. Many manufactures now have pre-built gateways or APIs. Check with your vendor to see what interoperability features they now offer.

Improve operational activities

Monitoring systems can automate activities. Automatically close your fresh-air intake dampers during generator runs. Produce and send out specific reports at predetermined intervals to designated people. Auto notifying the appropriate service contractor of critical alarms can save precious minutes.

Firmware updates

Do not overlook the value of keeping firmware current - new features, corrected deficiencies, etc. But take normal update precautions. Have the vendor provide you documentation of changes and determine how the updates be tested post-installation. What is the Method of Procedure (MOP) for implementing the update and is it specific to your site? Make sure you have a back-up copy in case you need to roll back.

Security

You have likely read stories about hackers "entering" via a monitoring system. Does your service contract have a provision in it that the manufacturer of the system must notify you in 24-hours once they become aware of a security deficiency or weakness?

About DCBs and the Author

Data Center Briefs are designed to stimulate expand your thinking. We hope that then generates additional thoughts on this topic. Tad Davies is a 34-year veteran of the data center industry. He advises on Business Centric issues such as consolidation, provider selection, and build vs. buy and Facility Centric issues such as risk assessment, planning, cost modeling and owner's representation. Tad is President of Fodere LLC which provides data center consulting guidance. Tad.Davies@FodereConsulting.com www.FodereConsulting.com