TOPIC BRIEF

ASSESSING CRITICAL INFRASTRUCTURE RELIABILITY FOR UNSEEN DATA CENTER FACILITY RISK

By Kaniel Tilow, Benjamin Kosbab

21 JULY 2021

Critical businesses—from finance and networking to water and electric utilities—have robust digital infrastructure systems that rely on a vast network of data centers and internet exchange hubs to deliver essential online services. These facilities can be housed and managed on site or outsourced to external colocation centers, and vary greatly in size and complexity. Our reliance on these digital backbones to underpin business services is rapidly expanding across all sectors of daily life. In today's technology-driven world, a business's financial well-being depends on the continuous operation of these facilities' assets—triggering significant investment to maximize digital infrastructure reliability and downtime.

Failures to these facilities can potentially devastate network performance and cause painful business disruption consequences to end users. When assessing a digital network's vulnerability, physical damage to, or degradation of, the facility housing these digital assets can get overlooked. This includes inherent construction defects, poor building enclosure design, inadequate structural system performance following building repurposing, or countless other problems. Although rare, water leakage, wind damage, and other natural and human-made hazards can lead to failures in cooling, power, or other auxiliary systems, which in turn can nullify any digital redundancy and IT backups credited for strong digital network reliability. To avoid these types of costly business interruptions, it is critical to assess the state of the physical facilities that house these digital assets.

DIGITAL NETWORK RELIABILITY: ONLY A PARTIAL SOLUTION

Digital businesses often measure service availability, or "uptime," by what they call the number of nines. Business delivered without interruption 99.9% of the time is "three nines" reliable; 99.999% has "five nines" reliability, and so on. When business interruption is costly, data owners maximize the number of nines, and their uptime, through robust and often redundant digital networks. However, this digital redundancy does not tell the whole story.

Determining the number of nines for a facility generally credits functional performance of the physical facility housing the digital assets. This inherently neglects the probability of unacceptable performance of the physical facility—however small it may be—in quantifying network availability. Actual network availability requires the facility to perform its design function. Facility performance is probabilistic in nature and depends on a number of variables, including when the facility was constructed, to what building code or standard it adhered to, and with what original purpose in mind. For example, an office facility built in the early 1990s to conform to the Uniform Building Code of the era may now have a reliability in 2021 of less than two nines when adapted for data center use (e.g., potentially 97% reliability depending on structure type). So, claiming an uptime of three or four nines for the digital infrastructure housed within that facility is overly optimistic.

> The vulnerability of physical facility performance can be overlooked when quantifying the network reliability of business-critical digital infrastructure, potentially overstating the underlying performance claims of digital availability.

MINOR FACILITY FAILURES WITH MAJOR CONSEQUENCES

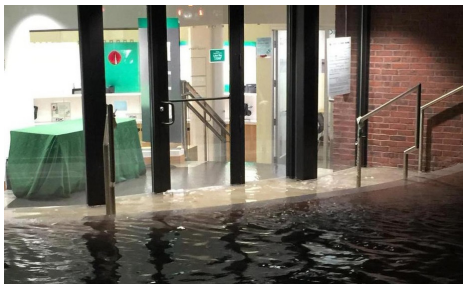
Business owners may not immediately recognize the business interruption consequences of their reliance on these digital systems until they go down. Facility and data owners occasionally tolerate some likelihood of failure based on a backup or redundant unit elsewhere but credit a potentially vulnerable electrical component or other physical mechanism to activate the redundant system.

Vastly different hazards can affect business-critical facilities depending on their type and location. For example:

- A repurposed, decades-old high-rise building in an urban setting may have water leaks associated with haphazardly installed cooling fans.
- A cooling failure initiated by poorly anchored, roof-mounted equipment subjected to a high wind event could lead to degrading thermal conditions and equipment damage.
- A lightweight facility with a large footprint in a rural setting may be situated in a newly recognized floodplain.
- Water leakage, even if far from servers, could occur near power supply equipment or corrosive materials and lead to an electrical failure.
- A facility with an outdated fire-protection system could fail to contain a fire that breaks out in the Uninterrupted Power Supply room.


Roof-mounted equipment subject to exterior elements


Metallurgy and corrosion evaluation of deterioration caused by water leakage


Flood damage from severe rainfall event

WHAT CAN BE DONE?

Business owners and facility managers can partner with experienced engineers to implement risk-based methods to identify high-value, proactive facility upgrades that significantly improve performance at a fraction of the potential cost of lost business due to network interruption. A tiered, three-phase approach to identify, evaluate, and mitigate physical vulnerabilities can help reduce risk to a tolerable level: Phase 1 casts a wide net to identify potential vulnerabilities, Phase 2 zeros in on the top risk contributors, and Phase 3 mitigates risk and enhances reliability.

Phase 1: RAPID SCREENING

- **Identify** physical vulnerabilities driving risk
- **Review** available documents, conduct initial site walkdown, interview risk manager
- **Assess** facility construction criteria, drawings, and operating experience

Phase 2: ASSESSMENT AND PRIORITIZATION

- **Evaluate** conditions by conducting detailed site visit, develop capacity evaluations and fragility calculations, perform non-destructive evaluation and extreme hazard assessment
- **Determine** the most impactful physical vulnerabilities (vs. most physically damaging) by using logic modeling to understand relationships of facility systems and components
- **Develop** conceptual enhancements and modifications to improve facility performance and reliability

Phase 3: MITIGATION AND ENHANCEMENT

- **Mitigate** potential hazards
- **Scope** upgrades, select contractors, oversee facility modifications
- **Design** and implement upgrades and modifications

HIGH RETURNS ON MITIGATION INVESTMENTS

The vulnerability of physical facility performance can be overlooked when quantifying the network reliability of business-critical digital infrastructure, potentially overstating the underlying performance claims of digital availability. Seemingly nominal adverse facility conditions can have a large impact on network performance and the business services it supports. A path is available for experienced engineers to help proactively mitigate the possibility of unacceptable performance by identifying and implementing value-added facility upgrades. Preemptive mitigation can have a comparatively outsized benefit, especially when business interruptions to critical operations are severe and costly.


Kaniel Tilow, P.E.
770.635.6703
kztilow@sgh.com


Benjamin Kosbab, Ph.D., P.E.
770.635.6702
bdkosbab@sgh.com