The Key to Boosting Network Resilience? It's in the Data.

Data-driven insights reduce network downtime and repair costs.

By Gordon Smith / *Sagent*

If enterprises didn't fully appreciate the importance of their networks at the beginning of 2020, they do now. The emergence of COVID-19 and the shutdowns that followed led to traffic spikes of up to 70 percent and put large network operators front and center in the eyes of businesses and consumers.

Today, companies of all sizes remain dependent on collaboration technologies, cloud services, remote access and other solutions – all of which rely on the network.

Unfortunately, 2020's myriad challenges followed a period of reduced investment in network infrastructure. According to a Global Network Insights Report from NTT, by 2019, almost half (47.9 percent) of businesses' network assets were aging or obsolete, up from 13.1 percent in 2017.

Enterprises are, in many cases, reaping the network failures they've sown through inattention. Opengear reports that nearly one-third (31 percent) of companies lost at least $1 million to network outages in the past 12 months. Network engineers and IT teams are becoming more and more concerned about network resilience as downtime increases in both frequency and cost.

It must be said, there's no problem with incorporating older networking equipment, assuming appropriate maintenance and life cycle assessments are in place. To the contrary, rushing to upgrade to the latest hardware – such as hurrying to adopt network automation and other advanced systems – threatens to bypass the most effective and affordable means of boosting network reliability to meet the moment. The best results come when organizations first reduce avoidable repairs.

AVOIDABLE OUTAGES PLAGUE NETWORK OPERATORS

I'll share the bad news first: Approximately one-third of network repairs performed are completely avoidable. I have seen this across numerous clients and industries. Trucks roll, field technicians diagnose equipment as faulty, the hardware is removed, and we receive it for repair. Repeatedly, we find that there is nothing physically wrong.

This has a huge impact on downtime. In the best-case scenario, a spare is immediately installed when the purportedly failed hardware is removed. In the worst case, network gaps remain while a replacement is obtained, and a technician returns to make the fix. Either way, if a component critical to network function goes down, network reliability probably takes a hit until field services arrive.

A variety of issues contribute to the prevalence of unnecessary repairs. They run the gamut from misconfiguration to inadequate technician training on equipment to ineffective life cycle management strategies. And there can be variation by product manufacturer and model, installation location, the group of technicians serving an area, and even the weather in a particular region. Think Minnesota's cold winters or Arizona's hot summers and the impacts on product life span.

With the large array of factors, hardware failure patterns can be lost in the noise, leaving network operators to resolve issues on a case-by-case basis. This is less efficient than systemic interventions and doesn't empower the organization to steadily improve resilience.

Greater leverage can be achieved with appropriate hardware failure data analysis, but the necessary information collection and business intelligence tools are surprisingly rare. These features are not part of traditional network analytics solutions. There are, however, options available in the third-party maintenance market, or systems can be built by a network operator determined to be more resilient than the competition. Here are the outlines of such a solution.

ADDRESSING HARDWARE FAILURE

To get a better understanding of network performance and stay ahead of potential issues, service providers should focus on three key areas when analyzing and responding to hardware failures:

- **Collect data.** The first necessity is information about network equipment failures. A large proportion of network operators do not catalog basic data on hardware sent in for repair, such as part number, installed location, technician responsible for on-site triage, failure reported by the originating technician, and diagnosis and root cause analysis by the repair facility. By tracking as many data points as possible, network operators increase their ability to identify patterns.

  A key barrier to such data collection is typically maintenance vendor relationships. Field support partners frequently avoid sharing such information, as it could reveal shortcomings in their own technicians, reduce the perceived value of their maintenance service, or increase their own data management burdens.

  For these and other reasons, most hardware maintenance providers purposefully obscure the diagnoses technicians arrive at in their repair facilities, and original equipment manufacturers (OEMs) can be similarly closed-mouthed about the results of warranty returns. The best response is for network operators to select vendor partners with full transparency policies in place or work to negotiate desired reporting mechanisms as part of the next contract renewal with existing providers.
- **Analyze across multiple variables**. With data in hand – preferably within a powerful business analytics tool – it's time to dig in. A purpose-built analytics system will provide a wealth of reporting features designed to highlight common causes of avoidable downtime.

  If you're building from scratch, on the other hand, a good starting place is to look at repair facility diagnoses to identify cases in which no physical repair was necessary. Then evaluate those incidents by part number, region, technician group and so on. This will tend to point to problems in configuration, on-site troubleshooting and patch application, which have potentially systemic remedies.

  Another fertile investigation is relationships between the OEM, product, age and location specifics and particular failures. This can help drive efficient life cycle management and maintenance strategies, enabling the organization to upgrade or maintain equipment often enough to reduce predictable downtime but not so frequently as to waste resources.
- **Target top priorities.** Avoidable downtime comes in various forms, and addressing all issues at once is impossible. Enterprises and network operators should prioritize their responses to initial findings based on total impact, including downtime and cost considerations. Considering the ease of implementing a solution is also helpful.

  As an example, if a spate of configuration problems appears on a particular Cisco switch in a particular region, there may be a training issue with one team. Perhaps the manual is confusing, and word of mouth among these technicians has spread an inaccurate interpretation of a certain step. Once this shortcoming is identified, it is relatively easy to develop a quick configuration guide or offer additional training. As configuration accuracy increases, the organization will gain substantial return on these modest investments.
- **Continue to refine.** As the most common and easily resolved causes of network outage are eliminated, network operators can start focusing on more isolated issues and those with longer-range response opportunities, such as shifts in network hardware acquisition choices and life cycle management adjustments.

  This is not, however, a linear process. Every new equipment deployment can raise problems in product reliability, warranty recalls, training issues and so on. Most organizations will, therefore, experience a staggered evolution. Impressive front-end savings and resilience improvements will generally be followed by increasingly narrow interventions alongside occasional large-scale troubleshooting when widespread failure patterns again emerge.

The job of hardware failure analysis is never done, but it does get easier with time. Custom-built tools can be improved, people leading the charge become more adept at noticing patterns, and remedies become more effective based on previous experience. With sustained effort, the organization will find itself with far fewer avoidable repairs and associated outages. And with millions of dollars in downtime costs along with brand reputation and customer loyalty at stake, there is good reason to grab for these attainable resilience gains right away. ❖

Gordon Smith is the CEO of Sagent, which provides advanced business analytics and support services to lower the costs of network ownership and the risks of downtime.