opengear
A DIGI COMPANY

RESEARCH COMMENTARY

The many costs of downtime – Why minimizing outages must become a higher business priority

Despite recent and significant investment in digital infrastructure, the prevalence of serious network outages continues to rise. Future-thinking businesses have already begun a migration to the cloud, that coupled with the advent of 5G, and the growing prevalence of connected devices and the Industrial Internet of Things, are making networks more widely dispersed and more complex. A constantly connected ecosystem is critical to building a bridge between organizations, their technology and their customers.

The migration of workers to home environments following the pandemic exacerbates both these trends. This adds vulnerabilities into the network and makes misconfigurations and cyber-attacks more likely, leading to a greater risk of downtime. According to Uptime's 2022 Data Center Resiliency Survey, 80% of data center managers and operators have experienced some type of outage in the past three years – a slight increase over the norm, which has fluctuated between 70% and 80%.

However, the same research found that the proportion of outages costing over $100,000 has soared in recent times. Over 60% of failures result in at least $100,000 in total losses, according to the report, up from 39% in 2019. The share of outages costing upwards of $1 million increased from 11% to 15% over that same period. A 2020 Opengear survey, which polled 500 senior IT decision makers, found that the top four causes of outages at the time were software/firmware upgrade; cyber-attack, human error and fault in network device – and all four are likely to remain key today.

This eBook looks at **the scale of the challenge with downtime** we are facing today; the **extensive impacts** outages can have on business from financial loss to loss of reputation. It then goes on to consider why it takes some organizations extended periods of time to **identify and then resolve issues**. Finally, with reference to network automation, why NetOps and out-of-band management are solutions that can be leveraged to to **help businesses quickly resolve issues.**

CONTENTS

FAR-REACHING IMPACTS ARE CLEAR

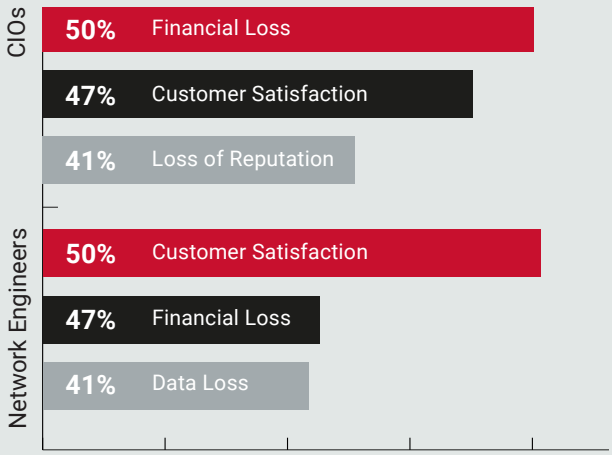
A global study conducted by Opengear in 2022 underlines just how far-reaching the downtime challenge is. In the survey, which polled the views of 500 network engineers and 500 CIOs, separately, 50% of CIOs ranked financial loss among the main impacts on their business due to network outages over the past two years. But the monetary impact is far from the only cost to businesses.

CIOs also reference customer satisfaction (47%); data loss (45%), loss of reputation (41%); loss of business opportunities/market competitiveness (35%) and SLA pay-outs (24%). Network engineers in contrast, rank customer satisfaction as the biggest impact (51%) with financial loss second on 29% and data loss third (28%).

The top priorities have remained similar over the past two years. In Opengear's 2020 poll of senior IT decision-makers, 41% referenced customer satisfaction among the main impacts on the business of network outages over the previous 12 months compared to data loss (34%) and financial loss (31%).

These topline survey findings don't take into account the less widely measured but nevertheless undeniable fact that outages can also have a significant impact on every organization's most valuable asset – their staff. The stress of coping with an outage and its aftermath can be all-but-unbearable for service staff having to deal with unhappy or angry customers. More specifically, downtime can really take its toll on engineers facing long journeys to investigate outages, followed by a battle against time to get systems up and running again.

Top 3 Impacts of Downtime for CIOs & Network Engineers



NEEDS TO BE A RAISED PRIORITY

For all these reasons and more, there is a clear understanding of the need to avoid downtime. In the Opengear survey, more than a third (36%) of network engineers said 'higher levels of downtime' were among the biggest risks to organizations from not putting networks at the heart of their digital transformation.

Moreover, 37% of engineers ranked 'avoiding downtime' among their organization's biggest networking challenges post digital transformation. It was second only to security in the list. 35% of CIOs concurred, although among this group five other challenges including skills shortages, network agility and performance are higher ranked.

The low position given to avoiding downtime in the priority list among CIOs is a concern given the shortcomings of many approaches to addressing outages after they have occurred.

In the Opengear survey, more than a third (36%) of network engineers said 'higher levels of downtime' were among the biggest risks to organizations from not putting networks at the heart of their digital transformation.

TIME AND COST - PAYING THE PRICE FOR OUTAGES

All the evidence suggests that outages are increasing, and it is taking longer for businesses to recover from them. 52% of network engineers say their organization has seen an increase in the number of network outages experienced over the past two years.

91% say their organization sometimes sends network engineers out to site to fix networks in person, with 42% in total saying that they do this for the majority of outages and downtime. This has been a real issue during the ongoing pandemic but it also results in huge costs to businesses in terms of travel and hotel bills; and, especially for global organizations, mean time to recovery (MTTR).

The survey reveals it is taking businesses an average of 11 hours to find and resolve a network outage after it has been reported. This was a significant problem even before the pandemic, with 38% of senior IT decision-makers polled by Opengear in early 2020 saying it was taking their organisations more than the length of one working day on average to find and resolve a network outage after it has been reported.

But it has become worse – the average in 2020 was 9.39 hours, nearly two hours faster than it is today.

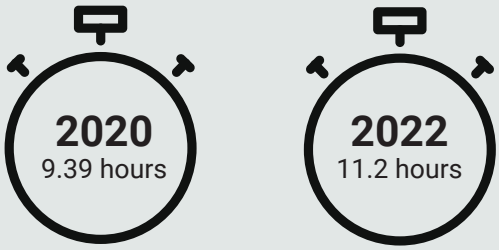
More than one in ten organizations in the 2022 survey (11%) say it is taking them more than 24 hours on average to do this. Moreover, the survey also reveals that engineers on average take 3.6 days fixing networks (including travel time to site, time fixing network and travel time back from site) when the company suffers a network outage.

Against this backdrop, Mean Time To Recovery (MTTR)is rising. Over the past two years, 52% of network engineers polled had seen an increase in the MTTR of their business customers. That compares with just 7% who said they had seen a decrease.

In terms of monetary cost to businesses 20% of CIOs polled stated that network outages have cost their business over $1 million over the past two years and for 3% of this group the costs escalated to over $25 million.

MTTR (Mean Time To Repair) has ramped up since 2020 by almost 2 hours. Main Impact is on companies' finances and reputations.

Average time taken to find and resolve a network outage:



RESOLVING ISSUES

Network outages are on the increase and so too is the time taken to resolve them. There is a lack of preventative planning. Too many businesses still rely on manual ways of working, sending engineers out to site and relying on manual methods of documentation.

So, what's the way forward? Preparation is key. It is vital that when disruption occurs, companies have an IT business continuity plan that enables them to recover quickly. They need to ensure their network is resilient. Every CIO needs to know without question that when trouble strikes for whatever reason, – whether it's a hurricane or a cyber-attack, a local power outage or a global pandemic, their network will be ready to deal with it.

One priority must be ensuring businesses have visibility and the agility to pivot as problems occur. Many are not proactively notified if something goes offline. Even when they are aware, it may be difficult to understand which piece of equipment at which location has a problem. To solve errors, an organisation might need to perform a quick system reboot remotely. If this does not work, there may be a problem with a software update or other significant issue.

That's where *Smart* Out-of-Band Management using an alternative path into the network really comes into its own. Relying on the main production network to access a corporate network in the event of a network outage is dangerous because when an issue occurs, an engineer may not have access to that production network.

To ensure networks get up and running again quickly when outages occur, *Smart* Out-of-Band Management provides secure, remote access to an organization's critical devices, helping ensure business continuity. Paired with Failover to Cellular, companies have the bandwidth necessary to continue business operations while diagnosing and remediating the issue. Devices can be rapidly reconfigured remotely without the need for deploying anyone on site – which has been an especially crucial consideration over the past two and a half years given the travel restrictions in play through the COVID-19 outbreak.

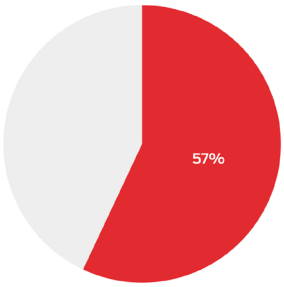
Having access to a separate, secure management plane, in the form of an out-of-band management network, ensures remote access to remediate even during an outage, whether caused by a cyber-attack, a misconfiguration, or a network cable being cut in error, for example.

However, bringing more automation into the network will also be key. Again, this often starts with an independent management plane, which has a key role to play in automating common network operations (NetOps) processes. The keynote of NetOps is its versatility. It can be there on Day One, enabling the deployment process to be managed via a centralised management software and ensuring network equipment can effectively self-configure. It is there for the standard day-to-day process of keeping the network running but it can also be to provide an alternative route to remediate the network when it has gone down. NetOps supports rapid resolution of network outages.

In the past, if a particular event had happened on the network, most companies would expect an engineer to log in, run through five or six routines to work out what was happening and then remediate the problem.

What NetOps does is automate that entire procedure so that when that event happens, the system automatically runs through those five or six steps. If that resolves the problem, fine. If not, the issue is escalated to the network engineer to manage the next level of troubleshooting. All this simplifies the process. But it also removes human error because so many downtime incidents are simply caused by someone pushing a wrong configuration or typing in the wrong letters when they are sending commands. By using a NetOps approach to correctly program an automation routine, an organisation can effectively remove these challenges.

A focus on Netops and network automation processes is key to success. 57% of CIOs highlight a reduction in downtime among the benefits of network automation.



57% of CIOs in the most recent Opengear survey highlight a reduction in downtime among the benefits of network automation. Companies around the world recognise that the ability to operate independently from the production network and detect and remediate network issues automatically can dramatically improve security, save time and reduce costs. At a time when most businesses are focused on doing more with less, that's absolutely critical.

With outages still on the up both in terms of prevalence and the average pecuniary loss incurred, organiztions need to ensure that their networks are resilient. A combination of out-of-band, automation, and NetOps will ensure they are building a bridge to the future – ensuring they're in an optimal position to meet growing needs.

SURVEY METHODOLOGY

The global study, which covered the US, the UK, France, Germany and Australia, polled 500 CIOs in total (100 in each region) and 500 network engineers (100 in each region), with separate but complementary sets of questions.