RESEARCH COMMENTARY

Measuring The True Cost Of Network Outages

The network and its efficient operation are vital to the success of almost every organization operating today. Whenever it is not available, productivity drops off, the business is financially impacted and its reputation suffers. And yet trends like remote working and virtualization, while they help drive business flexibility and productivity, may also make the network more vulnerable both to breakdown and to attack.

As the IT industry has become more virtualized, with the ongoing migration to the cloud, the rise of connectivity and the emergence of the Industrial Internet of Things (IIoT), the network becomes more complicated and onerous to manage. As more people work from home (a trend likely to be accelerated by the current coronavirus crisis) or connect remotely while off-site, it becomes more widely dispersed. Taken together, these developments make it more important that the network is kept up and running but also more likely that outages will occur.

WHY DOWNTIME HAPPENS

Organizations are adding layers of complexity to networks and that often results in more vulnerabilities. Today, we are seeing a raft of factors that can cause network or system outages – from ISP carrier issues to fiber cuts to simple human error. Added to this, network devices are becoming increasingly complex. That can make achieving robust network security more difficult.

As software stacks have to be updated more often, they become more vulnerable to bugs and cyber-attacks. On the one hand, there is a risk of external attacks by cyber-criminals intent on exploiting weaknesses in the corporate network, or external bots constantly looking for vulnerabilities that enable them to penetrate corporate networks. On the other, there is a growing threat from business employees themselves. The causes are just as diverse as the risks - from disgruntled employees who deliberately open the doors to cyber-criminals to good-faith users who are victims of phishing attacks.

Finally, the ongoing expansion of networks to encompass edge computing has led to increased compute being pushed to the edge e.g. last mile services like Netflix etc., and more complex equipment being put in place in remote locations, where there are no IT staff, and where redundancy is not feasible. In such scenarios, it is no longer sufficient simply to design a robust data center. The network is only as strong as its weakest point – and the proliferation of edge computing therefore requires a new way of thinking about the network.

Taken together, all this is driving up the level of network outages. In a recent independent study of 500 senior IT decision makers commissioned by Opengear and carried out by OnePoll, more than half (51%) of respondents said their organization had had four or more outages lasting more than 30 minutes in the past year. Indeed, nearly one in five (18%) said they had experienced seven or more such outages in the previous 12 months. Added to this, nearly two-thirds (65%) of respondents said the number of outages experienced by their organization had increased over the past five years..

The prevalence and length of downtime is also having a significant financial impact on businesses. Nearly one in three (31%) of senior IT decision-makers globally said network outages had cost their business over $1.2 million over the past 12 months and one in six in total (17%) said it had cost them $6 million or more. Moreover, fewer than one in ten of the sample (8%) were able to claim that these outages had cost them nothing at all over that time period.

NEEDING A RAPID RESPONSE

Compounding the difficulties they face, these outages are often challenging to resolve quickly. 38% of the research sample said it is taking their organizations more than the length of one working day on average to find and resolve a network outage after it has been reported.

Lack of planning is one issue. More than half (59%) of organizations surveyed have not implemented a preventative maintenance program to minimize downtime. With many running dispersed networks, it is unsurprising 41% of respondents to the survey list ‘travel time in getting engineers on site’ among the top two challenges they face in resolving a network issue quickly. Given the time taken to resolve network outages and the costs incurred, finding a solution that addresses these has become an urgent priority.

WHY RESILIENCE IS THE SOLUTION

Given all the challenges listed above, we are today seeing a growing focus on a concept known as network resilience. But what exactly do we mean by this, why does it matter and how can it best be achieved? There are a raft of different definitions.

According to Joshua Sanders, Lending Tree: “Network resilience for me is a drive to minimise downtime. And if the network does go down, having a way to get to it and not having to travel to the actual site to repair the network.”

Chris Weindel, Eldorado Resorts, added: “Network resilience means how quickly you can get back up after an outage. Right? The out-of-band network is our last line of defence. We hope to never use it but we’re glad we have it when we need it.”

In our view at Opengear, network resilience is the ‘the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.’ We see that as our official definition, which then also translates to our ‘shorter view’: ‘the ability to withstand and recover from a disruption of service’. One way of measuring it is how quickly the business can get up and running again at normal capacity following an outage.

Whatever the exact definition, most people are clear that true network resilience cannot be achieved by providing resilience to one single piece of equipment, whether that be a core switch or a router. Instead, it is important that any solution for resilience can plug into all equipment at an edge site or data center, map what is there and establish what is offline and online at any time.

One priority must be ensuring a business has visibility and the agility to pivot as and when problems do occur. Consider a large finance or healthcare enterprise with a network operations centre (NOC) that may require constant uptime for applications and customer service. They may well have several branch locations spread across the world with attendant time zone issues. As a result, they may struggle to get visibility that an outage has even happened because they 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 if nobody is on site to physically inspect.

SCOPING OUT THE ROLE OF OUT-OF-BAND AND NETOPS

To solve errors, an organization might need to perform a quick system reboot remotely. If this does not work, there may be a problem with a software update. That's where the concept of Out-of-Band comes into play. The traditional in-band network involves managing devices through the common protocols such as telnet or SSH, using the network itself as a media. Out-of-Band (OOB) management provides a wholly separate layer to the network which is why it can access and remediate quickly any affected equipment if the system is locked – especially important, for example, in a cyber-attack.

Network problems, like the software update issue highlighted above, can therefore be addressed by utilizing the latest *Smart* Out-of-Band (OOB) devices because an image of the core equipment and its configuration, whether it be a router or switch, for example, can be retained, and the device can be rapidly reconfigured remotely without the need for deploying anyone on site – an especially crucial consideration today given the travel restrictions in play around the current coronavirus outbreak.

If an outage did occur, it is also possible to deliver network resilience via Failover to Cellular™. This would allow critical services in the business to keep up and running while the original fault was remotely addressed, even while the primary network was down.

Though incorporating extra resilience through OOB costs money, the ROI can significantly exceed the expense. This alternative access path may only be used by an organization occasionally. However, when it is needed, it becomes a critical success factor. It's also worth considering that resilience is usually much cheaper than having to buy large amounts of redundant equipment. This is increasingly true as the deployment of edge locations grows. Though it may be feasible for an organization to purchase redundancy at a core data center, that same redundancy can't be built in each and every rack or data closet at a remote, small location.

The study identified time savings (referenced by 45%) and cost savings (41%) as the top two benefits to organizations from having a solution that could operate independently from the main in-band network; that could detect and remediate network issues automatically.

To solve errors, an organization may need to perform a quick system reboot remotely. If this does not work, there may be a problem with a software update. Luckily, this can also be addressed by utilizing the latest *Smart* OOB™ devices because an image of the core equipment and its configuration, whether it be a router or switch, for example, can be retained, and the device can be quickly reconfigured remotely without requiring the deployment of 'smart hands' on site.

Beyond ensuring an ironclad backup solution with tools like *Smart* OOB management and Failover to Cellular, organizations can provide further protection and achieve cost saving by stacking tools like NetOps automation on top of solutions for secure, offsite provisioning. This can eliminate a lot of repetitive tasks, remove potential for human error, and free up time. In line with this, 43% of the study sample said they were 'increasing the level of automation across the network' to drive up network resilience within their organization. Significantly also, 89% of respondents to the survey who had introduced a NetOps automation approach said that it had made their organization's network more reliable.

MOVING BEYOND THE IN-BAND TO ADDRESS THE NETWORK DOWNTIME CHALLENGE

Network downtime is a major issue for most large enterprises. Outages are prevalent and they cost businesses time, money and result in reputation loss. Yet, there is a lack of preventative planning, and businesses often spend significant sums getting the organization up and running again, not least in terms of getting engineers out to remote sites.

A solution capable of operating independently from the main in-band network and detecting and remediating network issues automatically is of huge value in this context. A strategy based on network resilience, supported by *Smart* OOB management, and within the context of a NetOps automation approach has to represent the best way forward.

SURVEY METHODOLOGY

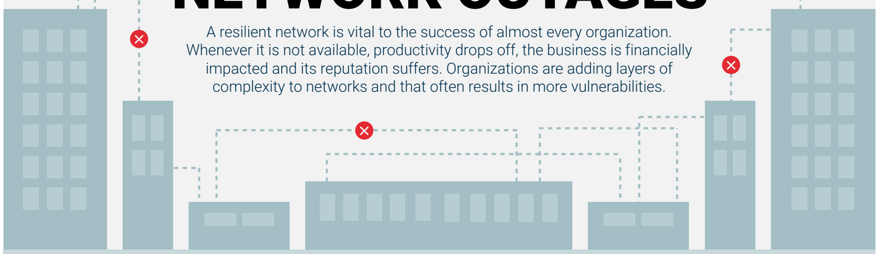
The data is based on a survey of 500 Senior IT decision makers located across North America and Europe. The survey was commissioned by Opengear, and conducted by OnePoll, a member of AAPOR, in January 2020.

opengear
A DIGI COMPANY

MEASURING THE **TRUE COST** OF

NETWORK OUTAGES

A resilient network is vital to the success of almost every organization. Whenever it is not available, productivity drops off, the business is financially impacted and its reputation suffers. Organizations are adding layers of complexity to networks and that often results in more vulnerabilities.



A recent global study* of Senior IT Decision Makers, commissioned by Opengear, discovered:

31%

have **lost more than $1 million** in the past 12 months due to network outages

83% stated network resilience is their top priority ! #1

23% reported a **25% or more increase** in network outages in the past 5 year

39% of network outages took more than one day to resolve

42% stated **engineer travel** is the most common challenge in remediation

Companies around the world recognize that the ability to operate independently from the production network, **to detect and remediate network issues automatically can dramatically:**

improve security by	save time by	reduce costs by
48%	**45%**	**41%**

Deploying a network resilience solution that addresses these is an urgent priority

Make the Resilient choice - Get *Smart* Out-of-Band by Opengear