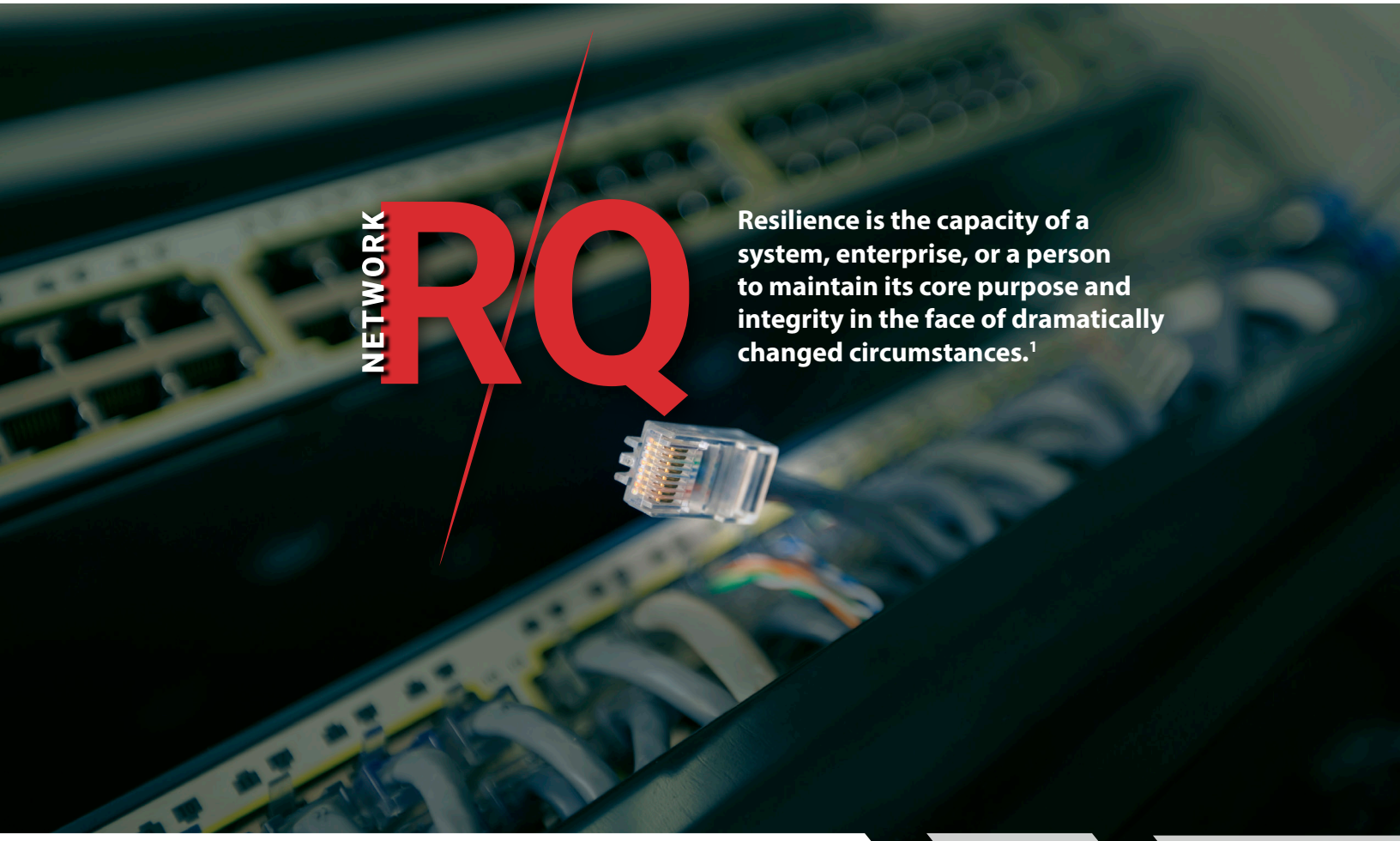
opengear
A DIGI COMPANY



Resilience is the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances.[1]

WHITE PAPER

Building Network Resilience

Your network is the backbone of your entire business. When it's not available, work stops, the company loses money, data security may be at risk, and the very reputation of your resilient network.

Consider network resilience as a competitive advantage. Resilience helps you to prevent data losses, minimizing damage while allowing you to continue doing business. Resilience will also allow your company to attract more customers, partners, and investors, who are becoming much more selective when picking vendors and partners.

In this paper, you'll learn what network resilience is and why it matters, why you should worry about your network's availability, and how you can achieve true network resilience.

WHAT IS NETWORK RESILIENCE?

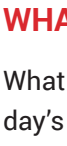
What do we mean when we talk about resilience in today's virtualized network world?

Network resilience is the ability to withstand and recover from a disruption of service.[2] One way to evaluate your network resilience is to measure how long it takes for your company to resume normal business operations after a failure is resolved. Many considerations go into the building of a resilient network, including backup and recovery strategies, disaster management, and redundant elements.

WHAT CAUSES OUTAGES?

System outages can result from a variety of factors which can include human error, environmental conditions and network elements.

ISP carrier issues, fiber cuts and cable interconnects are just a few network elements that may cause potential problems. Network devices are increasing in complexity. As software stacks require frequent updates, they become more susceptible to bugs, exploits and cyber attacks causing more outages.



REDUNDANCY IS NOT THE SAME AS RESILIENCE

It's important to understand the difference between resilience and redundancy. While a resilient network may contain some redundancy, a redundant system isn't necessarily sufficiently resilient.

A redundant system duplicates some network elements so that if one path fails, another can be used. For example, you may have duplicate routers or network connections from two different providers. But this doesn't mean that your network is resilient. Resilience considers the full ecosystem, from core to edge, whereas redundancy removes a single point of failure.

And redundancy is expensive. If your company has two separate data connections for network redundancy, you would want to use both connections rather than paying for a connection that is idle 99% of the time. If there is a failure, your network cannot be considered to be resilient when it is now only handling half as much traffic.

1. Andrew Zolli and Ann Marie Healy, Resilience: *Why Things Bounce Back* (New York: Free Press, 2012), 6, Kindle ed.
2. Ray A. Rothrock, *Digital Resilience* (AMACOM, 2018)

WHY IS NETWORK RESILIENCE IGNORED?

Your network may experience a failure for lots of reasons. In case of failure, your network should be able to bounce back quickly. True network resilience is more than having data backup or redundancy. Resilience is being able to get your network operating at normal capacity, sometimes even before resolving the cause of disruption. And yet many organizations neglect to consider resilience when designing and building their networks.

There are two big reasons that resilience is left out of a network:

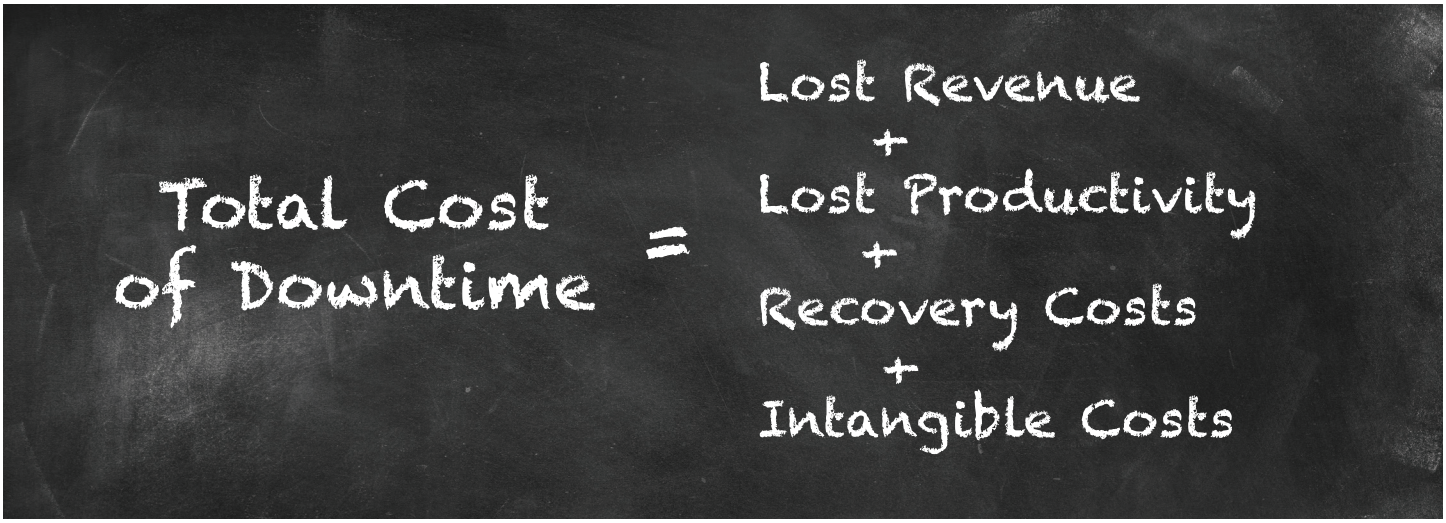
- Designing a resilient network is expensive and time consuming and often overlooked. The importance of resilience may not be appreciated by an organization and financial resources are not allocated for it.
- Few companies have the expertise to design a resilient network from the beginning. And if the network is already in place, it's much harder to add resilience. Network design also needs to focus on the future resilience requirements as well as current ones, something many businesses neglect to consider.

WHAT IS THE TRUE COST OF A NON-RESILIENT NETWORK?

Building in resiliency does cost money, but it also more than pays for itself over the long term. By being resilient, your company will save thousands of dollars in revenue when something brings down your network.

While there is pressure to limit networking expenditures, the actual cost of ignoring network resilience is much higher than the expense. By not building in resilience, companies actually end up increasing their operating costs. According to ITIC's 2017 Reliability and Hourly Cost of Downtime Trends Survey[3], 98% of businesses with at least 1,000 employees say that, on average, a single hour of downtime per year costs them more than $100,000 and 33% report that an hour of downtime costs their company $1 million or more.

And beyond the direct monetary damage, downtime hurts your company's productivity. On average, any interruption takes you 23 minutes to refocus on your work.[4] You also need to factor in recovery costs and less tangible losses, like damage to your organization's reputation.



3. Information Technology Intelligence Consulting conducted a survey, ITIC's 2017 Reliability and Hourly Cost of Downtime Trends Survey
4. Gloria Mark; Daniela Gudith; Ulrich Klocke (2008). *The cost of interrupted work: more speed and stress.* CHI '08 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 107–110.

ENSURING NETWORK RESILIENCE IN THE CLOUD

The parts of your network that interact with cloud-based services are not in your control. You need to make sure your data is safe and secure by asking questions of your cloud vendor, including:

- What happens in case of data loss and what is their downtime history?
- What steps do they take to protect your data in the real-world data center? Is their core location secure from threats, both human and environmental?
- What certifications do they have?
- How does their virtual network connect with the physical hardware? Are there any "last mile" vulnerabilities you should be aware of?

Pop Quiz

In the diagram below, the virtual server is up. The DNS service is down. What business issues does this disruption cause?

a. Customers cannot get to your ordering website
b. Employees cannot get to your email server
c. External Emails will not be delivered
d. Internal VoIP traffic will stop working
e. Internal File services will stop working

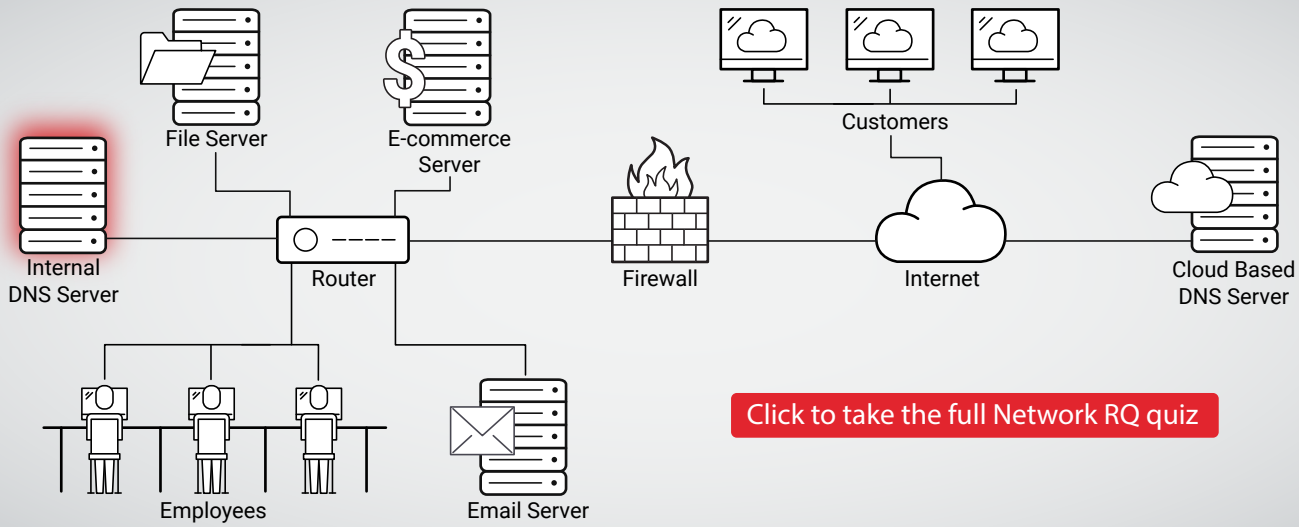
Answer bottom of next page

WHAT IS THE LAST MILE?

Cloud services are a core part of many retail businesses. And while connectivity has improved over the past few years, one weakness these services can't overcome is the last mile problem.

The last mile is the final segment of the WAN network that connects your network to any cloud services. These last miles are the weakest links in your connectivity.

All of the network traffic for a single office, store, branch, or distribution center is funneled through single links. The bandwidth of these links effectively limits the amount of data that can be transmitted to your ISP. This bottleneck leaves you exposed to DDoS attacks and basic human error leading to outages. And this last mile is vulnerable to physical issues. An accidental fiber cut can knock out your entire network and leave you disconnected from cloud services for significant periods of time.



Click to take the full Network RQ quiz

7 STEPS TO BUILDING ENTERPRISE-WIDE NETWORK RESILIENCE

Here are a few steps you can take to increase the resilience of your organization's networks:

- Start by assuming that your network is vulnerable and figure out where those weaknesses are likely to be found.
- Determine the average cost to your business of a network outage to justify any additional capital expenditure.
- Lead the push to increase resilience to keep your business thriving.
- Use network modeling software to create a map of your entire network and all connections. Keep it up to date and use it to identify potential weaknesses and points of failure.
- Try to build resilience in a way that protects the entire network rather than focusing on specific hardware devices. Pay attention to everything from the core to the edge.
- Deploy resilience features such as strategic redundancy, alternative routes, and segmentation of operations in all business processes.
- Create awareness of Network Resilience at all levels of your organization.

GETTING SUPPORT FROM TOP LEADERSHIP

Senior management has to lead the effort to protect your network. As an important step to getting buy-in from your company, you need to make sure that your company leadership considers and can answer these questions about the reliability of the business network:

- What network vulnerabilities can we prevent?
- What can we not control?
- What is the potential cost of a network outage?
- What can we do to manage and mitigate the risk we decide to accept?

When approaching management, treat network resilience as you would any issue that impacts the whole business enterprise. Plan and budget resilience as a positive business asset.

NETWORK RESILIENCE IS CRUCIAL TO YOUR COMPANY'S SUCCESS

As companies rely more and more on interconnected networks, virtualized cloud services, and edge and Internet of Things (IoT) technologies, the potential for downtime increases and the costs of outages will continue to rise. And when network services are unavailable, productivity stops. True network resilience is achieved when you focus on maintaining your services, removing single points of failure, and having a plan to bring your network back up to continue normal operation.

Your network is your business. Outages have a direct impact on your organization's bottom line and network resilience is crucial. The most important things you can do are to find out what downtime costs, get buy in from management, and build resilience into your network both for today and the future.

Answer: A & C