Akative™

The Ugly Truth About Internet Downtime

Whitepaper

Akative™

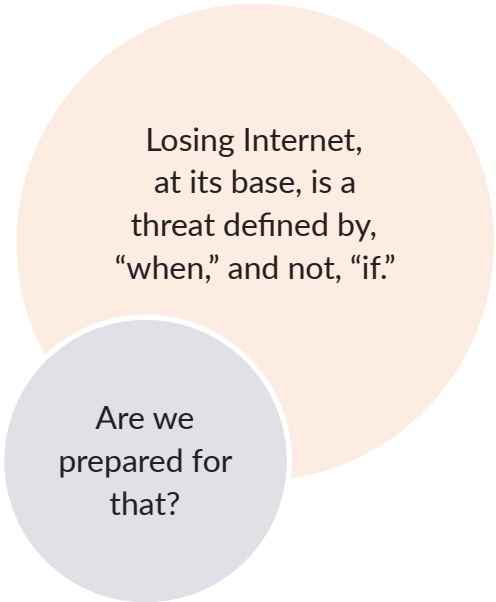
Table of Contents

The Ugly Truth About Internet Downtime

Introduction

Worldwide news provides a daily opportunity to evaluate business continuity plans for organizations from a sole proprietorship in a community of two thousand all the way to the Chief Information Officer of an international conglomerate. Natural disasters, social and political unrest, and the pervasive threat of terrorist attacks dominate the topics trending in the global consciousness and supply the next, “Are we prepared for that?” question to answer. It is sometimes easier to see the large threats, the frightening events where actual survival might be in question, due to their magnitude, but how well is your business continuity plan designed to handle the everyday threats you are more likely to face?

Precious little business happens without an Internet connection. Your Point of Sale, when offline, reduces spending to the cash in a customer’s pocket. The very same customer might comparison shop via WiFi connection, which is demonstrably more difficult without a WiFi connection. Customer service via VoIP, chat, and e-mail grinds to a halt. And what about your remote locations? How can you determine how they are faring when you don’t have the Internet available to monitor them?



The simple fact is virtually every business process requires Internet connection, and yet, even with a study from the Aberdeen Group stating 78 percent of respondents to a survey will suffer four or more Internet outages each month, many businesses do not include Internet failover within contingency planning[1]. No other threat to business continuity is comparable to the frequency with which Internet disruption occurs, and few provide opportunities of equal proportion to determine the immediate impact of neglecting to include failover solutions.

The purpose of this white paper is to detail the ways connection to the Internet can fail, list the financial impact of the failure events, discuss how organizations can add Internet connection failover to business continuity plans, and present the solution organizations can add to prepare themselves for the eventuality of losing connection without losing customers.

65 percent of organizations require an entire hour or more to resolve each individual Internet connection disruption.

Internet Connection Threat

A discrepancy exists between Internet service providers (ISPs) claims of 100 percent redundancy, thereby guaranteeing 100 percent uptime, and the study by the Aberdeen Group indicating three of four organizations experience four or more Internet disruptions per month. The 100 percent reliable Internet service claim lulls organizations into a false sense of security when 65 percent of organizations require an entire hour or more to resolve each individual Internet connection disruption. How does the Internet go down?

The fiber used in the Internet backbone as well as from ISPs to the organizations they serve can be cut accidentally by the person digging a posthole without having called for locate services or in coordinated attacks on Internet cables as occurred in San Francisco in 2014-2015[2]. The physical climate where an organization resides presents unique challenges be they lightning strikes, earthquakes, flood, or hurricane, all of which can damage and disable the infrastructure connecting the organization to the Internet. Regardless of cause, when the fiber breaks, it will take time to identify where the cut occurred and send crews to repair the damage.

Sorry, Cash Only!

Routers exist as a potential failure point and is one ISPs cannot always control as some routers reside outside the ISP infrastructure, and some outages are planned to service the device. The router's age and whether firmware updates are installed could bring the router to the failure point. An attack could occur, which would not only put data in danger but also the viability of the router itself. The solution could be something as simple as a reboot or as involved as purchasing and deploying a new router to the LAN, but regardless of ease, the solution will take time.

Lost Internet connection affects organizations regardless of service or market.

Losing Internet connection is, at its base, a threat defined by, "when," and not, "if." Too many failure points exist between the Internet itself and the end user of the infrastructure. Failure in ability to get online must be approached as a reality your organization will face and not a hypothetical you needn't prepare for in your business continuity plan.

Some negative results are felt immediately while the impact of others will not become evident until some point in the future.

When the Internet is Down

The ubiquity of the Internet in business and commerce prevents downtime from being as trivial as an inconvenience. Some negative results are felt immediately while the impact of others will not become evident until some point in the future. From the day's receipts in the cash register to a patient's health history to helping a customer get assistance, lost Internet connection affects organizations regardless of service or market.

The "Internet is Down" handwritten note hanging on a door, or taped to the credit card reader at the checkout counter, is so glaring and so devastating it might as well be written in neon. It means the cash register will either be ringing less often with a lower average order value or it will not be ringing at all. Every customer who turns around at the door or returns merchandise to the rack will be confronted with the choice of going to a competitor who can fulfil their need right away, contemplate whether the competitor will be better suited to serve them in the future, or, oftentimes, some combination of the two.

The formula to determine the amount of actual revenue lost to the Internet outage is straightforward: divide the average daily revenue by the minutes open for business. Now multiply the result by the number of minutes the outage event lasts.

$$\left(\frac{\text{Avg. Daily Revenue}}{\text{Minutes Open}}\right) \times \text{Minutes Down} = \text{Immediate Revenue Lost}$$

According to the Aberdeen Group study, three out of five organizations lose at least $1,000 in revenue per each minute down. Few are the organizations that lost $60,000 or less per years, and for some, the cost will reach six figures. Losing Internet connection leads to enormous revenue losses. Less well known is how much of the lost revenue will be accompanied by permanent the loss of customers and all potential revenue those customers might contribute to a business's performance in the days, months, and years to come.

While people running outside to enjoy fresh air during Internet downtime might make for a clever television commercial it is inherently bad for worker productivity. It means no e-mails or VoIP calls to existing or potential customers. Meeting deadlines with external customers becomes more difficult. Inbound calls, calls from customers who want to speak with you regarding your goods or services, go unanswered and potentially lead to customers lost without ever getting a chance to contribute to your bottom line. Your remote locations are not able to communicate with you or with one another. Your workers can do nothing without access to your cloud partners. A study from ISH in 2015 provides sobering data regarding the productivity costs of server, application, and network downtime. The annual aggregate cost of IT downtime is $700 billion revenue, which accounts for 17 percent of the cost while a staggering 78 percent is tied to productivity. Apply those percentages to your organization to get a sense of what Internet connection failure means to your organization[3].

Healthcare providers need Internet to provide access to records and best serve patients. Supply managers cannot update inventory status without connection to the Internet. Perhaps these are not applicable to your organization but evaluate your workflows and determine the points at which they require Internet connection 100 percent of the time. Those points exist, and those points are vulnerable.

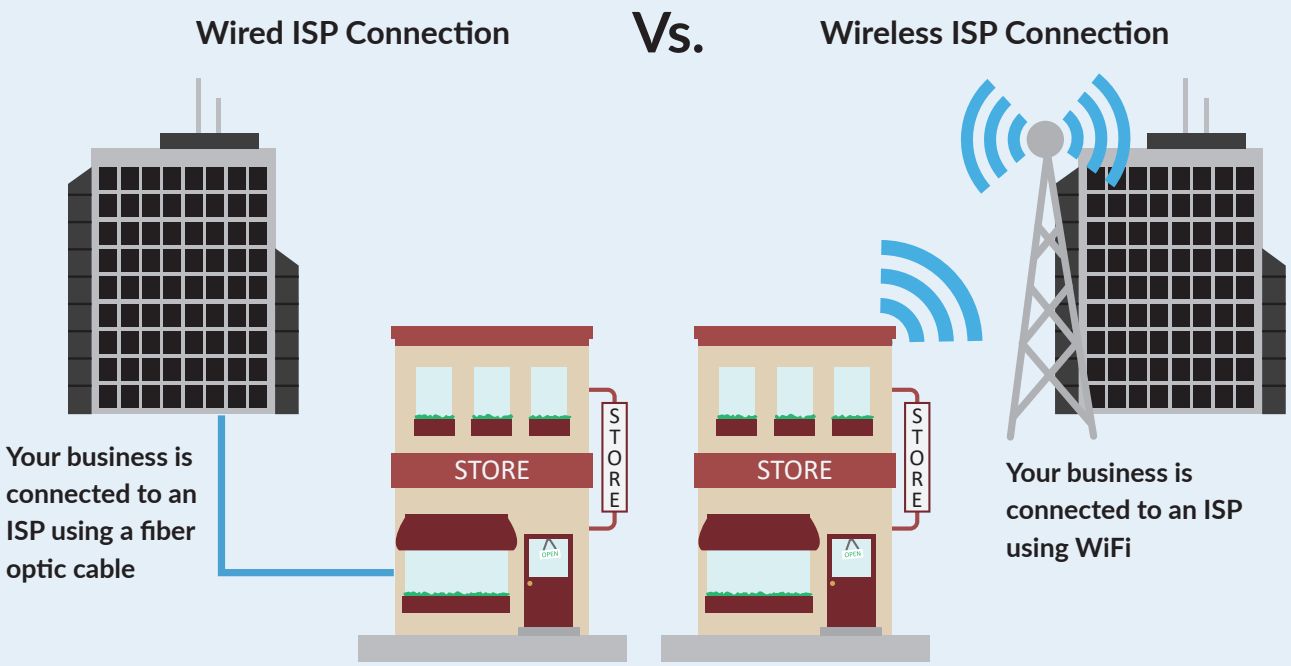
Less tangible but particularly impactful to businesses within the hospitality industry is the need for always-on WiFi networks. Guests might be out of area for their service providers and need WiFi, or perhaps they look to WiFi connections to manage Internet access without eating into data limits while traveling. WiFi as a service to guests loses its selling point without the ability to effectively maintain it at all times. These guests might be upset enough to post negative comments and negative ratings to hospitality locator services, and they might be turned off enough to not consider your business in the future. Every touch point matters in the hospitality industry, and WiFi connection is one of the most-visible of those touch points.

It is impossible to ignore the financial impact of Internet connection failure and reckless not to prepare for the fact connection to the Internet will fail, and will fail often, throughout the course of a year.

Internet Connection Failover

Implementing a viable Internet connection failover solution does not require a complete overhaul of existing network topology, but a fundamental understanding of your organization's need is necessary. Is the failover appliance guaranteeing service regardless of the reason the network failed, and is the transition to and return from the failover seamless? Does the failover appliance provide for prioritization of services to keep critical systems running while others are kept offline? Is continuous POS uptime important and, if so, does the failover include PCI compliance?

To mitigate the risk of relying on a single ISP, Internet connection failover employs a second Internet connection through a different ISP. What this looks like in the network topology depends upon whether the organization wishes to use wired or wireless for the connection.



The wireless option works best for areas where choice among ISPs using fiber is either limited or nonexistent, and it also nullifies the risk where the wired connection to all ISPs runs through the same conduit. A wired connection, perhaps the best option for organizations already employing a dual-WAN router, might make sense where choice among multiple ISPs is available or when the Internet need is more than a single wireless device can handle.

Ease of installation, necessary for smaller organizations without dedicated IT staff, is accomplished by a single wireless failover appliance installed on the network. The failover appliance is dropped into the LAN next to the broadband router with no disruption to the existing traffic flow. At the moment of connection failure, the device on the network fails over and runs until the primary connection is restored.

The best solution for more complex network topologies requiring a wired secondary Internet connection is to include a failover appliance to interface with existing firewalls and routers. The key to working with a wired ISP, as with wireless failover, is for the redundant connection to be available at the moment the primary connection fails.

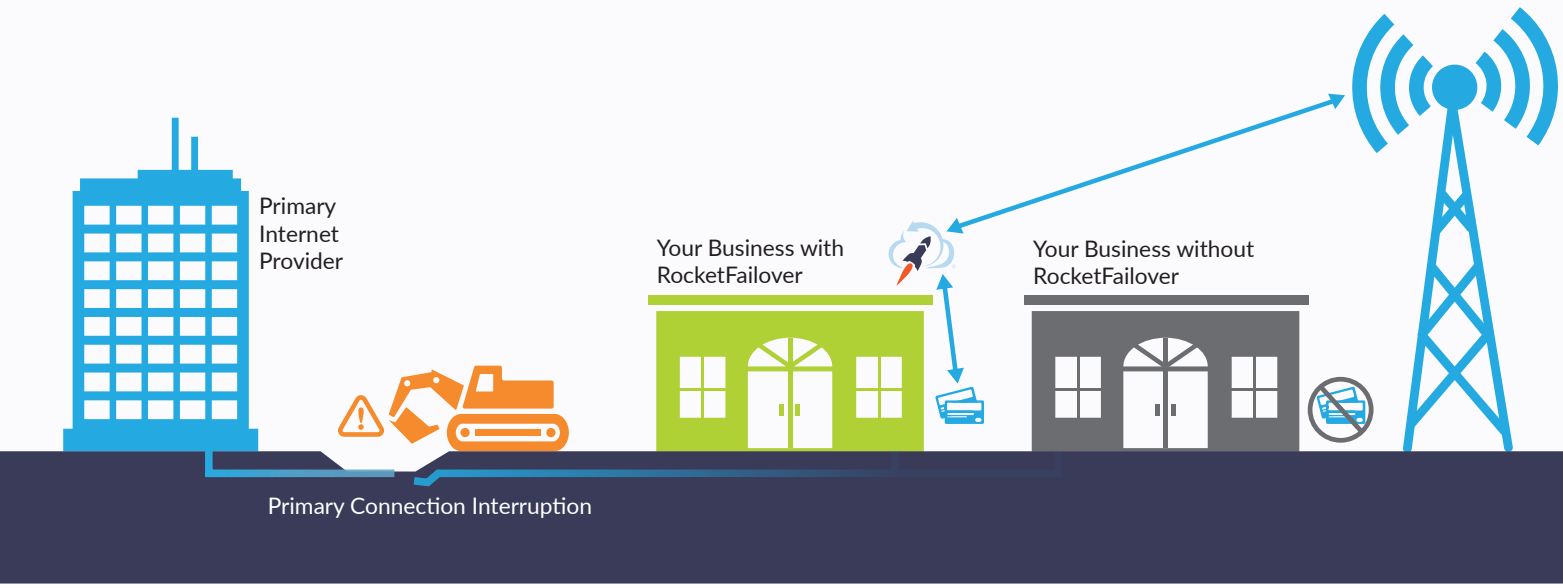
Organizations needing to be mindful of the amount spent in Internet connections might not be able to afford a failover providing the same amount of data as the primary connection. In fact, the secondary connection might not be able to provide the full data complement of the primary. This scenario requires organizations, particularly healthcare providers, to prioritize needs and allow access to the failover for critical systems and functions only.

Business continuity plans are not free of charge, and with installing a secondary Internet connection, the resources allocated to the contingency plans will increase. Internet connection failover provides the best opportunity to not only project ROI but show hard data behind the ROI as early as a month into having the failover connection.

RocketFailover®

RocketFailover from Akative provides your organization with the secondary Internet connection necessary to stay online, keep your employees productive, and allow your customers to purchase your goods and services. In addition to performing the basic need of providing the secondary Internet connection, RocketFailover will help you determine the root cause of the failure and monitor performance of the failover connection before and during use.

Your Internet connection needs are your own, and with RocketFailover, the solution can be tailored to suit those needs and work best within your existing network topology. Akative engineers can determine whether to deploy the RocketFailover as a traditional broadband-based connection, 4G LTE connection, or WiFi connection solution; design, implement, and monitor the failover connection; and be trusted resources during the times when RocketFailover keeps your business processes running. There is a version of RocketFailover for you no matter the size of your business or networking infrastructure needs.



Providing the secondary Internet connection is just one part of the process, but only RocketFailover includes iStatus® monitoring within the solution. The iStatus device monitors the primary Internet connection, with the system easily managed through mobile and PC apps, and alerts IT staff and key stakeholders not only of a disruption to service but also where the failure occurred. The ConnectionValidation™ technology within iStatus then monitors the secondary Internet connection to guarantee connectivity.

Look to Akative to provide the services you need to deploy RocketFailover as the secondary Internet connection to keep your organization up and running.

Conclusion

An Internet failover solution will keep the link to the outside world up and keep business going.

Building a comprehensive business continuity plan includes more than data backup. An organization needs its Internet connection to reach its cloud service provider, its backup locations, provide connectivity to its workforce and its customers, and continue generating the revenue needed to keep your business going. As technologies mature, as the threats to those technologies continue to multiply, it is imperative to be certain Internet connection, the basis of businesses for organizations large and small, is maintained to bring goods and services to the global market. An Internet failover solution will keep the link to the outside world up and keep business going.

References

1. Rapoza, Jim. (July 2016). Constant Website disruptions demand a new kind of performance management. The Aberdeen Group. Available. aberdeen.com/research/12979/12979-rr-new-performance-management/content.aspx

2. Will Greenberg, "String of West Coast attacks on Internet fiber optic cables leads to FBI investigation," Washington Post, July 2, 2015. Accessed October 17, 2016, washingtonpost.com/news/morning-mix/wp/2015/07/02/string-of-west-coast-attacks-on-Internet-fiber-optic-cables-leads-to-fbi-investigation/

3. Joe Stanganelli, "The High Price of IT Downtime," NETWORKComputing, January 28, 2016. Accessed November 2, 2016, www.networkcomputing.com/networking/high-price-it-downtime/856595126