SPECIAL REPORT

# The Business Case for Backup Internet

## Protecting Revenue, Productivity, and Continuity in a Cloud-First World

**Prepared by Dale Lyell – CTO at FlashForward**

May 2026 | North American Edition

FOR BUSINESS DECISION-MAKERS AND IT LEADERS

# Executive Summary

Internet connectivity has evolved from a convenience into a mission-critical utility for modern North American businesses. The migration to cloud-based platforms, software-as-a-service (SaaS) applications, cloud telephony, and video communications means that when the internet fails, business operations come to a standstill — regardless of how sophisticated a company's internal IT infrastructure may be.

This white paper examines the real cost of internet outages for US and Canadian businesses of all sizes, reviews common causes of outages and recent high-profile incidents affecting major carriers including AT&T, Comcast, Verizon, Rogers, Bell, and Telus, explores backup internet technologies and their pricing, and outlines how Software-Defined Wide Area Networking (SD-WAN) can intelligently manage multiple internet connections to ensure seamless continuity.

The central finding is straightforward: for virtually every business, the cost of a single significant internet outage far exceeds the annual cost of a backup internet connection. The AT&T outage of February 2024 alone blocked over 92 million calls across all 50 states and Washington D.C. The Rogers outage of July 2022 knocked approximately 25% of Canada's entire internet infrastructure offline, costing an estimated $142 million CAD in economic damage. Backup internet is not an IT luxury — it is a measurable, justifiable investment in business continuity.

# 1. The Changing Role of Internet Connectivity

## 1.1 The Cloud-First Business

Over the past decade, the way businesses consume technology has undergone a fundamental transformation. Servers that once sat in back-office rooms have been replaced by cloud platforms. Telephone systems that relied on landlines now route calls over the internet. Collaboration, file storage, accounting, customer relationship management (CRM), enterprise resource planning (ERP), point-of-sale systems, and security tools are increasingly delivered as cloud services accessed through a web browser.

Globally, 94% of organizations now use cloud computing in some form. In North America, Flexera's 2025 State of the Cloud Report found that small and medium-sized businesses (SMBs) saw their cloud workloads grow from 55% to 63% year-over-year, while enterprise cloud workloads reached 54% of total computing. By end of 2025, 87% of enterprises are expected to operate in a hybrid cloud environment. AWS, Microsoft Azure, and Google Cloud Platform collectively dominate North American cloud infrastructure.

This shift has created an inescapable dependency: the internet is now the backbone of business operations. Unlike on-premises server infrastructure that continued functioning during ISP outages, cloud systems are simply inaccessible when connectivity fails.

> **Key Statistic:** 63% of SMB workloads are now hosted in the cloud — meaning the majority of small business computing depends entirely on internet connectivity. That figure is growing every year.

### 1.2 Voice and Video Over the Internet

The traditional Public Switched Telephone Network (PSTN) is being decommissioned across North America. AT&T's copper network sunset, combined with the FCC's approval of PSTN discontinuation, has accelerated the shift to IP-based communications. Most businesses now rely on Voice over IP (VoIP) for their phone systems and platforms such as Microsoft Teams, Zoom, Cisco Webex, and Google Meet for video conferencing.

This means that a business internet outage no longer just disrupts email and file access — it completely cuts off telephone communications, customer-facing call centers, and the video conferencing that has become integral to both internal collaboration and client engagement. For businesses in financial services, healthcare, legal, real estate, and customer support sectors, the inability to communicate triggers immediate, measurable financial and reputational losses.

### 1.3 The Remote Worker Dependency

The normalization of hybrid and remote work has added another dimension to internet dependency. As of early 2025, nearly 80% of workers whose roles can be performed remotely are either working fully remotely (26%) or in a hybrid arrangement (52%). These workers depend on their home or mobile internet connections to access business systems — but they also depend on their company's internet connection being operational for office-hosted or VPN-dependent services.

68% of remote workers use a VPN to securely access company resources, with 62% of organizations still relying on VPN as their primary remote access method. A business office internet outage directly impacts remote workers who need VPN access to on-premises servers, domain controllers, internal applications, or on-premises phone systems. The connectivity requirements for remote workers encompass: secure VPN access to internal systems and file shares; access to cloud-hosted applications (Microsoft 365, Salesforce, QuickBooks Online); VoIP and video conferencing; and reliable upload speeds for video calls and cloud synchronization.

## 2. The Real Cost of Internet Downtime

Calculating the cost of an internet outage requires considering multiple layers of impact: staff productivity losses, direct revenue impacts, emergency IT support costs, reputational damage, customer service failures, and potential regulatory penalties. Industry research consistently finds that actual costs are significantly higher than most business owners initially estimate.

### 2.1 Industry Benchmarks

According to ITIC's 2024 Hourly Cost of Downtime research, over 90% of enterprises estimate their cost of downtime exceeds $300,000 USD per hour. BigPanda's 2024 research found that large enterprises incur average costs of $23,750 per minute — approximately $1.4 million per hour. For Fortune 500 companies, outage costs commonly range from $500,000 to $1 million per hour, with financial services and healthcare institutions potentially exceeding $5 million per hour. Even for small and micro businesses, conservative industry estimates place the cost at $1,670 or more per minute when all factors are included.

© 2026 FlashForward | Confidential

These figures encompass lost staff productivity (wages paid for idle time), direct revenue losses from transactions that cannot be processed, customer churn from service failures, emergency IT support costs, and the longer-term reputational cost of being perceived as unreliable.

## 2.2 Downtime Cost Estimates by Business Size

The following table provides a simplified illustration of the financial impact of internet downtime on North American businesses of different sizes. These calculations use a blended cost model that accounts for staff productivity loss (based on average US Bureau of Labor Statistics salary data) and a conservative estimate of foregone revenue using a 2.5x revenue-to-salary multiplier, which is typical for service and professional services businesses. It does not include emergency IT support fees, reputational damage, or regulatory penalties, which would increase all figures further.

| Business Size | Employees | Avg Salary | Cost / Hour | 4-Hour Outage | Full-Day Outage (8 hrs) |
|---|---|---|---|---|---|
| Micro Business | 5 | $55,000 | **$496** | $1,980 | $3,970 |
| Small Business | 25 | $62,000 | **$2,790** | $11,200 | $22,300 |
| Medium Business | 100 | $70,000 | **$12,500** | $50,100 | $100,200 |
| Large Business | 500 | $80,000 | **$72,100** | $288,500 | $577,000 |

* Figures in USD. Productivity loss = (employees × avg salary) ÷ 2,080 working hours/year. Revenue impact estimated at 2.5× salary cost. Does not include IT support, regulatory penalties, or reputational damage. Salary benchmarks sourced from US Bureau of Labor Statistics 2024–2025 data.

**Perspective Check:** A 4G/5G business backup connection costs approximately $69–$105/month — around $830–$1,260 per year. For a 25-person business, that annual cost is recovered in less than 25 minutes of avoided downtime.

## 2.3 The Hidden Costs Often Overlooked

Beyond direct productivity and revenue losses, businesses routinely underestimate these additional cost categories during an internet outage:

- Emergency IT support: After-hours call-out fees for technicians typically range from $150 to $350 per hour, with minimum charges of two to four hours.
- Cloud SLA penalties: Businesses providing internet-dependent services to their own customers may trigger SLA breach penalties or be liable for customer compensation and credits.
- Data integrity risks: Transactions in progress at the time of an outage — including financial records, inventory updates, and customer orders — may be corrupted or lost, requiring expensive reconciliation.

© 2026 FlashForward | Confidential

- Regulatory exposure: Businesses in sectors such as healthcare (HIPAA / PIPEDA), financial services (SEC / FINRA / SOX / CIRO), or those handling payment card data (PCI-DSS) may face compliance breaches and mandatory reporting obligations when systems are unavailable.
- Customer churn: Service failures — including inability to contact a business or process transactions — result in a measurable percentage of customers seeking alternatives. In competitive markets, a single high-profile outage can have lasting effects on customer retention.
- Payment processing losses: Businesses reliant on internet-connected payment terminals (Moneris, TD Merchant, Square, Stripe, Clover) lose the ability to process credit and debit card transactions entirely, forcing them to turn away customers or close.

# 3. Common Causes of Internet Outages

Understanding why internet outages occur is an important step in appreciating why no single provider or technology is immune to failure. Outages have multiple root causes, and many of the most severe are entirely outside the control of the affected business.

| Cause Category | Description | Mitigation via Backup Link |
|---|---|---|
| Physical Infrastructure Damage | Fiber optic cables are severed by excavation, construction, vehicle accidents, or severe weather events including hurricanes, ice storms, and tornadoes. A single cable cut can affect thousands of customers across a wide area. | A backup on a different physical medium (e.g., 4G/5G wireless) is completely unaffected by cable cuts. |
| ISP Equipment and Software Failure | Routers, switching equipment, or core network hardware can fail. Software bugs, firmware updates, or misconfigured routing rules can cause widespread outages affecting all customers on a network node — as seen with AT&T in February 2024. | A backup via a different ISP provides independence from any single provider's equipment or software. |
| BGP Routing Errors | Border Gateway Protocol (BGP) misconfiguration errors can propagate through interconnected networks, causing cascading internet disruptions. BGP errors have caused some of the largest global outages in internet history. | Dual-carrier SD-WAN detects BGP-related path failures and automatically routes traffic around them. |
| Network Maintenance and Upgrades | Carriers routinely perform planned maintenance that can cause unplanned disruptions. Bell Canada's May 2025 multi-province outage was caused by a router update that required a network-wide rollback. | A backup link ensures business continuity during carrier maintenance windows and failed update rollouts. |
| Power Failures | Power outages affecting ISP exchange buildings, node cabinets, or a business's | A 4G/5G backup router with UPS battery backup can maintain |

| Cause Category | Description | Mitigation via Backup Link |
|---|---|---|
| | premises can take down internet services. Node cabinets have limited battery backup and are vulnerable in extended outages. | connectivity even during local power grid failures. |
| DDoS and Cyber Attacks | Distributed Denial of Service (DDoS) attacks targeting ISP infrastructure or a business's own public-facing services can saturate bandwidth and render connectivity unusable for legitimate traffic. | A secondary connection with DDoS mitigation can maintain operations while the primary link absorbs attack traffic. |
| Last-Mile Infrastructure | Cable, DSL, and fiber connections are subject to degradation from aging copper infrastructure, damaged conduits, or flooded junction boxes — particularly in older urban areas and rural regions. | A wireless backup bypasses all last-mile fixed infrastructure, providing true technology diversity. |

# 4. Recent North American ISP Outage Case Studies

The following incidents are drawn from publicly documented outage events affecting US and Canadian businesses. They illustrate that major outages are not rare exceptions — they are regular occurrences affecting every major carrier, at any time of day or night.

## 4.1 AT&T National Outage — February 22, 2024

At 2:42 AM EST on February 22, 2024, AT&T implemented a network configuration update that contained an equipment error. Within three minutes, the error triggered a nationwide cascade, placing the entire AT&T network into "protect mode" — disconnecting all devices from the network simultaneously.

The outage lasted approximately 11 hours and affected customers across all 50 states, Washington D.C., Puerto Rico, and the U.S. Virgin Islands. The scale was extraordinary: more than 125 million devices lost service, over 92 million voice calls were blocked, and more than 25,000 attempts to reach 911 emergency services failed. The outage also impacted T-Mobile and Verizon customers roaming on AT&T infrastructure. The FCC launched a formal investigation into the incident, and AT&T issued bill credits to affected customers.

**Key Lesson:** AT&T is the largest telecommunications company in the United States, with hundreds of billions in infrastructure investment. A single configuration error eliminated service for 125 million devices for nearly 11 hours — across the entire country. No carrier is immune.

## 4.2 Rogers National Outage — July 8, 2022 (Canada)

On July 8, 2022, Rogers Communications — Canada's largest cable company and one of three dominant national carriers — suffered a total nationwide outage that knocked approximately 25% of Canada's entire internet infrastructure offline. The outage was caused by a faulty BGP routing filter update that propagated through Rogers' core network, disconnecting all traffic.

More than 12 million subscribers lost all connectivity. The business impact was profound and multi-sectoral: Interac — Canada's national debit card payment network — was taken entirely offline, meaning businesses across the country could not process debit card transactions regardless of who their own internet provider was. Banks, hospitals, government offices, and public transit systems were disrupted. Some businesses were forced to close for the day. At least one death was reported that may have been linked to the failure of emergency services. The economic damage was estimated at $142 million CAD. Rogers subsequently committed $261 million CAD to physically separate its wireless and wireline networks to prevent a recurrence, and the CRTC introduced new mandatory outage reporting regulations.

## 4.3 Bell and Telus Multi-Province Outage — May 21, 2025 (Canada)

On the morning of May 21, 2025 — a peak business weekday — Bell Canada pushed a software update that contained a routing error affecting core Bell routers. The update required a full rollback, during which Bell's network experienced a widespread outage across Ontario, Quebec, and Atlantic Canada. Due to interconnection agreements, Telus customers in Eastern and Atlantic Canada were simultaneously affected as their traffic normally transited Bell's network.

At the height of the outage, more than 130,000 incident reports were filed on Downdetector for Bell alone. The incident demonstrated a systemic risk in Canadian telecommunications: carrier interdependency means that an outage at one major carrier can cascade to affect customers of other carriers who rely on shared infrastructure.

## 4.4 Lumen (CenturyLink) Outages — 2024–2025

Lumen Technologies (formerly CenturyLink), a major US backbone carrier serving businesses and acting as a transit provider for many smaller ISPs, experienced multiple notable outages in 2024 and 2025. A December 2024 outage lasted 36 minutes, affecting customers and downstream ISP partners across the US and Canada. An October 2025 outage lasted over 40 minutes, with impacts spanning the US, UK, France, Brazil, Hong Kong, Singapore, and India.

These incidents highlight a less visible but significant risk: businesses whose ISP relies on a major backbone carrier like Lumen for transit can experience outages caused by a provider they have no direct commercial relationship with.

| Date | Provider | Duration | Business Impact |
|---|---|---|---|
| July 8, 2022 | Rogers (Canada) | ~19 hours | 12M+ subscribers; 25% of Canada offline; Interac down nationwide; $142M CAD economic loss |
| Feb 22, 2024 | AT&T (USA) | ~11 hours | 125M devices; 92M+ calls blocked; 25,000+ 911 failures; all 50 states affected |

| Date | Provider | Duration | Business Impact |
|---|---|---|---|
| Dec 2024 | Lumen (USA/Canada) | ~36 minutes | US and Canadian businesses and downstream ISPs impacted |
| May 21, 2025 | Bell / Telus (Canada) | Peak morning hours | 130,000+ incident reports; Ontario, Quebec, Atlantic Canada; carrier interdependency exposed |
| Oct 2025 | Lumen (Global) | ~41 minutes | Multi-national impact across US, Canada, UK, Europe, and Asia-Pacific |
| April 2026 | Verizon Business (USA) | ~63 minutes | US and international partners; peak business day hours; spike in US outage events |

Sources: Wikipedia (2022 Rogers Outage), FCC Report (AT&T February 2024), CBC News, NetworkWorld 2024/2025/2026 Outage Reports, MobileSyrup.

# 5. Backup Internet Options and Pricing

When selecting a backup internet service, the key considerations are independence from the primary connection (different technology and/or different carrier), adequate speed for critical business functions, reliability, and cost. The following section outlines the four most commonly deployed backup internet technologies for North American businesses, with indicative 2025–2026 pricing in USD.

The guiding principle: a backup connection should use a different technology type and a different provider than the primary service. This eliminates the risk of both connections failing simultaneously due to a single carrier outage, a shared infrastructure fault, or a cable cut affecting both services at the same point.

## 5.1 Fiber-to-the-Premises (FTTP) — 100 Mbps

Fiber-to-the-premises delivers fiber optic cable directly to the business location, providing the highest reliability and performance of any fixed-line technology. FTTP is not dependent on copper infrastructure, making it more resilient to weather and less susceptible to signal degradation. Major US providers include AT&T Fiber, Frontier Fiber, and regional fiber providers. In Canada, Bell Fibe, Telus PureFibre, and Rogers Ignite Fiber are the dominant options.

| | |
|---|---|
| **Download Speed** | 100 Mbps symmetric (upload = download) |
| **Upload Speed** | 100 Mbps (true symmetric fiber) |
| **Typical Business Price (USD)** | $80 – $150/month (AT&T Business Fiber from $80; Comcast Business from $99; regional providers vary) |
| **Typical Business Price (CAD)** | $100 – $200/month (Bell Business, Telus Business; competitive providers from $75/month) |

| | |
|---|---|
| **Best for Backup When** | Primary connection is high bandwidth dedicated fibre. FTTP provides high performance and reliability as a second fixed-line path from a different provider. |
| **Limitations** | Availability varies significantly by location. In rural areas, fiber may not be accessible. Two fiber connections from different providers at the same address provide the best diversity but may share street infrastructure. |

## 5.2 Fixed Wireless & 4G/5G — 50–200 Mbps

Fixed wireless internet using 4G or 5G mobile networks is one of the most effective backup solutions because it is entirely independent of all fixed-line infrastructure — no fiber, no coaxial cable, no copper. A 4G/5G router installed at the premises draws from the mobile carrier network, meaning physical cable cuts, fiber node failures, and last-mile infrastructure problems have no impact on the connection.

In the US, major 5G business internet providers include Verizon Business, T-Mobile for Business, and AT&T Business. In Canada, Rogers, Bell, and Telus all offer 4G/5G business plans. The critical consideration: always select a wireless backup carrier different from your primary internet provider to ensure true independence.

| | |
|---|---|
| **Download Speed** | 50–200 Mbps typical (4G); 100–600 Mbps in 5G coverage areas |
| **Upload Speed** | 10–50 Mbps typical (4G); higher on 5G |
| **Typical Business Price (USD)** | $69 – $105/month (Verizon 5G Business Internet from $69; T-Mobile Business from $50; AT&T Business 5G from $65) |
| **Typical Business Price (CAD)** | $80 – $130/month (Rogers, Bell, Telus 4G/5G business data plans) |
| **Setup** | Self-install router with no cable installation required; rapid deployment often within 24 hours |
| **Best for Backup When** | Primary is any fixed-line service (fiber, cable, DSL). Wireless provides maximum technology and infrastructure diversity. |
| **Limitations** | Speed varies by coverage and congestion. Select a carrier that is NOT your primary mobile provider for maximum independence. |

## 5.3 Cable Internet (DOCSIS/HFC) — 100–300 Mbps

Cable internet using DOCSIS (Data Over Cable Service Interface Specification) technology operates over the existing coaxial cable infrastructure originally built for cable television. Major US cable providers include Comcast (Xfinity Business), Charter (Spectrum Business), Cox Business, and Mediacom. In Canada, Rogers, Shaw (now Rogers), Videotron, and Cogeco are the dominant cable providers. Cable is broadly available in urban and suburban areas and offers high download speeds at competitive prices.

| | |
|---|---|
| **Download Speed** | 100–300 Mbps typical; up to 1.5 Gbps on DOCSIS 3.1 |
| **Upload Speed** | 10–35 Mbps typical (asymmetric; upload is slower than download) |

| | |
|---|---|
| **Typical Business Price (USD)** | $70 – $150/month (Comcast Business from $69.99; Spectrum Business from $69.99; Cox Business from $79.99) |
| **Typical Business Price (CAD)** | $80 – $160/month (Rogers, Videotron, Cogeco business plans) |
| **Best for Backup When** | Primary is fiber or DSL from a different provider; cable provides a cost-effective metro-area fixed-line backup path |
| **Limitations** | Shared infrastructure can cause congestion during peak hours. Upload speeds are significantly lower than download. Not available in rural areas. |

## 5.4 DSL / Fiber-to-the-Node (FTTN) — Up to 100 Mbps

DSL (Digital Subscriber Line) and its variant Fiber-to-the-Node (FTTN) use fiber optic cable to a street-level cabinet (node), and then the existing copper telephone network for the final leg to the premises. In the US, AT&T, Lumen/CenturyLink, Frontier, and Windstream are major DSL providers. In Canada, Bell, Telus, and their wholesale resellers offer FTTN services under various brand names. DSL is widely available but is being progressively retired as fiber reaches more locations.

| | |
|---|---|
| **Download Speed** | Up to 100 Mbps (actual speed highly dependent on copper line length from node) |
| **Upload Speed** | Up to 20 Mbps (asymmetric) |
| **Typical Business Price (USD)** | $50 – $80/month (among the most affordable options for backup; widely available) |
| **Typical Business Price (CAD)** | $50 – $100/month (Bell, Telus, and wholesale ISPs) |
| **Best for Backup When** | No fiber or cable available; DSL provides a cost-effective backup option from a carrier independent of the primary provider |
| **Limitations** | Copper dependency limits speed; more susceptible to weather-related performance issues. Being phased out in many areas. Not suitable for video-heavy workloads at distance. |

## 5.5 Backup Connection Cost Comparison Summary

| Technology | Monthly (USD) | Annual (USD) | Infrastructure Independence | Best Use Case |
|---|---|---|---|---|
| 4G/5G Fixed Wireless | $69 – $105 | $828 – $1,260 | **Highest (no cable dependency)** | Best backup for all fixed-line primary connections |
| Fiber (FTTP) | $80 – $150 | $960 – $1,800 | High (different provider) | High-performance backup from a second fiber carrier |

| Technology | Monthly (USD) | Annual (USD) | Infrastructure Independence | Best Use Case |
|---|---|---|---|---|
| Cable (DOCSIS/HFC) | $70 – $150 | $840 – $1,800 | Medium (different to fiber) | Cost-effective metro backup where cable available |
| DSL / FTTN (Copper) | $50 – $80 | $600 – $960 | Low-Medium (copper vulnerable) | Budget option; widely available where cable/fiber absent |

# 6. SD-WAN: Intelligent Management of Multiple Internet Connections

## 6.1 What is SD-WAN?

Software-Defined Wide Area Networking (SD-WAN) is a technology that uses software intelligence to manage, optimize, and secure traffic across multiple network connections — including multiple internet services from different carriers. Unlike traditional routers that follow static, manually configured routing rules, an SD-WAN device continuously monitors the health and performance of every connected link in real time, making dynamic decisions about which traffic should travel over which connection.

For businesses deploying a backup internet strategy, SD-WAN transforms a passive backup link from a dormant insurance policy into an active, intelligent network asset. Rather than sitting idle until a failure occurs, the backup connection can be used continuously — adding to total available bandwidth, carrying lower-priority traffic, or serving as the automatic fallback for critical applications the moment the primary link shows signs of degradation.

## 6.2 How SD-WAN Manages Multiple Links

An SD-WAN device monitors each internet connection by continuously sending probe packets and measuring key performance metrics: latency (delay), jitter (variation in delay), packet loss, and available bandwidth. Based on these real-time measurements, the SD-WAN applies configurable policies to determine how traffic is handled. The two primary operating modes are:

- Active-Passive (Failover Mode): The primary internet connection handles all traffic under normal conditions. The SD-WAN monitors the primary link in real time. When packet loss exceeds a defined threshold or the link becomes unavailable, traffic is automatically moved to the backup connection — often within milliseconds, without any manual intervention or disruption to active sessions.
- Active-Active (Load Balancing / Link Aggregation): Both connections are used simultaneously. The SD-WAN distributes traffic across available links based on configured policies, maximizing total available bandwidth and providing immediate resilience with zero failover delay. If one link degrades or fails, all traffic is concentrated on the remaining healthy link instantly.

## 6.3 Traffic Prioritization and Quality of Service

One of the most powerful capabilities of SD-WAN is application-aware traffic prioritization. SD-WAN applies Quality of Service (QoS) policies that distinguish between different traffic types and route them across connections accordingly:

- Voice and video (VoIP, Microsoft Teams, Zoom, Webex): Routed over the best-performing link with the lowest latency and jitter. Voice calls and video conferencing are extremely sensitive to network quality — even 50ms of jitter can cause audible distortion or choppy video.
- Critical cloud applications (Salesforce, Microsoft 365, QuickBooks, ERP): Routed over the primary high-performance link with guaranteed bandwidth allocation.
- General business traffic (email, web browsing, software downloads): Can be distributed across both links or directed to the backup link, freeing the primary connection for time-sensitive applications.
- Bulk background tasks (cloud backups, Windows Update, large file transfers): Throttled to avoid consuming bandwidth needed for real-time communications.

**Business Outcome:** With SD-WAN, a business maintains crystal-clear VoIP calls and uninterrupted access to Salesforce and Microsoft 365 even while the primary internet link is failing — the SD-WAN detects degradation and re-routes automatically before any user notices an impact.

## 6.4 SD-WAN vs. Traditional Dual-Router Failover

The critical differentiator between a traditional passive failover router setup and an SD-WAN solution is the speed and intelligence of failover. A traditional router may take 30 to 90 seconds to detect a link failure and reroute traffic — long enough to drop active VoIP calls, disconnect remote desktop sessions, and time out cloud application connections. A well-configured SD-WAN can detect link degradation in seconds and complete the failover in under one second, preserving active sessions transparently.

| Feature | Traditional Dual-Router Setup | SD-WAN Solution |
|---|---|---|
| Failover Detection | 30–90 seconds (link timeout) | **< 1 second (real-time monitoring)** |
| Traffic Prioritization | Manual, static rules only | **Dynamic, application-aware** |
| Backup Link Usage | Idle until primary fails | **Active — adds to total bandwidth** |
| VoIP Call Continuity | Calls drop during failover | **Calls maintained seamlessly** |
| Visibility and Reporting | Limited; requires manual checks | **Centralized dashboard; automated alerts** |
| Management | Manual reconfiguration required | **Software-managed; remote administration** |

# 7. Cloud Services and Remote Worker Connectivity Requirements

## 7.1 Cloud Applications at Risk During an Outage

The migration to cloud services is not a future trend — it is the operational reality for the majority of North American businesses today. The following categories represent the most common cloud-dependent business functions that are directly impacted when an internet connection fails:

- Productivity and Collaboration: Microsoft 365, Google Workspace, Slack, Zoom — email, calendars, documents, chat, and video conferencing are all inaccessible without internet.
- Cloud Phone Systems: RingCentral, 8x8, Vonage Business, Microsoft Teams Phone, Dialpad, VoiPro, — all cloud PBX and UCaaS platforms require continuous internet connectivity for every call.
- CRM and Sales Platforms: Salesforce, HubSpot, Zoho CRM — without connectivity, sales teams cannot access customer records, log interactions, or process quotes and contracts.
- Accounting and Finance: QuickBooks Online, FreshBooks, Sage Intacct, Xero — invoicing, payroll, and financial reporting halt completely.
- ERP Systems: Microsoft Dynamics 365, SAP S/4HANA Cloud, NetSuite — operational management, inventory, procurement, and production scheduling are all affected.
- Point of Sale and Payments: Cloud-based POS systems (Moneris, Square, Lightspeed, Toast) and all internet-dependent payment terminals cannot process credit or debit card transactions.
- Cloud Storage and File Access: OneDrive, SharePoint, Google Drive, Dropbox, Box — all shared documents and files become inaccessible for the duration of the outage.
- Virtual Desktops and Remote Access: Azure Virtual Desktop, Amazon WorkSpaces, Citrix Cloud — hosted desktop environments are completely inaccessible without internet.

**Operational Reality:** A business running Microsoft 365, Teams Phone, Salesforce, and QuickBooks Online loses 100% of its technology capability during an internet outage. There is no local fallback — the cloud requires the internet.

## 7.2 Bandwidth Requirements for Critical Cloud Services

| Application / Service | Bandwidth Required | Notes |
|---|---|---|
| VoIP voice call (per concurrent call) | 100 Kbps up/down | Low latency and jitter are critical; bandwidth requirement is minimal |
| Video call — SD quality (per user) | 600 Kbps – 1.5 Mbps | Microsoft Teams, Zoom, Google Meet minimum requirement |
| Video call — HD quality (per user) | 1.5 – 4 Mbps | Recommended for professional video meetings |
| Microsoft 365 / Google Workspace | 1 – 3 Mbps per user | Email, documents, SharePoint; higher for large file sync |

| Application / Service | Bandwidth Required | Notes |
|---|---|---|
| Salesforce / CRM | 0.5 – 2 Mbps per user | Light on bandwidth; latency matters more for responsiveness |
| Remote desktop / Virtual desktop (per user) | 2 – 10 Mbps | Highly variable; depends on screen resolution and activity level |
| Cloud backup (ongoing background) | 5 – 50 Mbps upload | Should be throttled to avoid impacting real-time services |

Example calculation: A 10-person office where 8 users are on active HD video calls and 10 have cloud applications open requires approximately: (8 × 4 Mbps video) + (10 × 2 Mbps apps) = 52 Mbps. A 5G backup connection at 100 Mbps fully supports all critical functions for this team.

## 7.3 Remote Workers and Office-Based Service Dependencies

Remote workers present a unique dual dependency on internet connectivity. Both their own home connection and the office connection must be available for them to work effectively. This is particularly important for businesses that have not fully migrated all services to the cloud.

Specific scenarios where office internet availability directly impacts remote workers include:

- VPN connectivity: Remote workers tunneling through a VPN to access internal company resources are directly affected by the office internet connection being unavailable — regardless of the quality of their own home service.
- On-premises hosted servers: Businesses running local file servers, internal databases, ERP systems, or Active Directory domain controllers that have not been moved to the cloud are completely inaccessible to remote workers when the office internet link fails.
- On-premises phone systems: Where the business phone system is hosted physically at the office location — even with SIP trunks — remote workers using softphones or IP handsets that route through the office PBX lose calling capability when the office internet fails.
- On-premises security appliances: Some businesses route all remote worker traffic through office-based firewalls, web filters, or Data Loss Prevention (DLP) appliances for policy enforcement. If the office internet fails, those remote workers may lose their compliant internet access path entirely.
- Multi-factor authentication servers: On-premises MFA or RADIUS authentication servers are unreachable when the office internet fails, potentially locking remote workers out of all company systems.

**Recommendation:** Businesses with any on-premises hosted services should treat backup internet at the office as directly protective of remote worker productivity — not just office-based staff. A backup link at the office protects both cohorts simultaneously, at no additional cost.

# 8. Building Your Business Continuity Strategy

## 8.1 The Return on Investment Case

The financial case for backup internet is clear when downtime costs are compared against the cost of protection. Using the conservative estimates from Section 2 and backup connection pricing from Section 5, the following table illustrates payback periods for a 4G/5G backup connection at $90/month ($1,080/year):

| Business Size | Annual Backup Cost | Cost of 1-Hr Outage | Cost of 4-Hr Outage | Payback Period* |
|---|---|---|---|---|
| Micro (5 staff) | $1,080 | $496 | $1,980 | **~2.2 outage hours** |
| Small (25 staff) | $1,080 | $2,790 | $11,200 | **~23 minutes** |
| Medium (100 staff) | $1,080 | $12,500 | $50,100 | **~5 minutes** |
| Large (500 staff) | $1,080 | $72,100 | $288,500 | **~54 seconds** |

* Payback Period = duration of avoided downtime required to recover the full annual backup connection cost of $1,080 USD.

## 8.2 Recommended Strategy by Business Size

### Micro to Small Businesses (up to 25 employees)

Recommended approach: Primary fiber or cable connection from one provider, plus a 4G/5G backup router or Fixed Wireless service (from a different carrier). By including a SD-WAN failover capability with automatic failover, business continuity is preserved .

The SD-WAN router automatically detects primary link failure and switches all traffic to the 4G/5G or Fixed Wireless connection within seconds — no manual intervention, no IT staff needed. This setup provides automatic failover protection, combined bandwidth during normal operations, and seamless voice call continuity through any outage.

### Medium Businesses (25–200 employees)

Recommended approach: Two diverse fixed-line connections from different providers (e.g., fiber from AT&T/Bell + cable from Comcast/Rogers) supplemented by a 4G/5G or Fixed Wireless backup, all managed via a commercial SD-WAN platform. At this scale, a managed SD-WAN service — available from $200–$600/month from providers including Verizon SD-WAN, AT&T SD-WAN, or specialist MSPs — provides application-aware routing, QoS policies, centralized management, and SLA reporting.

Businesses in this tier should also establish: business-grade SLA agreements with all ISPs (guaranteeing maximum fault response times and uptime commitments); static IP addressing on backup connections for VPN consistency; and 24/7 monitoring with automated failover alerts.

### Larger Businesses (200+ employees, multi-site)

Recommended approach: An enterprise SD-WAN platform deployed across all locations, with each site carrying a minimum of two diverse internet connections using different technologies and different

carriers. At this scale, SD-WAN delivers centralized policy management across all sites; integration with cloud security platforms (SASE — Secure Access Service Edge); optimized direct routing to AWS, Azure, and Google Cloud via preferred peering; and detailed per-application, per-site performance analytics.

MPLS or dedicated private circuits may remain appropriate for the most latency-sensitive inter-site traffic, with internet connections handling cloud breakout and serving as always-available backup paths.

### 8.3 Implementation Checklist

- Audit your internet dependencies: Document all cloud services, VoIP/UCaaS systems, and on-premises services that require internet connectivity to function.
- Evaluate your current primary connection: Identify your provider, technology type, and any single points of failure in the existing infrastructure.
- Select a diverse backup technology: Choose a backup on a different technology (preferably 4G/5G or Fixed Wireless) from a carrier that is different from your primary ISP and primary mobile carrier.
- Choose an SD-WAN solution: Decide between active-active load balancing or active-passive failover based on your bandwidth needs, budget, and application profile.
- Size the backup connection: Ensure the backup connection provides sufficient capacity for all critical business functions — voice, video, and cloud applications — for the full staff headcount.
- Test failover quarterly: Intentionally disconnect the primary connection and verify that the backup takes over seamlessly, that VoIP calls remain active, and that cloud applications remain connected without data loss.
- Review your ISP SLAs: Ensure both primary and backup contracts include acceptable maximum fault response times and uptime guarantees. Business-grade SLAs typically guarantee repair within 4–8 hours versus residential-grade which may take 24–48 hours or longer.
- Address remote worker dependencies: Identify which remote worker functions depend on the office internet link and include those scenarios explicitly in your continuity plan.
- Consider UPS backup power: Pair your primary router, SD-WAN device, and 4G/5G / Fixed Wireless backup router with an uninterruptible power supply (UPS) to maintain connectivity during power outages.

## 9. Conclusion

The evidence is unambiguous: internet connectivity is now as critical to North American business operations as electricity or running water. The migration to cloud services, the adoption of cloud telephony, the normalization of hybrid work, and the dependency of remote workers on office-hosted systems have collectively elevated internet availability from an IT consideration to a core business risk that belongs on every organization's risk register.

Recent outages from North America's largest and most trusted telecommunications providers — including AT&T's February 2024 outage affecting 125 million devices across all 50 states, Rogers' 2022 outage that took 25% of Canada's internet offline and brought the national debit card network down with it, and Bell and Telus's May 2025 multi-province outage at peak business hours — demonstrate that no single provider, regardless of size, investment, or reputation, is immune to extended service failures.

The financial case for backup internet is compelling at every business size. For a 25-employee business, the entire annual cost of a 5G or Fixed Wireless backup connection is recovered in less than 25 minutes of avoided downtime. For a 100-person company, the payback is measured in minutes. For larger organizations, in seconds. When combined with an SD-WAN solution that provides intelligent, application-aware failover without user disruption, backup internet transitions from a reactive safety net to an active, productivity-enhancing network asset.

FlashForward recommends that every business with internet-dependent operations — which now means virtually every North American business — implement a dual-connection strategy using diverse technologies and carriers, managed by SD-WAN. The cost of doing so is predictable and modest. The cost of not doing so, as millions of businesses discovered on February 22, 2024 and July 8, 2022, can be severe and immediate.

## About FlashForward

FlashForward consults on managed IT services, network infrastructure, vendor management and business continuity solutions. For an assessment of your business's internet resilience and backup connectivity options, contact Dale@flashforward.co.

### Disclaimer

This white paper is provided for general informational purposes. Pricing figures are indicative and based on publicly available information as of May 2026. Actual pricing varies by provider, location, plan tier, and promotional terms. Downtime cost estimates are illustrative models based on industry research and BLS salary data; actual costs depend on individual business circumstances and industry sector. FlashForward recommends obtaining specific quotes and professional advice before making infrastructure investment decisions.