The Marconi Society

BUSINESS RESILIENCE GUIDE

Strategies for Small and Medium-Sized Enterprises (SMEs) to Ensure Operational Continuity
Phase 1 Report, Marconi Society Internet Resilience Institute

June 25, 2026 | marconisociety.org

Business Resilience Guide

Strategies for Small and Medium-Sized Enterprises (SMEs) to Ensure Operational Continuity
Phase 1 Report, Marconi Society Internet Resilience Institute

About the Marconi Society

The Marconi Society builds communities of leaders and stakeholders that are at the forefront of emerging technology so that together we can create a more connected and sustainable world.

For over five decades, we have celebrated the innovators, both established and emerging, who have shaped our connected world. The Institutes provide platforms to convene our network of visionaries to collaborate on identifying, assessing, and recommending ways to ensure that emerging technologies benefit society.

About the Internet Resilience Institute

In 2024, the Internet Resilience (IR) Institute began with a straightforward idea: bring together a diverse community of experts to better understand how to strengthen the resilience of the global Internet. Since then, that idea has matured into an initiative that is generating original, practical tools for operators and businesses.

The Institute's work was sparked by a provocative question posed at its inaugural workshop at the National Academy of Sciences (NAS) in Washington, DC, in November 2024:

If the Internet suffered a global failure, what would be needed for a reboot?

This question exposed that Internet resilience is ultimately a global coordination problem, not just a technical one, and it is deeply rooted in governance and shared accountability across sectors. The Institute's work, now widely referenced in Internet governance and technical circles, are grounded in key activities, including:

- Critical briefings within the 2024 IR Report were presented to the U.S. Council for International Business (USCIB) Digital Policy Committee.
- Engaged with stakeholders at major global meetings, including ICANN Prague, ICANN Dublin, and in other fora, reinforcing the Institute's presence as a trusted convener.
- Hosted a high-profile session at the 20th Annual IGF Norway, "*Internet Resilience: Securing a Stronger Supply Chain*", highlighting systemic interdependence, electricity-digital infrastructure loops, and operational risk.
- Secured workshops at the 2025 and 2026 WSIS+20 High-Level Event in Geneva, reinforcing Resilient Infrastructure for a Sustainable Future.
- Held an online *Global Briefing* addressing pressing global challenges in Internet resilience and to set the stage for collaborative action through the Institute's working groups.
- Convened global leaders at the 2nd Annual IR Institute Experts Workshop and Forum from infrastructure providers, hyperscalers, financial institutions, utilities, and public-interest organizations to examine systemic vulnerabilities and produce practical tools toward a more resilient digital future.

The Institute's two flagship projects, the *Business Resilience Guide* and the *Internet Resilience Life of a Packet Mapping Exercise*, demonstrate the importance of multi-stakeholder partnerships, with continued expert engagement and renewed corporate funding, to continue positive momentum.

The Institute's progress has elevated the Marconi Society's standing in global resilience discussions. Its convening capability, combined with practical tools and credible expert leadership, positions the Society as a trusted actor able to bridge technical, operational, and governance communities.

The IR Institute continues to advance Internet resilience by convening global experts across technical, industry, and policy domains to identify challenges, foster collaboration, and drive actionable solutions for a secure, reliable, and accessible digital future.

Executive Summary

Internet resilience is a matter of global consequence. As digital connectivity becomes foundational to economic activity, public services, and human communication, all actors and institutions understanding their role and corresponding responsibilities to ensure the Internet remains reliable, secure, and resilient is essential.

This report presents the **Phase 1** findings and starting framework developed through the Marconi Society's IR Institute's *Business Resilience Guide* conducted under the auspices of the IR Institute's Hyperscaler Engagement Working Group. The purpose of this guide is to create a flexible, adaptable plan to help small and medium businesses maintain operations and communication effectively during unexpected challenges, tailored to their specific industry and needs.

The guide is now entering **Phase 2**, during which the starting framework and findings will be opened for broader community review and feedback to more fully capture the depth and complexity of Internet resilience across diverse global contexts.

Business Resilience Guide

Resilience Continuity Framework

The IR Institute's Hyperscaler Engagement Working Group set out to address the question: how can the operational discipline of hyperscalers be translated into practical, usable guidance for SMEs. Unlike large organizations with CISOs, engineering teams, and mature continuity processes, most SMEs are highly exposed to outages, misconfigurations, supply-chain failures, or local infrastructure disruptions, which are vulnerabilities that can cascade across entire economic networks, given SMEs' central role in global productivity.

In response, this working group set out to develop a guide distilling hyperscaler-grade resilience principles into accessible, actionable steps organized around four elements: awareness of Internet-layer dependencies, an impact-likelihood risk matrix with scenario tools, practical mitigation measures, and real-world case studies demonstrating how SMEs can strengthen continuity.

I. Availability Assessment Framework

A. Determine whether your organization needs to be available during unexpected outages and/or natural disasters
B. Evaluate organization's service level and 24/7 readiness response

II. Scenario Mapping and Case Studies

Prepare for potential disruptions, including:

A. Data loss
B. Remote work
C. Power outages
D. Natural disasters
E. Technology failures
F. Recovering from cyber attacks

III. Develop a Business Contingency Plan

A. Technology Infrastructure
    a. Cloud-based backup systems
    b. Remote access capabilities
    c. Resilient communication channels
    d. Disaster recovery tools
B. Communication Strategy
    a. Clear methods to inform customers/stakeholders about operational status
    b. Alternative communication channels during disruptions
    c. Ability to provide real-time updates
C. Practical Preparedness
    a. Backup payment methods
    b. Alternative work locations
    c. Redundant systems
    d. Staff training on emergency protocols

IV. Implementation Roadmap for Different Organization Types

A. Test and update your plan

Availability Assessment Framework

An availability assessment framework is based on a subset of the standard Business Continuity Assessment Framework[1] that has been tailored for SMEs to evaluate their exposure to incidents affecting Internet resilience and associated services (connectivity, DNS, cloud, SaaS, etc.). It's structured so organizations can quickly identify dependencies, assess impact, and decide on continuity measures that may be needed for their organization.

1. Map Internet-Dependent Functions

- List all business functions that rely on Internet services (e.g., email, cloud apps, VoIP, e-commerce, remote work).
- Classify them as:
  - **Mission-Critical** (must remain online)
  - **Important** (short downtime tolerable)
  - **Non-Urgent** (can pause without major impact)

2. Identify Internet Resilience Risks

The following are the most common Internet disruption scenarios that occur for SMEs:

- **Local ISP Outages**
  - Caused by infrastructure failures, maintenance, or weather events
  - Can halt access to cloud applications, email, and VoIP systems
- **Network Outages**
  - Caused by ISP infrastructure failures, internal hardware malfunctions, or cyberattacks
  - Can halt access to cloud applications, internal file servers, and VoIP systems
- **DDoS Attacks**
  - Targeted or collateral damage from attacks on shared hosting or service providers
  - Can overwhelm websites, APIs, or customer portals
- **Cloud Service Downtime**
  - Outages from providers like AWS, Microsoft Azure, or Google Cloud
  - Affects hosted applications, data access, and business continuity
- **SAAS Service Downtime**
  - Outages of business critical software (e.g., email, communication, accounting, payroll, supply)
- **DNS Failures**
  - Misconfigurations or attacks on DNS providers (e.g., cache poisoning, dangling DNS, DNS amplification, ghost domain delegations, and zone transfer leaks)
  - Prevents users from reaching websites or internal tools
- **Hardware Failures or Misconfigurations**
  - Routers, firewalls, or switches malfunctioning or misconfigured
  - Can isolate teams or block critical traffic
- **Cybersecurity Incidents**
  - Ransomware or malware infections that disrupt internet access or force shutdowns
  - Often require isolation from the network to contain damage
- **Power Outages**
  - Affect on-premise networking gear or local servers
  - Even with battery backups, extended outages can sever connectivity

[1] U.S. Department of Homeland Security. (2026, March). *Business Continuity Planning*. https://www.ready.gov/business/emergency-plans/continuity-planning.

To effectively operationalize a contingency strategy, it is essential for a SME to categorize risks by their potential impact and probability. The following Impact-Likelihood Risk Matrix serves as a diagnostic tool for distinguishing between low-frequency annoyances and high-impact systemic threats, ensuring that planning efforts are focused where they are needed most.

Likelihood / Impact	Rare (unlikely to occur)	Possible (could occur occasionally)	Likely (expected to occur)
Low Impact	Short local ISP outage; minimal disruption	Regional connectivity slowdown; minor delays in cloud access	Brief Wi-Fi or VPN disconnection; no major loss
Medium Impact	DNS misconfiguration detected early; limited user impact	Partial SaaS outage (e.g., Microsoft 365 down for hours); noticeable work disruption	DNS propagation issues (when updated records haven't yet reached all global servers due to cached data lingering until its TTL (Time to Live) expires) or upstream routing errors; temporary loss of availability
High Impact	Complete cloud provider failure (multi-region) – unlikely but severe	DDoS attack on primary website/API causing multi-day service outage	Major routing hijack, extended cloud downtime, or third-party dependency failure (payment gateway/CDN/ID provider) causing severe operational disruption

Figure 1. Impact-Likelihood Risk Matrix

Likelihood / Impact	Scenario	Mitigating Actions
Rare / Low	Short local ISP outage; minimal disruption	Dual ISP setup; 4G/5G failover; local caching of key data
Rare / Medium	DNS misconfiguration detected early; limited user impact	Secondary DNS provider; use managed DNS provider
Rare / High	Complete cloud provider failure (multi-region) – unlikely but severe	Multi-cloud redundancy; offsite data backup; vendor resilience testing
Possible / Low	Regional connectivity slowdown; minor delays in cloud access	SD-WAN deployment; optimize routing paths; monitor regional performance
Possible / Medium	Partial SaaS outage (e.g., Microsoft 365 down for hours); noticeable work disruption	Alternative SaaS providers; local fallback tools; data export readiness
Possible / High	DDoS attack on primary website/API causing multi-day service outage	CDN/WAF protection; rate limiting; upstream provider coordination

Likely / Low	Brief Wi-Fi or VPN disconnection; no major loss	Improved internal network monitoring; VPN redundancy; clear incident procedures
Likely / Medium	DNS propagation issues or upstream routing errors; temporary loss of availability	DNS failover automation; BGP monitoring; RPKI adoption
Likely / High	Major routing hijack, extended cloud downtime, or third-party dependency failure (payment gateway/CDN/ID provider) causing severe operational disruption	Vendor risk assessment; contractual SLAs; backup payment gateways and CDN providers

Figure 2. Practical Mitigation Measures for SMEs

3. Impact Assessment Matrix

For each function and risk area, assess the following:

Impact Area	Low Impact	Medium Impact	High Impact
Financial	<1 day revenue loss	1–3 days loss	>3 days loss
Customer Impact	Minor delays	Noticeable disruption	Major trust/contract loss
Regulatory	No breach	Minor compliance issue	Major fines/legal breach
Reputation	Minimal	Negative reviews	Long-term brand damage

4. Recovery Objectives

- **RTO (Recovery Time Objective):** Max downtime tolerated for each Internet-dependent service
- **RPO (Recovery Point Objective):** Max acceptable data loss if systems fail (e.g., 1 hr, 24 hrs)

As a best practice, SMEs should build and have a **checklist** for the first hour of a major incident (e.g., "Step 1: Get out the emergency contact list; Step 2: Notify the bank"). The current plan is too conceptual for a non-tech manager.

5. Continuity Requirement Decision

Assessment exercise:

- If downtime exceeding the RTO would cause high impact or severe harm, then Continuous Service is Required (e.g., redundant ISPs, failover DNS, or multi-cloud deployment).
- If downtime is tolerable and the impact is low, then Planned Recovery is Acceptable (e.g., manual workarounds or recovery within a few hours or less than one day).
- SMEs (Subject Matter Experts) can conduct a tabletop exercise by reviewing each Internet-dependent service, applying the impact matrix, and determining the appropriate continuity measures.

Scenario Mapping and Case Studies

Scenario mapping helps SMEs anticipate and prepare for potential disruptions that could impact business continuity. Each scenario should identify critical assets, assess potential consequences, and define mitigation or recovery strategies.

1. Local ISP Outages

- **Example Scenario:** A construction crew accidentally severs the primary internet fiber optic cable in your office park, causing a total loss of connectivity for the entire workday.
- **Mitigation:** Use two independent Internet providers or a 4G/5G failover router to maintain connectivity during an outage.
- **Best Practice:** Continuously monitor uptime with tools like Pingdom or UptimeRobot and configure alerts for disruptions.
    - **Reference Example**: 11 Best Uptime Monitoring Tools in 2025 (Ranked & Compared) - UptimeRobot Knowledge Hub

2. DDoS Attacks

- **Example Scenario:** An attacker launches a sophisticated volumetric DDoS attack against your primary website and customer portal, overwhelming your servers and rendering your online services inaccessible for several hours.
- **Mitigation:** Use a DDoS protection service (e.g., Cloudflare, Akamai) to absorb and filter malicious traffic.
- **Best Practice:** Apply rate limiting, geo-blocking, and web application firewalls (WAFs) through cloud security platforms like Cloudflare, AWS, or Azure for scalable protection.
    - **Reference Example**: Small businesses can follow this best practice by implementing rate limiting, geo-blocking, and WAFs through cloud-based security platforms like Cloudflare, AWS, or Azure, which offer scalable and easy-to-configure protections.

3. Cloud Service Downtime

- **Example Scenario:** A regional outage at a major cloud provider (e.g., AWS, Azure, Google Cloud) affects the availability of critical virtual machines, databases, and hosted applications, causing an immediate halt to mission-critical business functions.
- **Mitigation:** Use multi-cloud or hybrid cloud architectures to reduce dependency on a single provider.
- **Best Practice:** Regularly back up critical data and maintain offline access for essential workflows (e.g., local copies of key files or cached data).
    - **Reference Example**: Understanding Multi-Cloud Strategy for SMEs | Flexible & Resilient Cloud Solutions

4. SAAS Service Downtime

- **Example Scenario:** Your company's primary email, CRM, or accounting SaaS provider experiences an unexpected global service interruption, preventing employees from communicating internally or processing core business transactions**.**
- **Mitigation:** Backup Critical Data Regularly. Use automated backups or third-party tools to export and store data securely outside the SaaS platform.
- **Best Practices:**
    - Subscribe to your provider’s status page and incident feed.
    - Deploy tools that provide real-time alerts for outages or performance degradation.
    - For mission-critical functions (e.g., CRM, email, file storage), consider using multiple SaaS providers to avoid single points of failure.
    - Review vendor SLAs to ensure acceptable recovery time objectives.

5. DNS Failures

- **Example Scenario:** A misconfiguration during a domain name system (DNS) update or an attack on your DNS provider leads to domain resolution failures, meaning customers and partners cannot reach your website or connect to your cloud services.
- **Mitigation:** Use redundant DNS providers (e.g., Google DNS + Cloudflare DNS) to ensure domain resolution continuity.
- **Best Practice:** Implement DNS failover and test domain resolution quarterly.
    - **Reference Example**: Comprehensive Tutorial on DNS Failover in Site Reliability Engineering - SRE School

6. Hardware Failures or Misconfigurations

- **Example Scenario:** A core router or firewall in the office network fails unexpectedly, or an administrator applies an incorrect configuration, leading to a complete isolation of the internal network from the Internet and all cloud services.
- **Mitigation:** Maintain spare networking equipment and store baseline configurations for rapid recovery.
- **Best Practice:** Conduct regular hardware audits, apply firmware updates, and verify backup configurations.
    - **Reference Example**: Network Device Patch Management for Small and Medium-sized Businesses | SecOps® Solution

7. Cybersecurity Incidents

- **Example Scenario**: Malware encrypts critical systems, halting operations.
- **Mitigation:** Segment networks to limit lateral movement, enforce strong endpoint protection, and implement zero-trust controls (e.g., user authentication per resource).
- **Best Practice:** Run cybersecurity tabletop exercises and maintain a current incident response playbook.
    - **Reference Examples**: Zero Trust for SMBs | SMB Cybersecurity Guidance | CSA

8. Regional Issues, Natural Disasters and Power Outages

- **Example Scenarios**:
    - Floods, storms, or earthquakes disrupt power and network access.
    - Regional instability causes power disruptions, data center shutdowns, or supply chain breaks.
- **Mitigation:** Install uninterruptible power supplies (UPS) for all critical networking devices.
- **Best Practice:** Test power failover systems quarterly replace aging batteries, and consider portable generators for extended outages. Maintain regular communication with power delivery providers to ensure open communication channels. Ensure power supply reinstatement priority is understood and agreed by the utility.
    - **Examples**: Use UPS systems, portable generators, and cloud-based failover environments
- **Cross-Impact Note**: Natural disasters often lead to both *data loss* and *operational downtime*.

Governance

- Assign an Internet Resilience Owner (typically the IT Lead or Operations Manager).
- Create and maintain key personnel contact list and a critical communication media plan as necessary.
- Conduct annual testing of failover procedures (ISP switch, DNS cutover, SaaS outage simulations).

- Review and update the continuity plan annually or after major incidents.
- Track lessons learned and adjust strategies based on new technologies or dependencies (e.g., new SaaS platforms).
- Prioritize essential controls such as data backup, access management, and critical system redundancy. Identify non-essential expenditures that can be deferred without jeopardizing resilience.

1. Data Loss

- **Action**: Inventory all business data (customer information, financial records, operational systems). Quantify the business impact if this data is lost or corrupted.
- **Exercise**: Develop a *3-column Risk Matrix* listing (1) *Scenario*, (2) *Likelihood/Impact*, and (3) *Mitigation Strategies*.
- **Mitigation Examples**: Implement automated backups, test data recovery regularly, and use secure cloud storage with versioning.

SME Scenario: Securing Applications in the Cloud with Redundancy

Company: A 75-person SaaS startup offering a web-based project management tool for healthcare clients.

Challenge: As the company scales, it needs to ensure its application is secure, resilient, and compliant—especially as it handles sensitive customer data. While their cloud provider (e.g., AWS or Azure) offers built-in infrastructure redundancy, the team must still secure their own application layer and business logic.

How They Secure Their Applications

- **Application-Level Security**
  - Implemented role-based access control (RBAC) and OAuth 2.0 for user authentication.
  - Adopted secure coding practices and integrated SAST/DAST tools into their CI/CD pipeline to catch vulnerabilities early.
  - Deployed a Web Application Firewall (WAF) to block common threats like SQL injection and cross-site scripting.
- **Redundancy & Resilience**
  - Relied on the cloud provider's multi-AZ and multi-region failover for infrastructure-level redundancy.
  - Added application-level health checks and auto-scaling groups to ensure uptime during traffic spikes or node failures.
  - Used managed database services with automated backups and replication to prevent data loss.
- **Ongoing Protection & Monitoring**
  - Enabled rate limiting and geo-blocking to reduce exposure to bot traffic and high-risk regions.
  - Scheduled quarterly security audits and monthly patch cycles for dependencies and container images.
  - Leveraged cloud-native security tools (e.g., AWS GuardDuty, Azure Defender) for continuous threat detection and alerting.

SME Scenario: Cloud Outage

Impact Area	Likelihood	Severity	Risk Level	Mitigation Strategy
Customer Support	High	High	Critical	Use backup mobile hotspots; reroute to call centers
Cloud-Based Operations	Medium	High	High	Implement offline failover systems; local caching
Internal Communication	High	Medium	High	Enable SMS or alternate messaging apps
E-commerce Transactions	Medium	High	High	Notify customers; switch to manual order intake
Remote Work Access	High	Medium	High	Provide VPN alternatives; mobile data stipends
Security Monitoring	Low	High	Medium	Ensure local logging; backup alert systems
Data Sync & Backups	Medium	Medium	Medium	Schedule sync retries; use hybrid cloud storage
Social Media & PR	Medium	Low	Low	Pre-schedule posts; use mobile access
Financial Transactions	Low	High	Medium	Notify finance team; delay non-critical transfers

Figure 3. Internet Outage Risk Matrix

Conclusion

The Internet's resilience depends not on any single actor or technology but on the interconnected health of technical systems, supply chains, institutional practices, and human coordination. **Phase 1** of the *Business Resilience Guide* offers a roadmap for distributed resilience building that respects the Internet's architecture while addressing its systemic vulnerabilities.

Phase 2 requires sustained commitment, resource investment, and willingness to challenge assumptions about dependencies, threats, and responsibilities. Yet the alternative—continued fragmented approaches to resilience—risks significant failures with global consequences. Both work products represent a critical step toward ensuring the Internet's stability, security, and availability for the billions who depend on it daily.

This initiative's power lies in its multi-stakeholder foundation: bringing together operational expertise, policy perspective, and governance experience to produce practical, actionable guidance. No actor can address systemic risk alone; collective preparedness must become a deliberate, structured priority supported by cross-sector cooperation. To learn how to get involved with the Marconi Society's Internet Resilience Institute, visit marconisociety.org.

IR Institute Advisory Council Members

Fiona Alexander
Distinguished Fellow
American University

Maarten Botterman
Director
GNKS Consult BV

David B. Cross
CISO
Atlassian

Brian Cute
President and Chief Executive Officer
Global Cyber Alliance

Taher Elgamal
General Partner
Evolution Equity Partners

Olaf Kolkman
Principal, Internet Technology,
Policy & Advocacy
Internet Society

Victor Kuarsingh
Vice President
Capital One

Ram Mohan
Chief Strategy Officer
Identity Digital

Moritz Müller
Research Engineer
SIDN

Mark Nottingham
Standards Lead
Cloudflare

Shernon Osepa
Senior Caribbean Telecommunications and
Internet Governance Strategist

Ramakant Pandrangi
SVP, Architecture and Engineering
Verisign

Radia Perlman
Fellow
Dell Technologies

Paul Vixie
Distinguished Engineer

Dan York
Senior Director, Online Trust & Safety
Internet Society

IR Institute Working Group Members

Fiona Alexander
Distinguished Fellow
American University

Maarten Botterman
Director
GNKS Consult BV

David B. Cross
CISO
Atlassian

Brian Cute
President and Chief Executive Officer
Global Cyber Alliance

Damian Huising
AI & Security Lead
Ready.net

David Huberman
Technical Engagement Director
ICANN

Darren Kara
Principal Engineer
Quad9 DNS

Olaf Kolkman
Principal, Internet Technology,
Policy & Advocacy
Internet Society

Victor Kuarsingh
Vice President
Capital One

Angelique Medina
Head of Internet Intelligence and
Product Solutions Architecture
Cisco ThousandEyes

Ram Mohan
Chief Strategy Officer
Identity Digital

Shernon Osepa
Senior Caribbean Telecommunications and
Internet Governance Strategist

Jeff Simmons
Founder and Principal
Simmons Energy Advisors

Mimi Tam
Author & Adjunct Professor, Computer Science
Boston College

Dan York
Senior Director, Online Trust & Safety
Internet Society

Marconi Society Contacts

John R. Janowiak
President and CEO
john@marconisociety.org

Flora Tromelin
EVP, International Engagement
ftromelin@marconisociety.org

Marina Pappas
Institute Director
mpappas@marconisociety.org

Barry Sullivan
Institute Director
bsullivan@marconisociety.org

Elizabeth Hibbler
Institute Director
ehibbler@marconisociety.org

Yeimidy Lagunas
Director, Communications and Membership
ylagunas@marconisociety.org

Jaymee Bohannon
Executive Relations
jbohannon@marconisociety.org