The Marconi Society

INTERNET RESILIENCE FRAMEWORKS FOR COORDINATED GLOBAL ACTION

A Supply Chain and Operational Resilience Assessment of Global Internet Infrastructure
Phase 1 Report, Marconi Society Internet Resilience Institute

INTERNET RESILIENCE INSTITUTE

June 25, 2026 | marconisociety.org

Internet Resilience Frameworks for Coordinated Global Action

A Supply Chain and Operational Resilience Assessment of Global Internet Infrastructure
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 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 findings and starting framework developed through the Marconi Society's Internet Resilience (IR) Institute's *Life of a Packet Mapping Exercise* conducted under the auspices of the IR Institute's Supply Chain Mapping Working Group. The purpose of this exercise is to systematically identify and analyze "from a 30,000ft view" the complex, interconnected components that collectively underpin the resilience of the modern global Internet—spanning service and control functions, physical and transport infrastructure, and the broader ecosystem of dependencies such as power, cybersecurity, equipment supply chains, and financial flows.

Additionally, this report presents the 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.

This report presents the findings of **Phase 1** by introducing both a preliminary guide and a visual mapping model representing Internet infrastructure, service flows, and critical dependencies. The *Business Resilience Guide* distills hyperscaler-grade resilience principles into accessible, actionable steps. The *Mapping Exercise* uses real-world communication scenarios to ground abstract infrastructure concepts in practical, recognizable contexts, making the findings relevant and accessible to a broad range of global stakeholders. The efforts of both working groups are now advancing into **Phase 2**, during which the starting framework and findings of each product will be opened for broader community review and feedback to more fully capture the depth and complexity of Internet resilience across diverse global contexts.

The Mapping Model - Life of a Packet Exercise

Layering Framework

The suggested IR mapping follows a layering where the Internet Resilience Mappings are split into upper and lower layers as well as mappings to key dependencies. The "layering" described in this exercise is conceptual and should not be confused with traditional protocol layering models such as the OSI stack. Within this context, layering is a way to identify functional groupings that affect the customer experience. The two primary layers are defined as follows:

- **Upper Layer – Service & Control**: Functions that directly interact with, influence, or participate in the primary application flow. These are the elements most visible to the end user.
- **Lower Layer – Physical & Transport**: Functions and networks that are essential but operate transparently to the main application flow. They support the experience but are not directly visible to the customer.

Within this model, there are primary communication flows for things like a WhatsApp message, Zoom call, social media update, or banking transaction, that directly interact with upper layer networks supported by a variable set of upper layer functions such as trust mechanisms, proxies, firewalls, and load balancers.

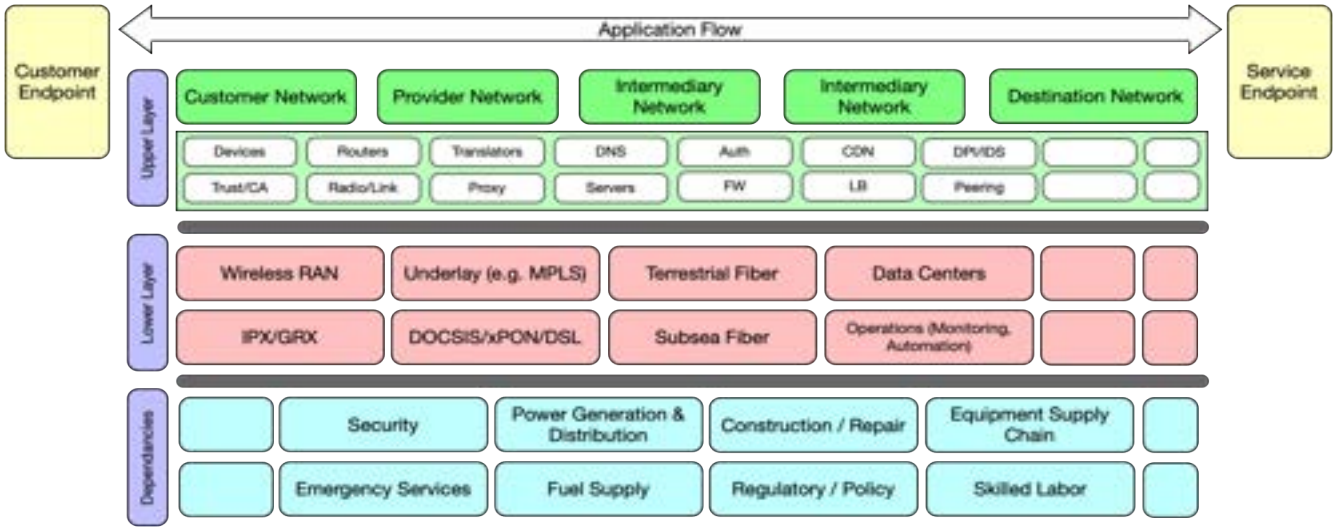

Figure 1. Internet Resilience Layering Framework

Below the upper layers are abstracted, but relevant, lower layer infrastructure elements that often have complex networking, interactions, and operational needs supporting upper functions. An example of this is the IPX (IP eXchange) interconnect global exchange, which supports network services access for roaming wireless customers.

Dependencies

Dependencies are abstracted supporting needs that are not directly related to upper or lower layer functions, but are needed to maintain communication flows at both runtime and during event (outage) periods. The dependency layer can be thought of as the power, water, machinery, supply chains, governance frameworks, and other infrastructures without which the Internet cannot operate.

Key examples identified in **Phase 1** include:

- **Power Generation & Distribution**: Needed to support data centers, access and other networks. Impairments, outages and instability of this function can disrupt or prevent Internet flows.
- **Fuel Supply & Equipment Supply Chain**: More specific to data center and provider operations, but if not available or impaired, could impact operations or service redundancy.
- **Security**: Needed to protect physical assets in the field and within key premises including locks, vaults, shielding and coverings preventing damage or malicious intrusion. Active security personnel and processes are most often needed to prevent the larger infrastructure from invasion, vandalism, and sabotage.
- **Financial Flows**: Need to be reliable to ensure transactions in the value chain take place and to make sure all resources needed for the process remain available.
- **Cybersecurity Ecosystem**: Encompasses not only technologies but also organizational practices, processes, and capabilities such as running a Security Operations Center (SOC) in support of ensuring smooth and continued operations.

Scenario Analysis: Zoom Call from Cape Town to London

Scenario Description

To ground the mapping model in a practical, real-world context, Phase 1 developed a detailed scenario analysis built around a common, globally recognizable use case. Here, working group members chose to map a Zoom call from Cape Town, South Africa to London, UK, with the caller in South Africa on the mobile network (roaming) calling their parents back in London. This scenario was selected because it traverses multiple network types, international boundaries, and infrastructure layers – making it a rich illustration of Internet supply chain complexity.

Assumptions for this mapping include use of a roaming over [remote] Wireless Network, Radio Access Network (RAN), Intermediary Tier 1 network, destination provider network with broadband, remote wireless provider network, and Cloud Service Provider.[1]

Supporting (non-exhaustive) upper layer functions include NAT translation at the home wireless network PGW, public key exchange, Global Server Load Balancing (GSLB) functions for Zoom, load balancing and firewall functions for the Zoom cloud hosted Multimedia Relays (MMRs), public DNS service, and inter-network peering. Supporting (non-exhaustive) lower layer functions include the sub-sea fiber, landing stations, terrestrial fiber, remote network RAN, 3GPP DNS service, and regional cloud service provider metro area network.

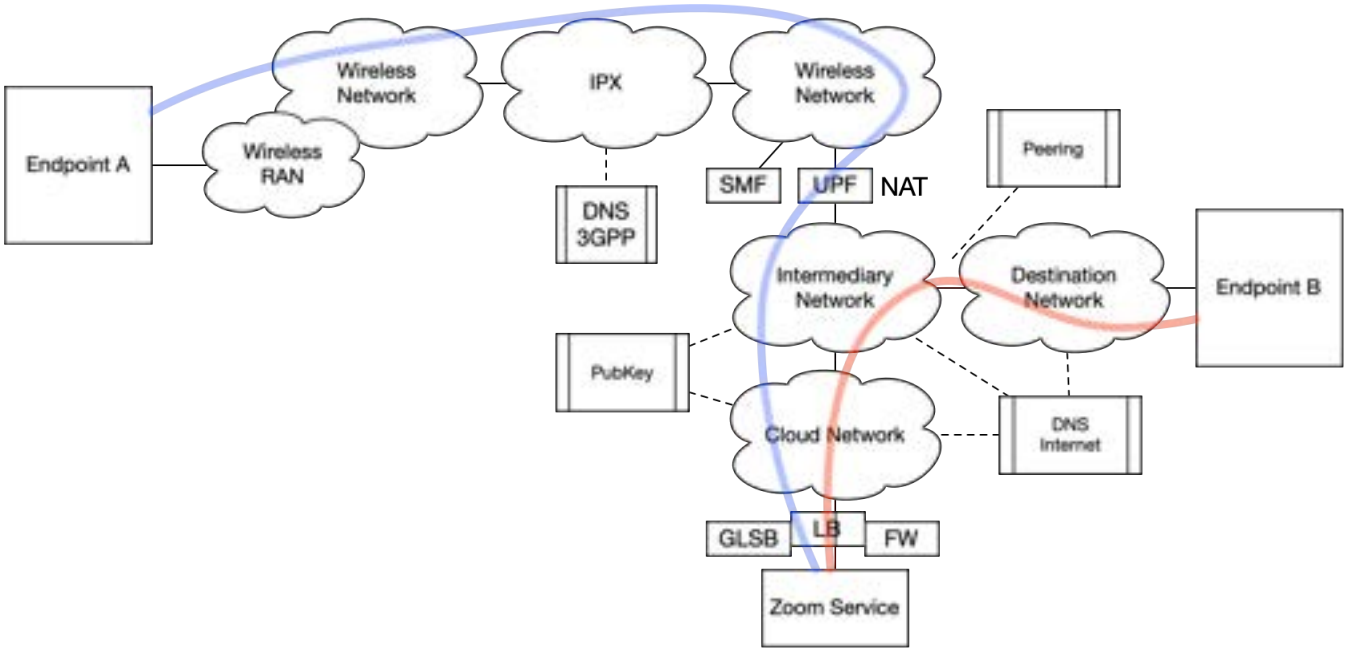

Figure 2. Cape Town to London Zoom Call Flow

Upper Layer: Primary Application Flow

The primary application flow includes endpoint-A (handset), remote OS (e.g. IOS/Android), Mobile Gateway, home wireless provider network, peering to intermediary, intermediary network, cloud provider overlay, intermediary to destination network, access to endpoint-b and endpoint-b operating system (e.g. macOS/Windows).

[1] This example does not show local breakout in South Africa should Endpoint A move off the microcellular network onto a local provider network. The model also assumes that sub-sea cabling is used by the IPX or one of the wireless networks to move from South Africa to the UK.

Underlay Analysis: Wireless and Cloud

Working group members mapped supporting system flows for this particular use case to include remote wireless network, interconnection to IPX to home network from the customer handset to the SMF/UPF.

Wireless Underlay

The wireless network has a large set of functions that operate at the underlay and are transparent to the application flow. The (typical) wireless endpoint (UE) connects through RF to tower, RAN (Radio Access Network), and packet core towards a PGW (LTE) / UPF (5G). That connection creates a bearer plane or tunnel that effectively looks like one hop to the endpoint flow. Connection setup delay, latency, quality all impact the upper layer flow, but would be transparent from an application's perspective so to the nature of the connection.

The wireless network described here directs traffic from the wireless endpoints through various radio base stations, which may change as the endpoint moves, through the RAN network that is most often an IP network that directs traffic throughout a topology, then through the packet core connecting control plane and data plane traffic endpoints.

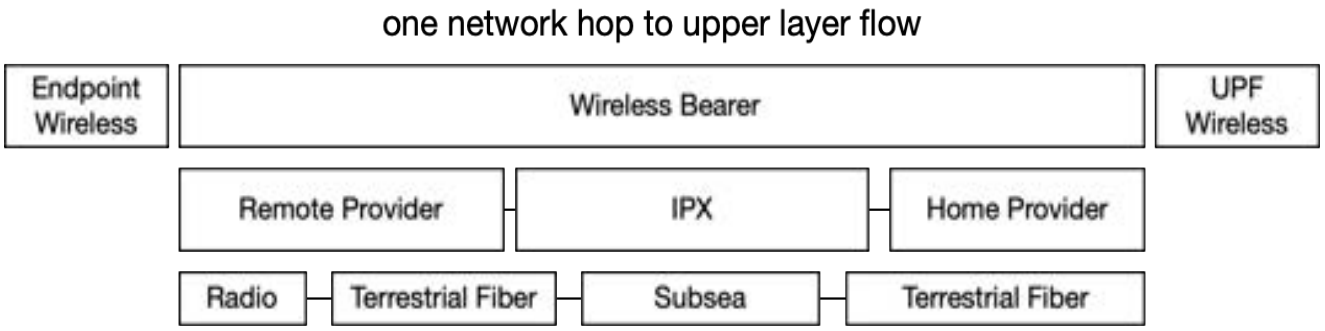

Figure 3. Wireless Underlay Network

The 5G use case architecture is seen below (taken from 3GPP 23.501) showing the visited network (where use is roaming) and home network (actual paid provider of the person with the cellular plan).

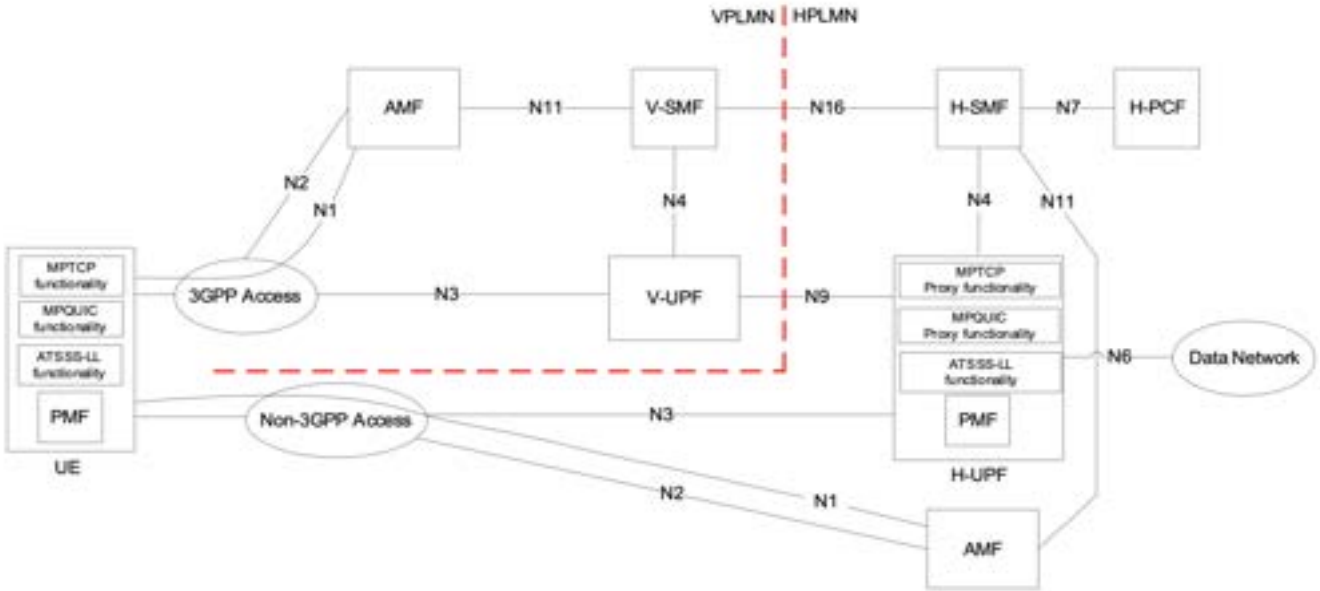

Figure 4. 5G Use Case Architecture

The **5G Roaming Connection Sequence** follows the architecture defined in 3GPP 23.501[2] and proceeds as follows:

1) UE Registration and PDU Session Establishment.
2) UE Sends PDU session establishment via AMF in the visited network.
3) V-AMF contacts H-SMF (via SEPP/N32 signaling if inter-PLMN).
4) H-SMF allocates the PDU Session ID, selects an H-UPF, and instructs the V-SMF to instantiate a V-UPF via N16.

V-SMF and H-SMF Signaling:

- The V-SMF acts as a "proxy SMF" to the H-SMF.
- It translates local access parameters and establishes a tunnel toward the H-UPF.
- The H-SMF uses N4 to configure the H-UPF, defining QoS, PDRs, and forwarding rules toward the V-UPF.

UPF Interconnection (User Plane):

- The N9 interface is used between V-UPF and H-UPF.
- User packets are GTP-U encapsulated, maintaining PDU session integrity across PLMNs.
- The H-UPF becomes the anchor toward the Data Network (DN) (e.g., internet or enterprise network).

Given the connection is based on a roaming case, there is an intermediary network that supports IPX (IP eXchange) functions that allows traffic to flow between wireless network providers and is governed by the GSMA (GSM Association). Since the flow is between networks on different continents, the intermediary network (e.g. Syniverse) would also have connections over terrestrial and sub-sea connectivity.

Cloud Underlay

The cloud underlay operates independently from the main application flow and is a set of networks and infrastructure that provides support for overlay networks (upper layer). The lower layer is generally comprised of internet facing connectivity that includes peers and potentially transport. Upper layer functions include perceived gateways, firewalls, load balancing functions to connectivity to the service endpoint. That endpoint can be a VM, container or other service element.

Below the overlay is a separate set of network functions which include POPs, metro interconnects, routing infrastructure and data centers that support the substrate elements. The substrate is often built using interconnecting fabrics dedicated for multiple functions such as metro wide interconnections between data center-based fabrics.[3] Those data center fabrics typically support local data center connectivity.

A typical flow at the substrate layer would or could be:

Encapsulation endpoint (gateway) → POP fabric → metro fabric → metro interconnect → metro fabric → local DC fabric → server/compute → Encapsulation endpoint.

Cloud networks are built typically facing the Internet. The top elements interact with the application flow, whereas the substrate does not directly, and is not perceivable by the main application flow.

---

[2] 3GPP, "System architecture for the 5G System (5GS)," 3GPP Specification #23.501, Version 20.1.0, March 2026. (https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144).

[3] The regional network substrate composed of metro/WAN routing/routers, fabrics, optical transport and supporting services/functions.

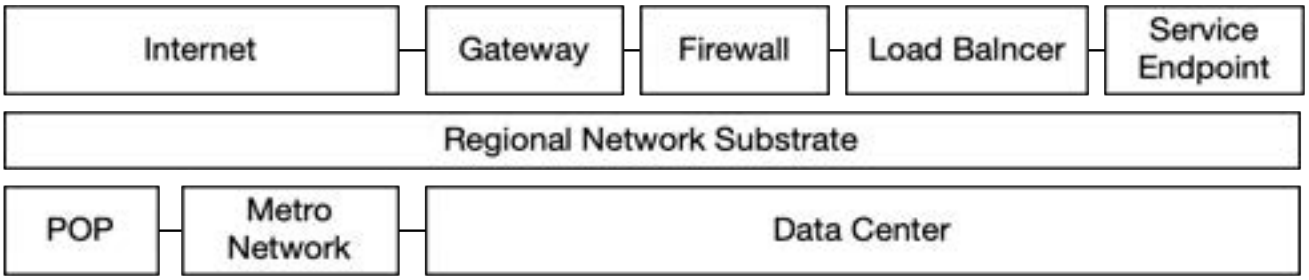

Figure 5. Cloud Network Overlay, Substrate and Underlay

Failure Use Cases

Failures to an upper or lower layer operation are often intertwined with dependencies in normal operations and failure modes. Below are two examples based on real life situations, with details obfuscated from any one specific event, for discussion and consideration. Both examples look at Internet disruption from the vantage point of a power event and a vandalism event.

Disruption Use Case: Data Center Power

Data Center hosting multi-media service endpoints supporting customers. Transmission / feeder sub-station has a blown transformer removing utility power - single three-phase feed - to the data center. To remain "up" without disruption, UPS batteries take over while generators start-up to take load and remain running until utility is restored.

What can go wrong here? (examples of non-Internet level issues)

- UPS battery farm was not maintained, did not take [full] load
- Generators were not tested, did not fire up, and power fails after UPS depletion
- Diesel fuel is unavailable or undeliverable to site, site loses power after on-site reserves exhausted
- Failed power, network equipment cannot be replaced with local supply chain
- Failed power/cooling, components are unavailable to repair on-site models/equipment
- Operations staff was untrained / unable to manage event, resulting in failed power moving back to utility

Disruption Use Case: Vandalism or Construction Led Connectivity Cut

Terrestrial Fiber Plant supporting intra-city and inter-city connectivity for multiple providers. A group of malicious actors, in a coordinated event, enter fiber vaults and access ways over a 20KM radius and purposely cut fiber impacting multiple operators primary and redundant paths simultaneously. Transport systems and networking systems detect failures, but overall service is impacted. In this case, it is expected that some service providers will have partial and full outages. The goal here is how well are systems monitored, operated and access to repair teams.

What can go wrong here?

- Operators that own the fiber paths may have poorly documented locations of fiber paths including failure to document changes
- Network operators do not have sufficient operational muscle to adequately detect failure or help isolated failure
- OTDRs (Optical Time Domain Reflectometry) cannot be run
- Repair crews are inadequately staffed or at ready to deploy to various cut points throughout the city/region
- Insufficient security is available to protect/guard the repair locations following re-splicing

- Following repair and equipment failure, some transport equipment cannot be repaired as insufficient local depot supply exists requiring out of region inbound shipping
- In some regions, inbound supply subject to national brokerage, and therefore cannot be delivered in an emergency

Business Resilience Guide

Resilience Continuity Framework

While the failure use cases above illustrate the systemic vulnerabilities inherent in global infrastructure, the following *Business Resilience Guide* applies these insights to provide actionable, practical strategies for small and medium-sized enterprises (SMEs) to ensure operational continuity.

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

Identifying Risks

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 6. Impact-Likelihood Risk Matrix

Critical Scenarios and Mitigation Best Practices

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.

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; 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 7. Practical Mitigation Measures for SMEs

Several key insights emerged from hyperscaler experiences and adapted for the SME context in **Phase 1**:

(1) Concentration risk remains largely invisible. Many SMEs believe they are protected by redundancy, but in practice their "independent" connections often share that same physical trench or upstream infrastructure. This creates hidden single points of failure that only become obvious during a crisis.

(2) Resilience requires testing. A backup connection, a mirrored server, or a cloud failover plan is meaningless if it has never been exercised. Hyperscalers routinely test failure scenarios; SMEs rarely do.

(3) Distributed models increase resilience. Workloads, data storage, and connectivity pathways benefit from diversification, not only for performance but to mitigate systemic risk.

(4) Cloud interoperability remains a barrier. Despite the rhetoric of multi-cloud strategies, moving workloads across providers remains deeply challenging. Standards for interoperability are still immature, limiting SMEs' ability to adopt resilient architectures.

(5) Transparency builds trust. Industry best practices should include outage disclosures, detailed post-incident analyses, and explicit corrective actions. A culture of transparency strengthens resilience ecosystems by allowing others to learn from each failure.

For a more in-depth exploration of the topics covered in this framework, scan the QR code to access the detailed version of the *Business Resilience Guide*.

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 two work products, *Business Resilience Guide* and *Supply Chain Life of a Packet Mapping Exercise*, offer 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 more about the two products and 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

2026 MARCONI AWARDS GALA & INSTITUTE FORUMS

FAIRMONT SAN FRANCISCO
NOVEMBER 4-6, 2026

The 2026 Marconi Awards Gala & Institute Forums brings together the brightest minds in technology, from pioneering researchers and global executives to policymakers, academics, and innovators, for a convergence of ideas, dialogue, and impact.

The convening culminates with the Marconi Awards Gala, honoring Robert Calderbank, the Marconi Prize recipient, John Hennessy, Lifetime Achievement Award recipient, and the next class of Paul Baran Young Scholars.

KEY THEMES

Cross-Sector Institute Forum: Where Wireless, AI, and Internet Resilience Meet

Trust & Safety

How do we build and maintain trust in the systems, algorithms, and networks that billions of people depend on every day?

Infrastructure & Energy Transformation

How do we build, power, and sustain the massive physical and digital infrastructure that next-generation connectivity demands without resulting in global disruptions?

Internet Resilience

How do we ensure the Internet remains open, trustworthy, and functional in the face of escalating disruptions for every person who depends on it?

SAVE THE DATE

APWireless ARIN American Registry for Internet Numbers ATLASSIAN

aws Comitato Nazionale Marconi 150 cohere technologies

Coalition on Digital Impact Duke Quantum Center ECE FOUNDATION

EDGE Fondazione Guglielmo Marconi IEEE-Eta Kappa Nu HKN

identity digital KPMG ncta THE INTERNET & TELEVISION ASSOCIATION

San Francisco Center for Economic Development STDN VERISIGN

SPONSORSHIP OPPORTUNITIES
FLORA TROMELIN
FTROMELIN@MARCONISOCIETY.ORG

SPEAKING OPPORTUNITIES
MARINA PAPPAS
MPAPPAS@MARCONISOCIETY.ORG

2026 MARCONI AWARDS GALA

Celebrating the Past, Catalyzing the Future

NOVEMBER 6, 2026
FAIRMONT SAN FRANCISCO
6:00PM RECEPTION | 7:30PM AWARDS & DINNER

Paul Baran
Young Scholar Award

2026 Marconi Prize Recipient
Robert Calderbank

Lifetime Achievement Award
Recipient
John L. Hennessy

2026 Marconi Awards Gala

Held at the historic Fairmont San Francisco, the evening honors the 2026 Marconi Prize recipient, the Marconi Society Lifetime Achievement Award, and recognizes the next generation of leaders advancing information and communications technology.

Learn More

Marconi Society Lifetime Achievement Award

John L. Hennessy has been named as the recipient of the Marconi Society Lifetime Achievement Award. The award recognizes individuals with an established history of distinguished work who, during their lifetimes, have made creative contributions and a positive impact to the field of communications and to the development of the careers of others.

Marconi Prize

Robert Calderbank is recognized for pioneering contributions to the theory and practice of voiceband modems, space-time coding, and quantum error correction. Marconi Fellows carry forward the legacy of Guglielmo Marconi, whose breakthroughs opened the door to global communication and continue to shape the technologies that define modern life.

Paul Baran Young Scholars

The Paul Baran Young Scholars program honors emerging leaders whose research demonstrates exceptional innovation, leadership, and a commitment to technology that benefits humanity.

The Marconi Society

The Marconi Society is a 501(c)(3) nonprofit dedicated to building communities of leaders and stakeholders at the forefront of emerging technology, so that together we can create a more connected and sustainable world.

Book at the Fairmont