The Marconi Society

# INTERNET RESILIENCE

## Technology Institute Report

November 2024

marconisociety.org

# Table of Contents

# 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.

Throughout our 50-year history, we have celebrated the innovators, both established and emerging, who have shaped our connected world. Our technology institutes provide a platform to convene our network of visionaries to collaborate to identify, assess, and recommend ways to ensure that emerging technologies benefit society.

*The invitation-only, global experts workshop on Internet Resiliency took place in November 2024 at the National Academy of Sciences (NAS) in Washington DC, USA.*

**Executive Summary**

The Internet Resiliency Workshop brought together over 30 experts to examine critical challenges facing Internet infrastructure resilience. A Marconi Society Internet Resilience Institute initiative, the workshop's objective was to discuss **the resilient Internet we all want, and how to get there.** The gathering was held under the Chatham House Rule, with the exception that participants can be identified, though no attributions are to be made to individuals or entities.

**The Internet's fundamental technical architecture continues to provide a solid foundation. However, discussions identified areas for ongoing refinement and strengthening, specifically within the Border Gateway Protocol (BGP) for Internet address routing, the Domain Name System (DNS), and the Certificate Authority (CA) system.**

The workshop identified four primary threats: increasing system complexity, intensifying regulatory pressures, insufficient funding for preventive measures, and software supply chain vulnerabilities. For instance, the interdependence between electrical power and Internet infrastructure creates a "circle of dependencies" where each requires the other to function. Modern software development practices have introduced a "crisis of complexity," with applications depending on numerous APIs and third-party services whose security is often indeterminate.

The regulatory landscape emerged as perhaps the most pressing challenge, with policy issues expected to influence Internet development over the next 10-20 years in a more direct way than before. The relationship between technical operators and government policymakers and regulators has become strained as Internet and Internet-enabled services are now embedded in every aspect of modern life. The technical community's traditional approach of fixing problems as they arise is now politically untenable. Governments demand clear accountability and quick responses to incidents given the impact of the Internet on all aspects of the economy and national security. There is a clear need to build and maintain constructive public-private partnerships.

The workshop revealed a fundamental tension in how resilience is funded and prioritized. Participants repeatedly emphasized that "resilience is a prevention problem, and prevention does not attract money." While reactive measures to incidents readily attract funding and attention, the crucial work of preventing failures through good operational practices, proper training, and systematic thinking about dependencies is often underfunded. This challenge is compounded by information asymmetry between different stakeholders – operators, regulators, and users often have different levels of information and understanding about incidents and their causes.

The software supply chain emerged as a critical concern, with participants noting widespread dependence on poorly validated and under-funded open-source libraries. This led to recommendations

for developing systematic curricula for Internet-scale infrastructure operations, moving beyond the current reliance on anecdotal "war stories" for training. The workshop identified key audiences including network operators, engineers, and C-suite executives (CIOs, CFOs, CISOs), with regulators and policymakers as important secondary audiences globally.

The workshop established nine comprehensive workstreams addressing best practices, accountability protocols, infrastructure support mechanisms, operational practices, and talent development:

1. **Best Practices Framework/Badges**
2. **Accountability, Agency and Risk Management**
3. **Create a group, process or funding mechanism to support critical infrastructure**
4. **Build and Promote "Always Be Rolling" Program**
5. **Collaborative Exercises and Information Sharing**
6. **Infrastructure and Sectoral Dependencies**
7. **Education and Talent Development**
8. **Governance and International Collaboration**
9. **Evolving Resilience Goals**

These initiatives aim to balance immediate operational needs with long-term strategic goals. The workshop emphasized connecting resilience efforts to business metrics like Service-Level Agreements (SLAs) and customer experience, while noting the challenge of justifying investment in infrastructure components that appear low value until they fail. The Marconi Society was designated to serve as a channel for raising awareness rather than implementing technical solutions directly. Discussion included plans to produce a comprehensive paper providing concrete examples and evidence for stakeholders and convening follow-on meetings that advance the understanding of these topics.

**In conclusion, participants agreed that to get the resilient Internet we want, a few important things must happen: 1) improved dialogue between technical experts and policymakers; 2) better incident response frameworks; 3) systematic approaches to identifying and managing complex interdependencies; and 4) learning from best practices in other industries (for example, power, telecom). Research should be conducted to evaluate best practices in other critical infrastructure sectors, including inviting relevant experts in those fields.**

The workshop recognized that Internet resilience is part of a complex interdependent system and that dependencies must first be identified to provide a foundation for future building blocks. The path forward involves partnering across sectors with technical organizations, academic institutions, civil society organizations, and Internet governance bodies to amplify the message and reach key

stakeholders, while addressing the persistent challenge of funding preventive measures over reactive responses.

**Workshop Structure and Agenda**

The Marconi Society convened thirty subject matter experts from academia, industry, and the technical community at large over a day and a half to address current Internet fragility and points of failure, and to outline opportunities and concrete ways to bolster resilience, especially in light of emerging and frontier technologies. The workshop was organized around smaller breakout groups to engage participants and give them ample opportunity to contribute to the discussions.

The agenda shown below provides an outline of how the workshop was structured to achieve the goals described above. Each of the breakout groups was led by an expert in the subject areas covered, with a scribe assigned to each group to take detailed notes. Following each breakout session, the full group reconvened for readouts by the breakout leaders and facilitated discussion to arrive at common themes and recommended actions.

***Workshop Day 1***

The first day of the workshop included an opening panel session to provide an overview of the topics to be discussed in the breakout sessions that filled most of the day:

- Welcome, Introductions and Workshop Overview
- Opening Session
    - This panel discussion explored the current state of the Internet's resilience, highlighting areas of vulnerability and interdependencies that need to be addressed and existing initiatives that are underway. The panelists engaged in an interactive discussion regarding what Internet resilience meant, primary concerns about the resiliency of the network, and the processes needed to ensure its ability to withstand shocks. They also shared their views on worst-case scenarios and approaches to counter them. The opening session set the stage for the in-depth breakout groups' work.
- Morning Breakout Discussions
    - The thirty participants were divided into four breakout groups of 7-8 experts each.
    - The breakout discussions gathered the perspectives of the experts for contribution to the larger group discussions/debates and identified concrete actionable recommendations to include in this report.
    - Discussion topics
        - **Defining Internet Resilience:** Focus on defining what comprises Internet Resilience and developing a proposed definition as an outcome of this workshop to help further and deepen discussions and develop strategies and design approaches to ensure the Internet's resilience is strengthened for the future.
        - **Routing System & DNS:** Brainstorm and share perspectives on a series of questions related to the vulnerabilities in the routing system today, new potential

failures in the future, what needs to be done, how and by whom. Areas of focus include identification of points of fragility, dependencies in the routing system and restoration processes.

- **Subsea Cables & Physical Infrastructure:** Identify infrastructure weaknesses such as single points of failure, and exchange views/responses to a set of questions that focus on what needs to happen, how and by whom. The areas for discussion include identification of the dependencies, unintended and intended failures, and possible restoration solutions.
- **Elements of Resilience More Broadly:** Identify other critical elements of resilience that need to be addressed toward the future because of geopolitical developments or technology advancements. Given the Internet's multiple layers, the discussion will 'white board' critical points of potential failure in other aspects of the system e.g. hardware, software, supply chain, governance, and operational aspects.

- Morning Session Readouts and Facilitated Group Discussion
- Afternoon Breakout Discussions
  - A deeper dive into the topics, driving towards concrete measures, recommendations, and actions
- Afternoon Session Readouts and Facilitated Group Discussion
- Day 1 Closing and Next Steps

***Workshop Day 2***

Following an evening to reflect on the discussions of the first day, the workshop participants reconvened on the morning of Day 2 to recap the previous day's work and consolidate the recommendations in preparation for this report:

- Workshop Day 1 Recap
- Facilitated discussion and Identification of recommendations
- Report Planning and discussion regarding how to get the messages heard around the world by those who need to act on the recommendations
- Closing Remarks and Adjourn

**Opening Session Panel on Resilience**

This panel discussion revealed deep concerns about the evolving challenges to Internet resilience, with a particular focus on the growing tension between technical operators and government regulators. Policy issues, more than technical challenges, will define the Internet's future over the next 10-20 years. Governments want systems to work and need to be able to explain problems to constituents. However, the relationship between government and industry has become increasingly strained.

The panelists identified several critical threats to Internet resilience. These included the "circle of dependencies" between power and Internet infrastructure, increasing centralization of services, and "a crisis of complexity" in modern application development, where applications might depend on 30-40 different APIs without consideration for resilience. Panelists were concerned about single points of failure in all layers of the Internet. They highlighted three challenges:

1. Increasing regulation around competition and privacy,
2. Centralization creating chokepoints, and
3. "Security-induced ossification" where cybersecurity mandates make it difficult to evolve protocols and services.

The discussion revealed significant disagreement about prioritizing threats. When asked to identify the most important issue, responses ranged from regulation to restoration capability to single points of control. Some panelists argued that Internet resilience is a complex systems problem that cannot be reduced to single issues. A particular concern emerged around the changing expectations of reliability. The traditional technical approach of "things just break; we'll fix it" is no longer acceptable to governments and users. Following the assertion that "95% of the problem is regulation," the argument was made that while these issues are solvable, the technical community has not done enough to maintain strong working relationships with policymakers about how the Internet works and the implications of their policies. Incentives for private sector action are also missing and industry inaction, or the perception of it, is often driving poor policy choices. Continued focus on ‘resilient to what’ is needed.

**Breakout Discussions**

The readouts from the breakout discussions revealed a common thread: the tension between technical solutions and human factors and governance in maintaining Internet resilience. Whether discussing the preservation of collaborative culture, the transfer of operational knowledge, or the challenge of working with governments, the most pressing challenges combine organizational, governance, and social elements, in addition to technical ones.

Another common theme across all the breakout groups was the recognition that improving resilience requires both technical and organizational solutions, with particular emphasis on creating the right incentives for different stakeholders. Selling these ideas requires crafting different narratives for different audiences based on their specific incentives. The groups also highlighted the importance of understanding infrastructure dependency loops and unexpected coupled dependencies between different sectors (e.g., between Internet and electricity networks – no power, no internet connection – no data, no power).

Notes taken during the breakout sessions and the facilitated discussion that followed were compiled and organized around common themes, specifically considering this is one world we share, in which diversity and inclusion must be considered. Nine key themes were identified:

1. Best Practices Framework/Badges
2. Accountability, Agency and Risk Management
3. Create a group, process or funding mechanism to support critical infrastructure
4. Build and Promote “Always Be Rolling” Program
5. Collaborative Exercises and Information Sharing
6. Infrastructure and Sectoral Dependencies
7. Education and Talent Development
8. Governance and International Collaboration
9. Evolving Resilience Goals

**Key Themes and Recommendations**

***Theme 1. Best Practices Framework / Badges***

Consensus around developing a framework for identifying best practices for resilience emerged, coupled with a system for validating resilience capabilities and awarding badges for compliance. This would represent a shift from process attestation to measuring and validating recovery capabilities.

Such a framework should also promote continuous improvement by using a "crawl, walk, run" maturity model to guide organizations toward higher resilience standards. In addition, the framework should be adapted to industry-specific needs while ensuring consistent benchmarks. Resilience scales (e.g., 1-5, logarithmic, etc.) should be defined for diverse scenarios, ranging from minor network outages to large-scale natural or human-created disasters. Demonstrating resilient workload behaviors and best practices will be key to standards development.

Resilience certification can follow existing models such as the Cybersecurity & Infrastructure Security Agency (CISA) attestation process for secure software development or the Payment Card Industry (PCI) compliance regulations, with badges awarded to reflect resilience readiness and encourage accountability. A well-defined certification process may also help regulators understand the framework it implements and adopt it for oversight and evaluation.

There will be challenges to creating and implementing a Resilience Framework. For instance, aligning diverse objectives across industries, balancing flexibility with standardization to ensure the framework remains robust yet adaptable will be challenging aspects.

*Recommendation: Explore the creation of a Resilience Framework to validate resilience capabilities and promote continuous improvement. This could be visually represented by a badge of some type. As a first step, recognizing this as a valid framework has value in itself, because not adhering to it could be seen as "negligence" in case of harm done.*

***Theme 2. Accountability, Agency, and Risk Management***

Accountability for resilience must be clearly defined at all levels, from industry executives to their boards, and integrated into industry standards. In addition, implementation of risk management frameworks covering design, maintenance, protection, governance, and recovery must be promoted, also in the case of actions by (semi-)autonomous systems (e.g., AI driven). Finally, transparency in assessing and providing agency in managing resilience without exposing vulnerabilities to malicious actors should be encouraged.

The importance of dialog and communications between government and industry as an essential element of building accountability, agency, and addressing risk management was stressed.

*Recommendation: Clearly define accountability for resilience at all levels, from executives to boards to industry standards. Build resilience as a key aspect of Risk Management at all levels.*

***Theme 3. Create a Group, Process or Funding Mechanism to Support Critical Infrastructure***

Certain critical infrastructure is at risk of insufficient funding and support. Potential examples of critical software and services may include Resource Public Key Infrastructure (RPKI) validators and OpenSSL. Regional Internet registries (RIRs) are non-profit organizations and typically not well funded. To address these risks, achievable goals must be clearly defined.

Supply chain risk management is another area of concern. Governments and organizations worldwide are now awake to the problems of software and hardware supply chain dependencies that may cause catastrophic impact. The National Institute of Standards and Technology (NIST) does not sufficiently decouple things that have systemic impact. Procurement requirements, financial incentives, and frameworks like the Software Bill of Materials (SBOM) can be implemented to encourage resilience.

In all these areas, compliance enforcement should be balanced with voluntary, incentivized adherence to best practices.

*Recommendation: Fund urgent efforts to improve the resilience of RPKI validators and OpenSSL, two examples where a critical vulnerability would cause international problems. Further explore the creation of a sustainable mechanism to support critical infrastructure.*

***Theme 4. Build and Promote "Always Be Rolling" Program (Operational Resilience)***

Regular practice is key to operational resilience. The expression "Always Be Rolling" speaks to a culture of always rolling out new patches into production, in an automated and validated manner. To do such a thing, organizations need processes and methods to quickly recover from problems in deployment. "Always Be Rolling" (ABR) as a core discipline leads to continuous updates and standardized practices to advance resilience.

To achieve this, educational resources, tools, and frameworks must be provided to help organizations adopt and integrate best practices. Industry-led approaches should be encouraged by recruiting organizations such as the Internet Society (ISOC), Global Cyber Alliance (GCA), Forum for Incident Response and Security Teams (FIRST), and others that can develop and promote resilience standards.

*Recommendation: Promote "Always Be Rolling" (ABR) as a core discipline for resilience.*

***Theme 5. Collaborative Exercises and Information Sharing***

Global tabletop exercises should be facilitated as a mechanism for testing and refining resilience strategies. This can start with academic networks and should include the role of Internet measurement to convert anecdotal "war stories" into evidence-based cases. Such an approach will stimulate the development of secure, collaborative platforms for sharing resilience data, emphasizing privacy and non-attributable data aggregation.

To further facilitate resilience data sharing, severity scales for incidents – similar to the Richter scale for earthquakes – should be introduced to standardize impact assessment. ISOC's work on geographic maturity is relevant here. This also links to the maturity models mentioned under Theme 1.

*Recommendation: Facilitate global tabletop exercises, starting with academic networks. Focus on Incident Response communications and protocols.*

***Theme 6. Infrastructure and Sectoral Dependencies***

The Internet does not exist in isolation from other critical infrastructure sectors. Dependencies across sectors including power, third party data centers, water, and others must be addressed. Mutual dependencies must be identified to avoid unexpected or unknown critical infrastructure dependency loops that can lead to spiraling failure events.

Lessons can be learned and best practices gathered from other industries such as water, food, and banking, to reveal similar potential for cascading failures. A focus on distributed, localized solutions is recommended to enhance resilience, especially in regions with unreliable infrastructure.

*Recommendation: Address critical dependencies across sectors like power, third party data centers, water, etc.*

***Theme 7. Education and Talent Development***

A workforce educated in the principles of resilience is essential to achieving and sustaining a more resilient Internet. The knowledge and expertise of the current generation must be captured and passed along to the next generation. Investments in training programs and knowledge-sharing must be made and platforms developed to bridge generational and institutional gaps in technical expertise.

With respect to Internet resilience, these principles must be embedded into educational curricula and Internet workforce development initiatives. Consideration should be given to educational materials,

programs and campaigns for software developers, and in other allied areas. In addition to training for a future Internet workforce, there is also a need for education aimed at government officials and the general population.

*Recommendation: Invest in training programs and knowledge-sharing platforms to bridge generational and institutional gaps in technical expertise. Focus on Knowledge Creation.*

***Theme 8. Governance and International Collaboration***

Realizing the goal of a more resilient Internet will require governance actions and international collaboration. Organizations like the Marconi Society, National Cybersecurity Center of Excellence (NCCoE), Forum for Incident Response and Security Teams (FIRST), and Internet Society (ISOC) can be leveraged to lead resilience initiatives and foster global cooperation. Governments and organizations must advocate for international frameworks to protect critical infrastructure, including subsea cables.

*Recommendation: Leverage organizations to lead resilience initiatives and foster global cooperation.*

***Theme 9. Evolving Resilience Goals***

Internet resilience is not a static thing guaranteed to persist once it is achieved. Rather, it is continuously evolving along with the Internet and the applications that rely on it. Thus, it is necessary to track shifting Internet usage trends (e.g., increased reliance on streaming and e-commerce) and adapt resilience strategies accordingly. This can be approached by focusing resilience efforts on four core scenarios: failure, attack, recovery, and insufficient support.

*Recommendation: Focus resilience efforts on four core scenarios: failure, attack, recovery, and insufficient support.*

**Summary and Conclusions**

The Internet Resiliency Workshop, which brought together 30 leading experts on resilience, revealed a complex landscape of challenges facing the future of Internet infrastructure. While the technical foundations of the Internet remain mostly sound, the workshop identified several critical threats to its continued resilience, stemming from four main areas: vulnerabilities in core protocol infrastructure (e.g., DNS, BGP, WebPKI/Certificate Authorities), increasing system complexity, regulatory pressures, and the challenging economics of prevention versus reaction.

The complexity challenge manifests in multiple, interconnected ways. Participants highlighted the intricate interdependencies between power infrastructure and Internet infrastructure, dubbing this the "circle of dependencies" – a situation where the Internet needs power to function, but power systems increasingly rely on Internet connectivity for operation. Another example cited was BGP and the global routing system's reliance on key elements of the DNS, where each requires the other to work in order to properly function. Modern software development practices have introduced what one participant called a "crisis of complexity," with applications depending on numerous APIs and third-party services, each representing a potential point of failure. The centralization of services through cloud providers and Content Delivery Networks (CDNs) adds another layer of complexity while potentially creating new single points of failure.

The regulatory landscape emerged as perhaps the most pressing challenge. The observation from an opening panelist that "policy issues are what are going to define the Internet in the next 10-20 years, not technical challenges" reflected a broad consensus among participants. The relationship between technical operators and government regulators has become increasingly strained, with one participant noting that in the United States, this relationship has become "antagonistic" rather than collaborative. Regulators are being held accountable by their constituents for reliability and stability of critical infrastructure, often resulting in reflexive responses. The technical community's traditional approach of fixing problems as they arise has become politically untenable as governments demand clear accountability and quick responses to incidents.

The workshop revealed a fundamental tension in how resilience is funded and prioritized. Participants repeatedly emphasized that "resilience is a prevention problem, and prevention does not attract money." While reactive measures to incidents readily attract funding and attention, the crucial work of preventing failures through good operational practices, proper training, and systematic thinking about dependencies often goes underfunded. This challenge is compounded by information asymmetry between different stakeholders – operators, regulators, and users often have different levels of information and understanding about incidents and their causes.

The workshop did not merely identify problems; it proposed several concrete solutions. Nine priority workstreams emerged from the discussions, ranging from establishing best practices frameworks to evolving resilience goals. These workstreams address critical needs including accountability protocols, infrastructure support mechanisms, operational practices, and talent development. Participants emphasized that these initiatives must balance immediate operational needs with long-term strategic goals.

The workshop identified several target audiences for its recommendations. Network and security operators and engineers form the primary technical audience, while CIOs, CFOs, and CISOs represent crucial executive stakeholders who control resource allocation. Boards, regulators and policymakers constitute an important secondary audience, though participants stressed the need for careful engagement with these groups. The discussion emphasized reaching beyond US and EU stakeholders to achieve truly global impact.

Significant attention focused on the role of the Marconi Society in advancing these initiatives. Rather than implementing technical solutions directly, participants suggested the Society should leverage its neutral platform and communication channels to raise awareness and facilitate industry (and relevant stakeholder group) discussions. *This could include producing a comprehensive paper with concrete examples and evidence to educate stakeholders about critical infrastructure challenges*. Discussion also ensued about two follow-on meetings, one convened at an academic institution in Spring 2025 and the other on the occasion of the annual Marconi Society Awards Gala in Fall 2025, that would include the current attendees and other relevant experts.

The software supply chain emerged as a particular concern, with participants noting widespread dependence on poorly understood open-source libraries. This led to recommendations for developing systematic curricula for Internet-scale infrastructure operations, moving beyond the current reliance on anecdotal "war stories" for training.

The path forward requires connecting resilience to business metrics that executives understand, such as Service-Level Agreements (SLAs) and customer experience. However, participants noted the challenge of justifying investment in infrastructure components that appear low value until they fail. The workshop emphasized partnering with technical organizations, academic institutions, civil society organizations, and Internet governance bodies to amplify its message and reach key stakeholders.

To get the resilient Internet we want, four important things must happen: 1) improved dialogue between technical experts and policymakers; 2) better incident response frameworks; 3) systematic approaches to identifying and managing complex interdependencies; and 4) learning from best

practices in other industries (e.g., power, telecom) to get templates and established mechanisms that could be adopted for the Internet. Research should be conducted to evaluate best practices in other sectors to the Internet sector, including inviting relevant experts in those fields to contribute to the effort.

Perhaps most importantly, the workshop recognized that Internet resilience is part of a complex interdependent system, and that we need to identify these dependencies and build on this data to get the resilient Internet we want. The path forward involves partnering with technical organizations, academic institutions, civil society organizations, and Internet governance bodies to amplify the message and reach key stakeholders, while addressing the persistent challenge of funding preventive measures over reactive responses. Building improved dialogue between governments and industry will be essential to the path forward.

# Workshop Participants

**Fiona Alexander,** Distinguished Fellow, Internet Governance Lab, American University

**Hari Balakrishnan**, Professor, MIT EECS

**Robert Blumofe**, EVP & CTO, Akamai Technologies

**Maarten Botterman**, Director, BoD, GNKS Consult/ICANN

**Vint Cerf**, Chairman Emeritus, The Marconi Society

**Girish Chandran**, Corporate CTO, Viasat

**Leo Cloutier,** Managing Director, Zettacycle, LLC

**Andrew Coward**, GM, Software Defined Networking, IBM

**Jim Cowie**, Founder, Internet History Initiative

**Steve Crocker**, President, Edgemoor Research Institute

**David B. Cross,** Chief Information Security Officer

**Brian Cute,** COO and Capacity & Resilience Program Director, Global Cyber Alliance

**Taher Elgamal**, General Partner, Evolution Equity Partners

**Guy Gryspeerdt,** Vice President, Global Head of Operational Resilience, Honeywell

**John Klensin**, Principal, John C Klensin & Associates

**Olaf Kolkman**, Principal - Internet Technology, Policy, and Advocacy, Internet Society

**Warren Kumari**, Senior Network Security Engineer, Google

**Matt Larson**, Vice President, Research, and Managing Director, ICANN

**Tony Li**, VP & Juniper Fellow, Juniper Networks

**Kyle McEneaney**, Head of Strategic Investments, Astera Institute

**Danny McPherson**, EVP Technology & Chief Security Officer, Verisign

**Ram Mohan**, Chief Strategy Officer, Identity Digital

**Mark Nottingham**, Standards Lead, Cloudflare

**Alec Peterson**, Vice President, AWS Resilience, Amazon Web Services

**Anand Raghavan**, VP of Engineering, AI, Cisco

**Dennis Roberson**, President & CEO, Roberson & Associates

**Paul Vixie**, Deputy CISO, Amazon Web Services

**Dan York**, Senior Advisor, Internet Society

**Ellen Zegura**, Division Director, CISE/CNS, National Science Foundation

# Scribes

**Donald Hale**, Vice President of Philanthropy, Marconi Society

**David R. Huberman**, Director of Technical Engagement for North America & Global Standards Development Organizations

**Hana Qureshi**, Product Marketing Manager, Microsoft

**Vikram Thanigaivelan**, Product Manager, Microsoft

# Contacts

**John R. Janowiak**
President and CEO
Marconi Society
john@marconisociety.org
1-312-404-3337

**Ayesha Hassan**
Executive Relations Officer
Marconi Society
ahassan@marconisociety.org
33 6 12 26 05 18

**Barry J. Sullivan, Ph.D.**
Director, Program Development
Marconi Society
bsullivan@marconisociety.org
312-286-1382

**Kim Simpao**
Director, Corporate Development and Sponsorship
Marconi Society
ksimpao@marconisociety.org
773-315-7779

**Donald Hale**
Vice President of Philanthropy
Marconi Society
dhale@marconisociety.org
407-406-0427

**Yeimidy Lagunas**
Director, Communications and Membership
Marconi Society
ylagunas@marconisociety.org
224-399-7333