MANRS: Eight Years of Successes and Challenges

And how you can help for the next eight

Andrei Robachevsky

robachevsky@isoc.org

MANRS is an industry initiative aimed at improving the security and reliability of the global Internet routing system.

MANRS is based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm for network operations

Why is routing security so hard?

- Each network can contribute to routing security
  - And be the cause of an incident
- Most of them would like to have a more secure routing system
  - Routing incidents are hard to debug and fix
- Most of them have little incentive
  - One’s network security is in the hands of others

Solving the collective action problem

Regulation doesn’t really help

- Global span and dependencies

Making good practices a norm

- Widely accepted
- Not exactly a least common denominator, but not too high either
- Visible and Measurable

An approach: Mutually Agreed Norms for Routing Security (MANRS)

- Defines the baseline security in the form of Actions
- Builds a visible community of operators implementing this baseline

MANRS Programs

Network Operators (2014)

Internet Exchange Points (2018)

Content Delivery Networks (CDNs) and Cloud Providers (2020)

Network Equipment Vendors (2021)

Filtering

Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-Spoofing

Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure

Coordination

Maintain globally accessible up-to-date contact information

Global Validation

Publish your data, so others can validate routing information on a global scale

Tools

Provide monitoring and debugging tools to help others

Promotion

Actively encourage MANRS adoption among peers, customers, and partners

MANRS: A Collaborative Effort

MANRS toolkit

Mutually Agreed Norms for Routing Security Tools

https://www.manrs.org/

Overview | Repositories 9 | Projects | Packages | Teams 4 | People 8 | Settings

Popular repositories

contrib — Public

In-development tools contributed by the community

Go ☆ 10 ⑂ 2

labmgr — Public

ISOC Lab Manager

Python ☆ 8

MANRS-validator — Public

A BGP Security Auditing Tool that runs locally and checks configuration the router config against the best practices as defined by MANRS

RobotFramework ☆ 5 ⑂ 1

MANRS-IXP-validation-tool — Public

A tool that validates conformance of the IXP RS filtering policy with Action 1 of the MANRS IXP Program

Python ☆ 4 ⑂ 1

MANRS-Implementation-Guide — Public

MANRS Implementation Guide

☆ 4 ⑂ 2

GNS3-Appliances — Public

GNS3 Appliances for the MANRS Lab Manager

⑂ 1

Self-governance: Steering Committee

9-member committee coordinates and develops the MANRS initiative, including:

- Reviewing and improving MANRS Actions and conformance criteria
- Supervising the auditing process for new applicants and handling appeals
- Recommending suspension or termination of organizations fall short of minimum conformance criteria
- Supervising incident handling processes
- Appointing Advisors, Ambassadors, and Fellows

3 seats open in the November 2022 election

Measuring MANRS

MANRS Observatory https://observatory.manrs.org/

Provides a factual state of MANRS readiness and tracks it over time

Measurements are:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – MANRS community decide what gets measured and how

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH September 2019 RIR REGIONS APNIC

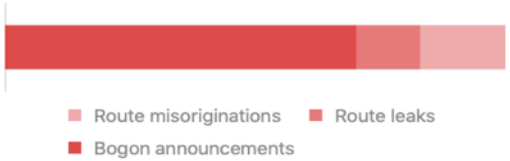
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

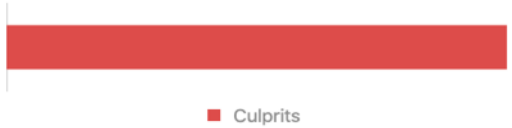
Incidents

Total		
398	Route misoriginations	68
	Route leaks	51
	Bogon announcements	279



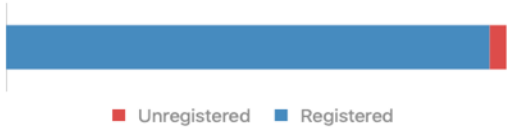
Culprits

Total		
180	Culprits	180



Routing completeness (IRR)

Total		
100%	Unregistered	3%
	Registered	97%



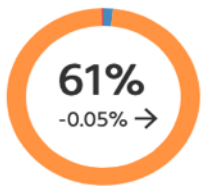
Routing completeness (RPKI)

Total		
100%	Valid	12%
	Unknown	87%
	Invalid	1%

MANRS Readiness

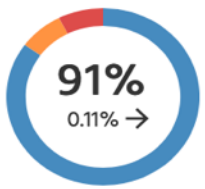
Filtering

Anti-spoofing



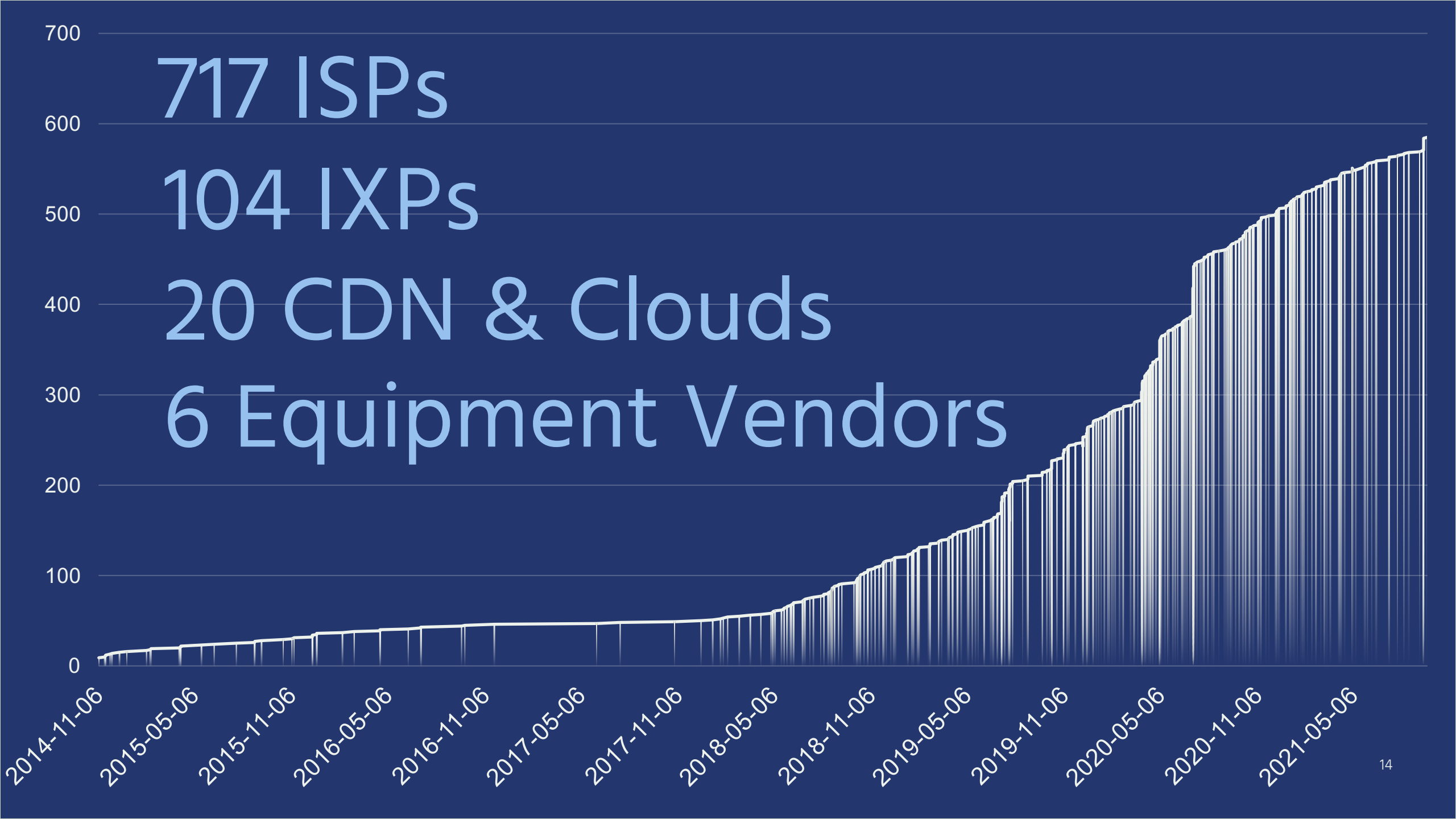
Coordination

Global Validation IRR



Global Validation RPKI

Ready Aspiring Lagging

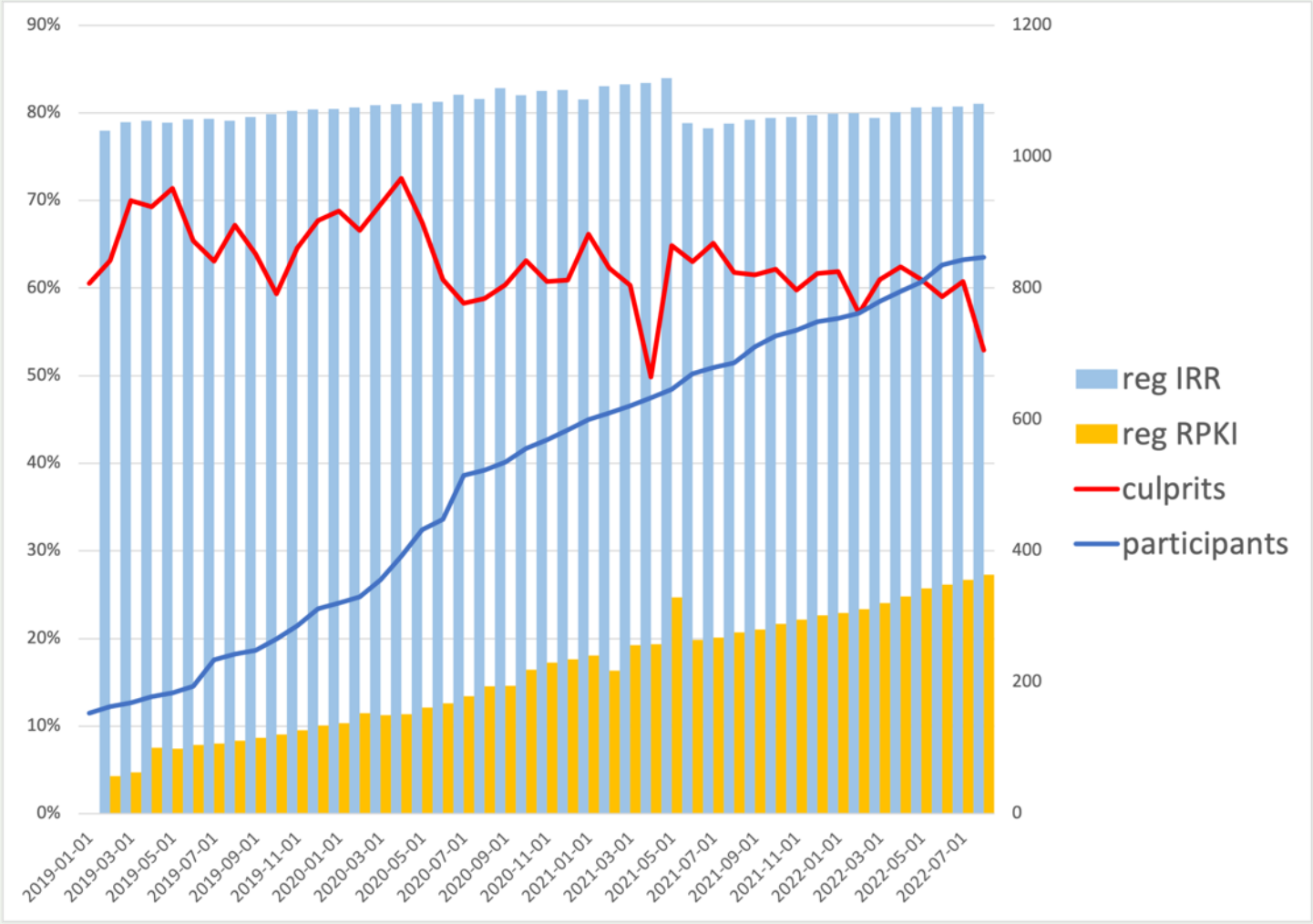

717 ISPs
104 IXPs
20 CDN & Clouds
6 Equipment Vendors
700
600
500
400
300
200
100
0
2014-11-06
2015-05-06
2015-11-06
2016-05-06
2016-11-06
2017-05-06
2017-11-06
2018-05-06
2018-11-06
2019-05-06
2019-11-06
2020-05-06
2020-11-06
2021-05-06

Progress in routing security

81% of all ASNs have their routes registered in the IRR and 27% in RPKI, and these numbers steadily grow.

Number of “culprits” – ASNs implicated in one or more suspicious routing events – declines

Data sources: MANRS Observatory, BGPStream, GRIP.



MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with low risk and cost-effective actions.

MANRS is not a one-stop solution to all of the Internet's routing problems, but it is an important step toward a globally robust and secure routing infrastructure.

Why join MANRS?

- **Improve your security posture and reduce the number and impact of routing incidents**
- Demonstrate that these practices are reality
- **Meet the expectations of the operator community**
- Join a community of security-minded operators working together to make the Internet better
- **Use MANRS as a competitive differentiator**

Increasing the Value Proposition

Challenges and opportunities

- The MANRS approach works
  - Community based
  - Leverages peer pressure
  - Provides reputational value
- Areas for improvement
  - Weak business case – little commitment
  - Little incentive to excel
  - Requiring ongoing conformance is challenging
  - Caveats of the audit framework

MANRS+

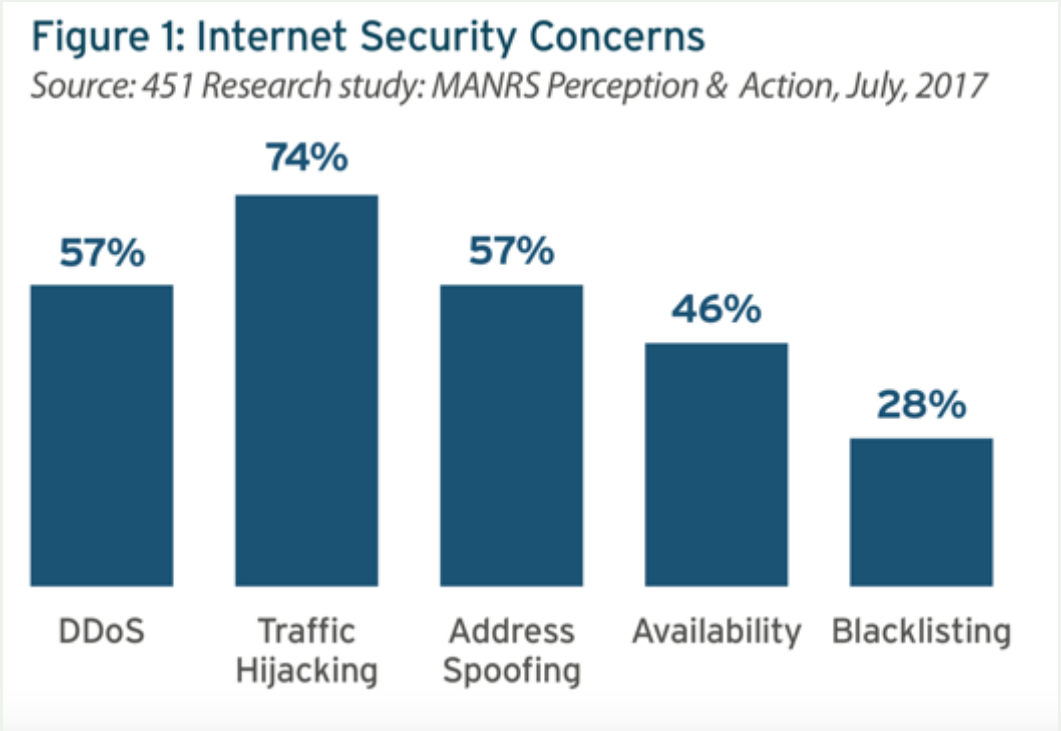
Create a second, elevated tier of MANRS participation for network operators that comply with more stringent requirements and auditing

Focus on customer-provider relationships. Work with industry partners to increase demand for security from their connectivity providers

We need network operators and their potential customers willing to co-develop the requirements of the future quality mark with the goal of eventually incorporating it in procurement policies/recommendations

Scope of the Requirements (Actions)

MANRS+ requirements should be broader than the existing MANRS program baseline to make the certification or quality mark worth industry attention. It should be better aligned with the demands and expectations of business partners.



Conformance Tests

Auditing and conformance must provide a much higher level of confidence than current MANRS metrics.

Current MANRS auditing practices rely on passive measurements; MANRS+ will require active cooperation from the audited organization's networks (e.g. by asking them to run an auditing tool, or to provide additional information about their topology, or to participate in a measurement infrastructure, such as route collectors).

What’s next?

Join MANRS

Help us raise awareness about routing security

Contact us to get involved in elections, MANRS+ development, etc.

Ask your peers and providers about MANRS compliance

LEARN MORE:

https://www.manrs.org

FOLLOW US:

/RoutingMANRS

Thank you.

manrs@isoc.org

manrs.org