

A business case for routing security

MANRS - Mutually Agreed Norms for Routing Security



Andrei Robachevsky
robachevsky@isoc.org

What do a healthy lifestyle and security management have in common?



The Problem

A Routing Security Primer



Routing Basics

~60,000 networks (Autonomous Systems) across the Internet

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path

Routers use unique Autonomous System Numbers (ASNs) to identify themselves to all other routers

The Problem

Border Gateway Protocol (BGP) is based entirely on trust

- No built-in validation of the legitimacy of updates
- The chain of trust spans continents
- Lack of reliable resource data



Which leads to ...

c|net Search CNET [Q] Reviews News Video How To

CNET > Tech Culture > How Pakistan knocked YouTube offline (a) **How Pakistan knocked YouTube offline (and how it happens again)** Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

Routing Leak briefly takes down Google MARCH 12, 2015 COMMENTS (35) VIEWS: 37374 ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY DOUG MADORY

Massive route leak causes Internet slowdown Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

DDoS Attacks Storm Linode Servers Worldwide BY DOUGLAS BONDERUD • JANUARY 5, 2016

UK traffic diverted through Ukraine MARCH 13, 2015 COMMENTS (34) VIEWS: 47297 SECURITY DOUG MADORY

Global Impacts of Recent Leaks OCTOBER 14, 2015 COMMENTS (2)

Event type	Country	ASN
BGP Leak		Origin AS: PO box T511 Leaker AS: Viettel Corp
BGP Leak		Origin AS: Lirex net E Leaker AS: Traffic Br

BGP hijack incident by Syrian telecom Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

On-going BGP Hijack Targets Palestinian ISP VIEWS: 23018 UNCATEGORIZED DOUG MADORY 2016-01-13

The Vast World of Fraudulent Routing JANUARY COMMENTS (17) VIEWS: 36909 SECURITY DOUG MADORY

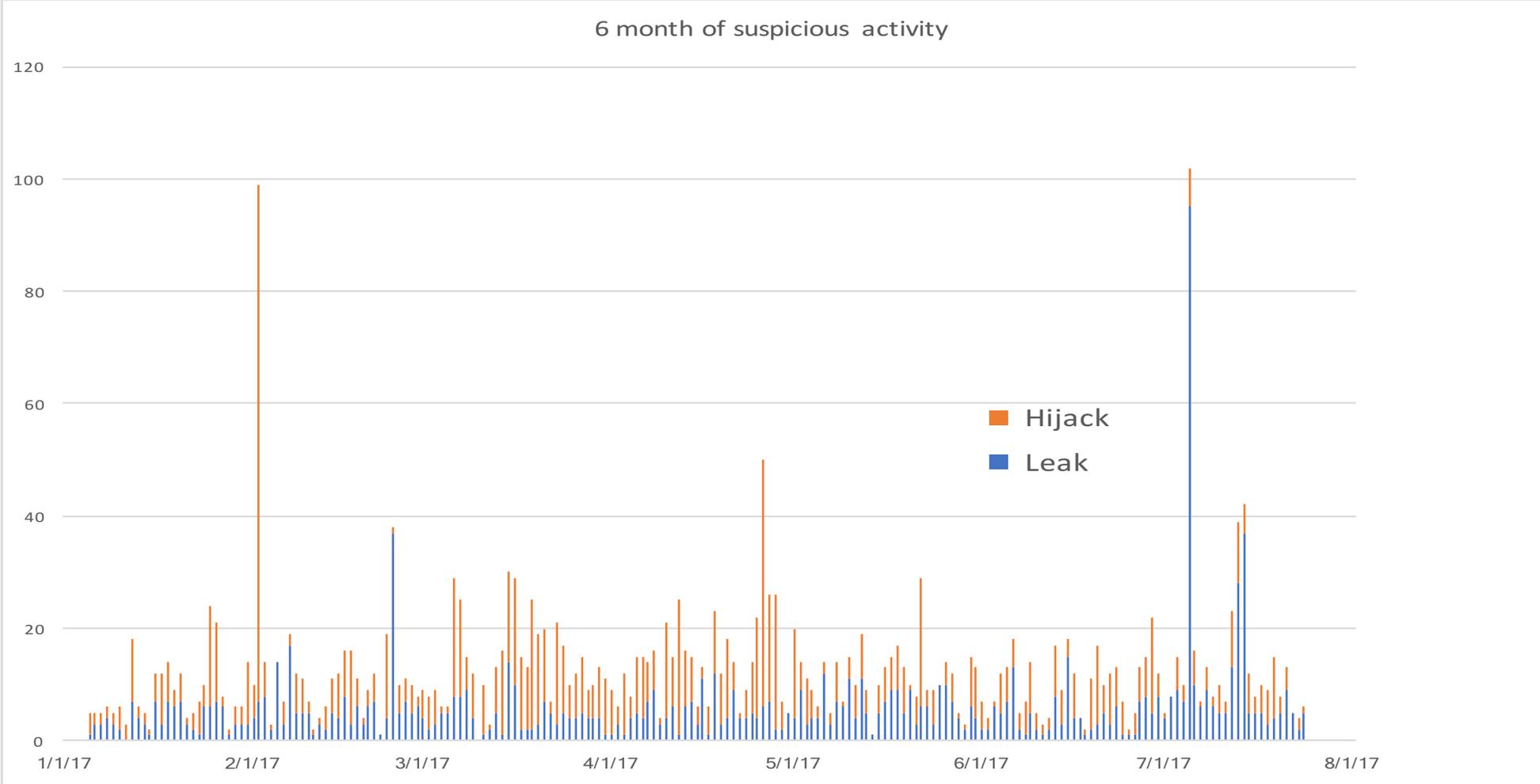
CSO Home > Data Protection > Cyber Attacks/Espionage **Most read:**

DDoS attack on BBC may have been biggest in history

DDoS attack on BBC may have been biggest



No Day Without an Incident



<http://bgpstream.com/>



What's Happening?

IP prefix hijack

- AS announces prefix it doesn't originate and wins the 'best route' selection
 - AS announces more specific prefix than what may be announced by originating AS
 - AS announces it can route traffic through shorter route, whether it exists or not
- Packets end up being forwarded to wrong part of Internet
- Denial-of-Service (DoS), traffic interception, or impersonating network or service

Route leaks

- Violation of valley-free routing (e.g. re-announcing transit provider routes to another provider)
- Usually due to misconfigurations, but can be used for traffic inspection and reconnaissance
- Can be equally devastating

IP address spoofing

- Creation of IP packets with false source address
- The root cause of reflection DDoS attacks

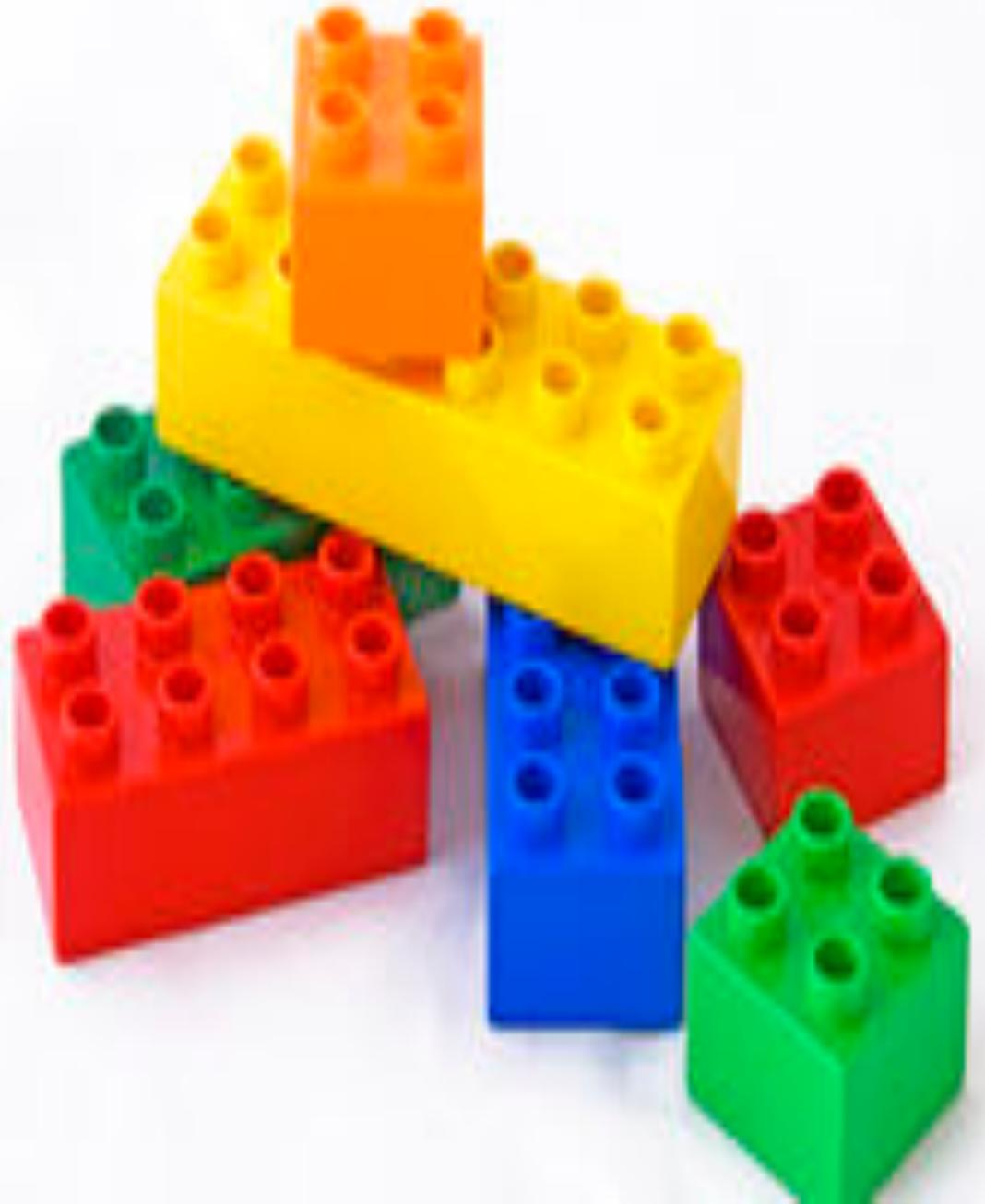
Are There Solutions?

Tools - Yes!

- Prefix and AS-PATH filtering, RPKI, IRR, ...
- BGPSEC under development at the IETF
- Whois, Routing Registries and Peering databases

But...

- Lack of deployment
- Lack of reliable data



A Tragedy of the Commons

From a routing perspective, securing your own network does not necessarily make it more secure. Network security is in someone else's hands.

— The more hands – the better the security

Is there a clear, visible, and industry-supported line between good and bad?

— A cultural norm?



MANRS

A vital part of the security solution



MANRS was founded with the ambitious goal of improving the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for Internet infrastructure.



Mutually Agreed Norms for Routing Security

MANRS defines four concrete actions that network operators should implement

- Technology-neutral baseline for global adoption
- *A minimum* set of requirements

MANRS builds a visible community of security-minded operators

- Promotes culture of collaborative responsibility



MANRS

MANRS Actions

Filtering – Prevent propagation of incorrect routing information

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

Anti-spoofing – Prevent traffic with spoofed source IP addresses

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

Coordination – Facilitate global operational communication and coordination between network operators

- *Maintain globally accessible up-to-date contact information*

Global Validation – Facilitate validation of routing information on a global scale

- *Publish your data, so others can validate*



A Note on MANRS' Limitations

MANRS is an *absolute minimum* an operator should consider, with *low risk* and *cost-effective* Actions

The more operators implement MANRS, the fewer routing incidents we will see, and the smaller will be their scope

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



So what is the business case for MANRS? (and routing security)

Engaged 451 Research to better understand the attitudes and perceptions of Internet service providers and the broader enterprise community around the project

Comprehensive Research Study

Questionnaire-based study

- Assessment against existing 451 Research data
- Common perception elements

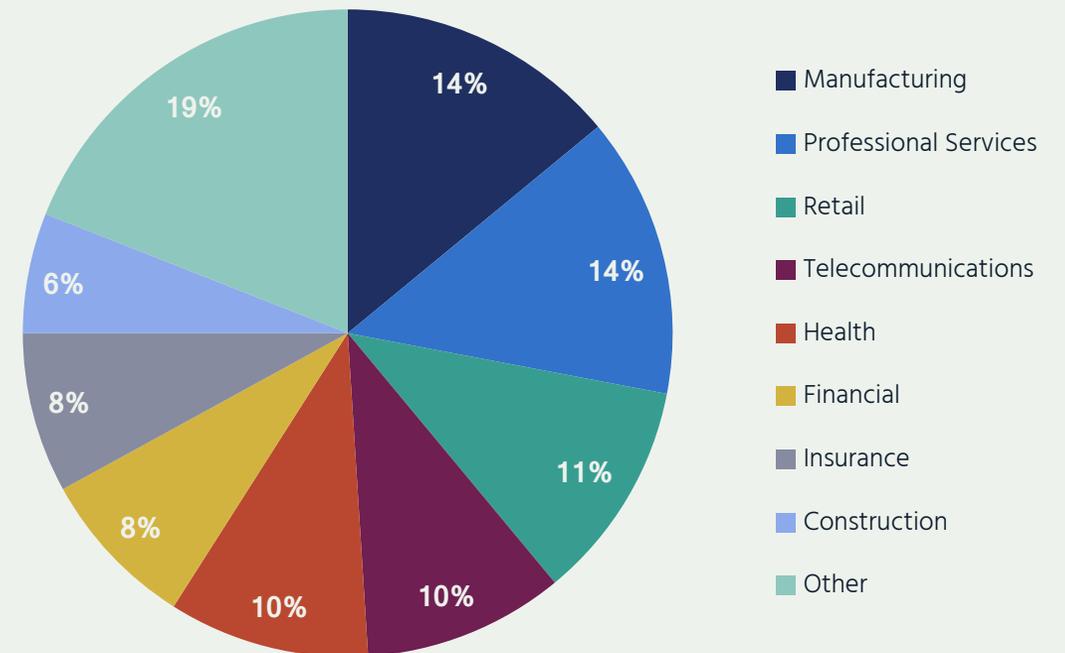
Service providers

- Initial targeting interviews
 - Global demographic
- 25 telephone interviews

Enterprise Internet teams

- 250 web questionnaires
- 1,000 employee minimum
- Primarily North America

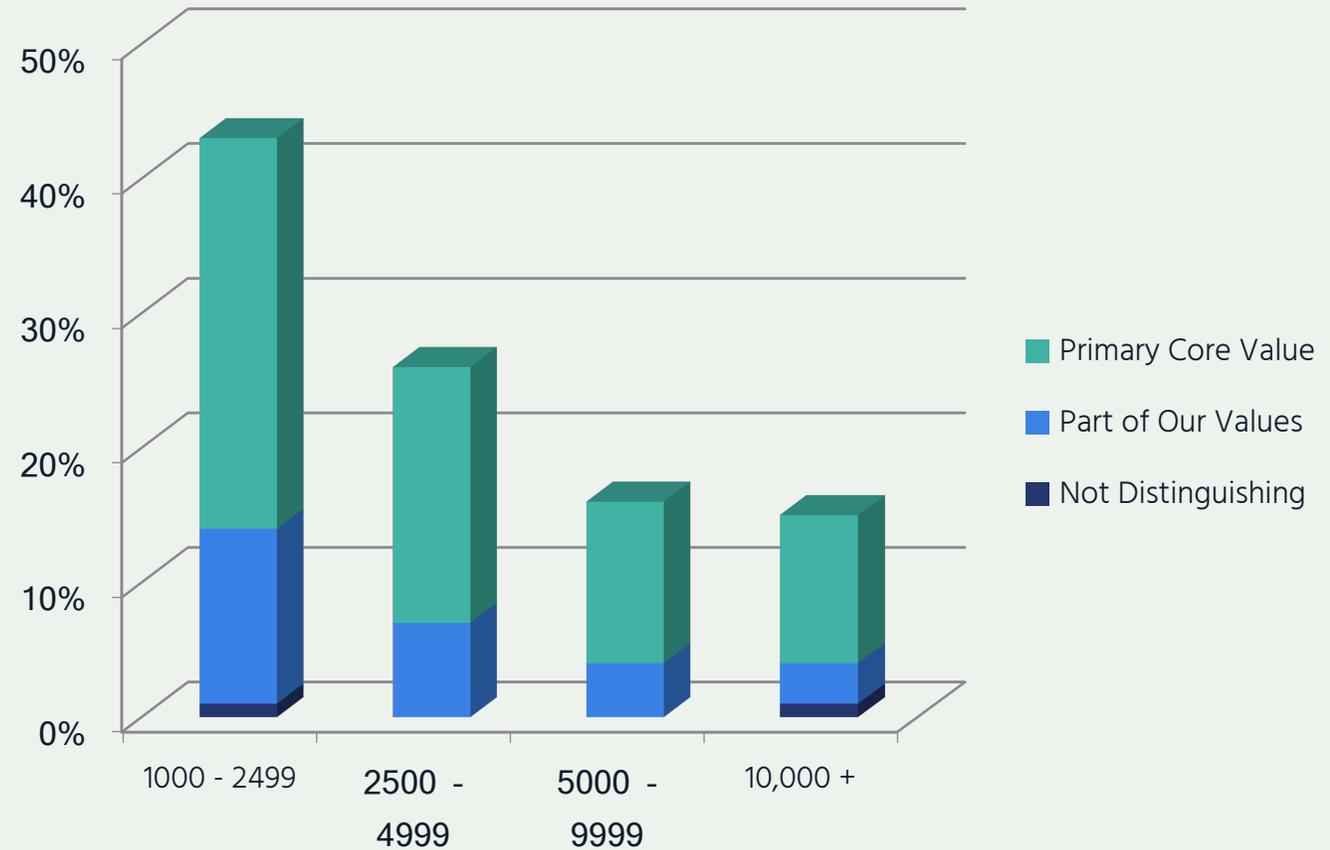
Enterprise Demographics



Enterprises Are Concerned About Security

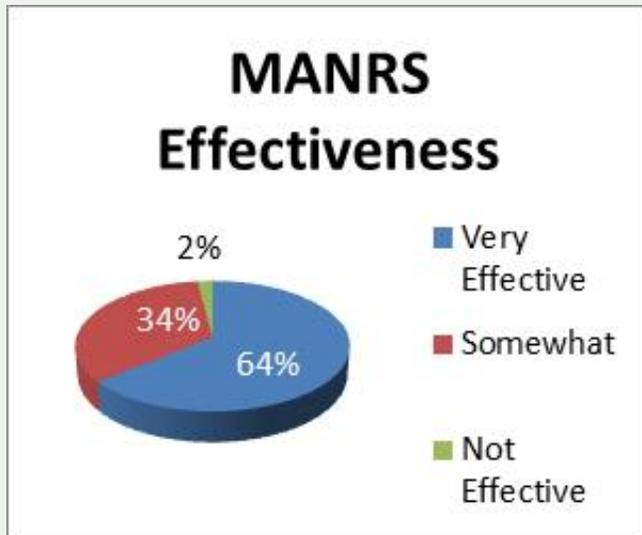
A core value for a majority

Smaller enterprises had an outsized concern about security as part of their primary values

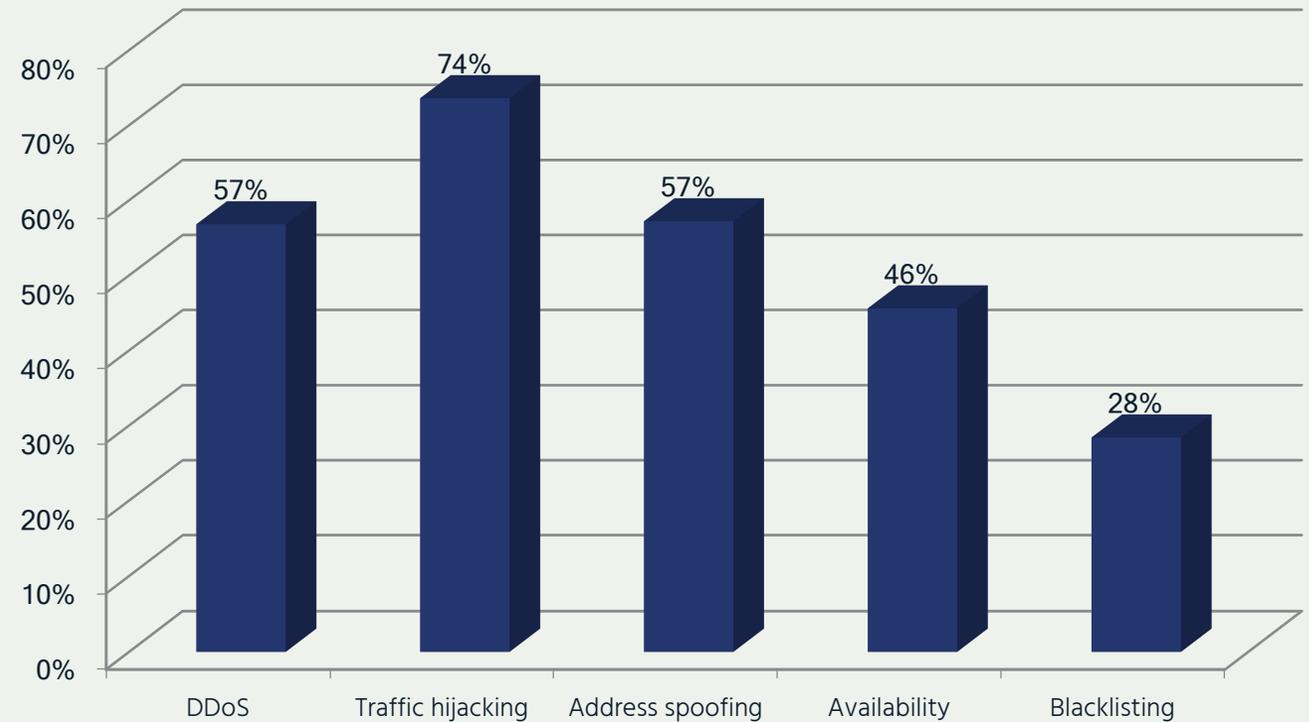


Enterprise Concerns Around Security

- Widely varying concerns across a range of issues
- Security focus is aligned with type of issues MANRS is looking to address



Internet Security Concerns

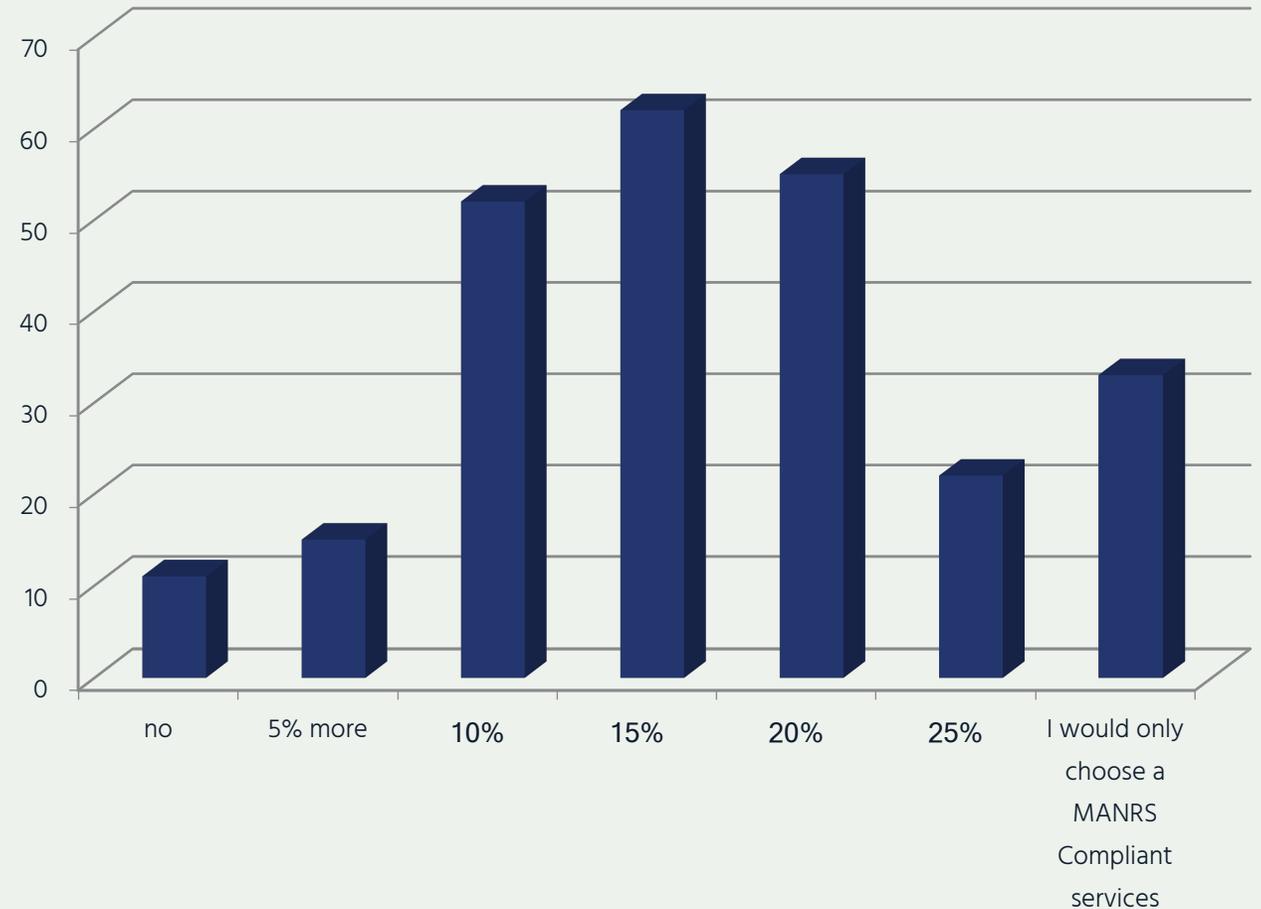


- Confidence that MANRS can help

Enterprises are Willing to Pay for MANRS

Significant value on security posture

- Median premium of 15%
- 13% would only choose MANRS compliant providers

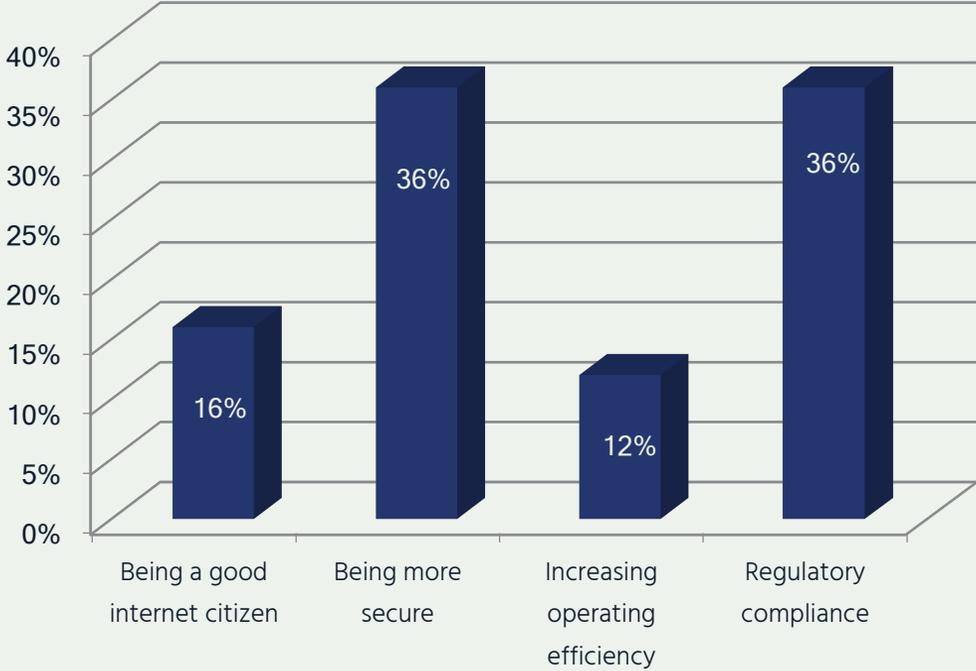


Q: Would you pay a premium for MANRS compliant services?

Service Provider Motivations are Misaligned with Enterprise Perceptions

No one mentioned customer demand as a reason

Reasons for Implementation



Q: Which aspect of MANRS would provide the greatest reason for implementing for your organization?

What We Learned from the Study

Security is Vital to Enterprises

- MANRS knowledge is low, but the desire for security is high
- Enterprises are willing to put MANRS compliance into RFPs and require it of their service providers

MANRS Adds Value for Service Providers

- Service providers can differentiate from their competitors; Identifiable value in a vague market
- Service providers may be able to add additional revenue streams based on information security feeds and other add-on services
- MANRS compliance may reduce customer churn



Why ENTERPRISES Should Require MANRS

- MANRS communicates an enterprise's security investment to its customers
- Larger enterprises with peering arrangements that involve BGP can incorporate the MANRS actions into IT operations, which can add maturity and increase operational efficiency
- Enterprises can require MANRS compliance in RFPs, tender, and purchasing processes
- In regulated industries, MANRS can be an additional factor for auditors to consider when assessing the overall security posture of an organization

Why SERVICE PROVIDERS Should Join MANRS

- MANRS is a sign of security proficiency and commitment
- MANRS is one indication that a provider is contributing to solving network problems at a global scale
- MANRS distinction can add competitive value and enhance operational effectiveness
- Enterprises surveyed indicate willingness to pay more for secure services

Can you stand up publicly and say:

- ✓ I care about routing security
- ✓ I am prepared to spend resources on it
- ✓ I am prepared to be held accountable by the community

Join MANRS Today

Commit to Routing Security, Collaborative Action,
and the Good of the Internet



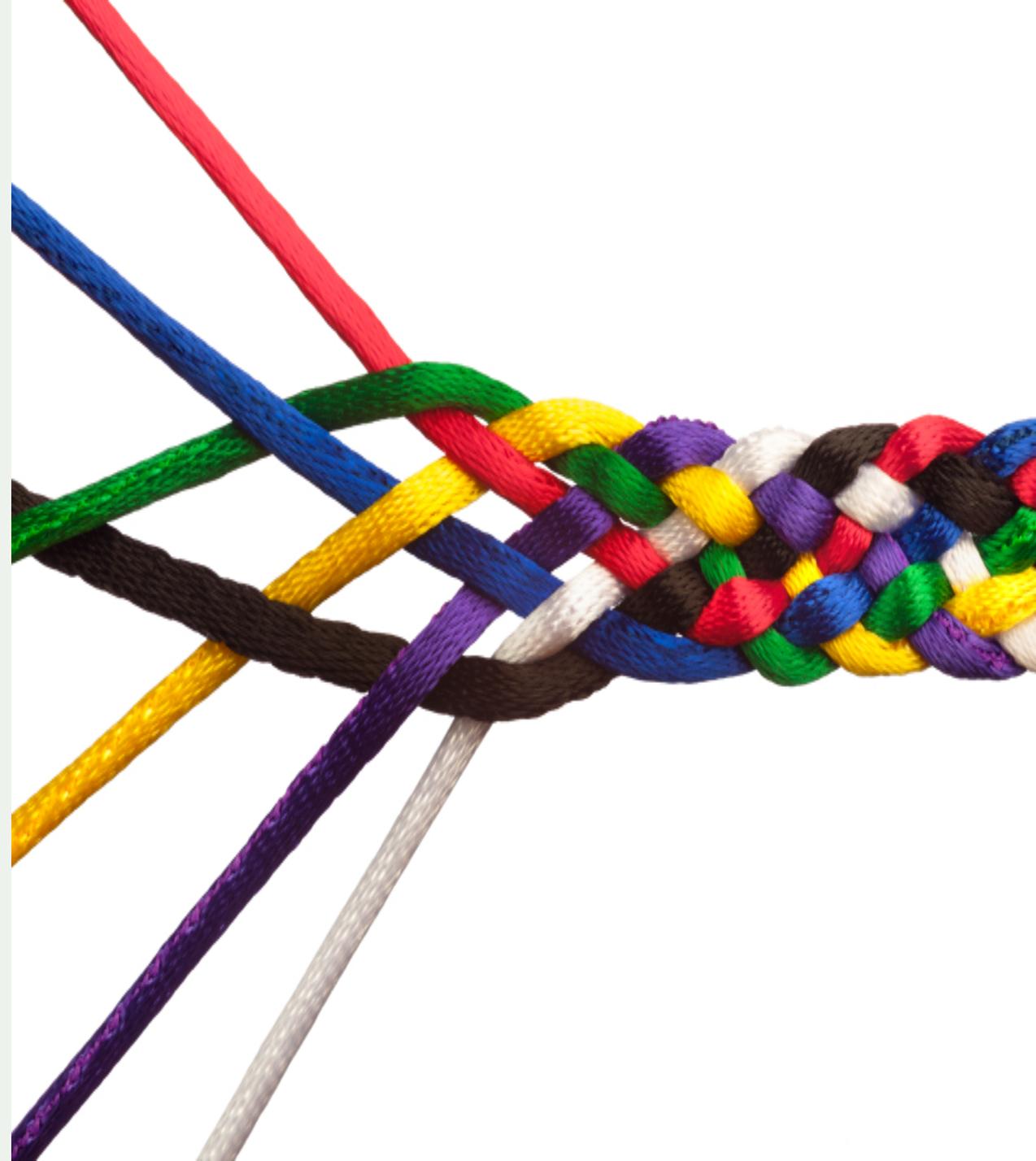
Join Us

Visit www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives



MANRS Implementation Guide

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- <http://www.routingmanifesto.org/bcop/>



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

1. What is a BCOP?
2. Summary
3. MANRS
4. Implementation guidelines for the MANRS Actions
 - 4.1. Coordination - Facilitating global operational communication and coordination between network operators
 - 4.1.1. Maintaining Contact Information in Regional Internet Registries (RIRs): AFRINIC, APNIC, RIPE
 - 4.1.1.1. MNTNER objects
 - 4.1.1.1.1. Creating a new maintainer in the AFRINIC IRR
 - 4.1.1.1.2. Creating a new maintainer in the APNIC IRR
 - 4.1.1.1.3. Creating a new maintainer in the RIPE IRR
 - 4.1.1.2. ROLE objects
 - 4.1.1.3. INETNUM and INET6NUM objects
 - 4.1.1.4. AUT-NUM objects
 - 4.1.2. Maintaining Contact Information in Regional Internet Registries (RIRs): LACNIC
 - 4.1.3. Maintaining Contact Information in Regional Internet Registries (RIRs): ARIN
 - 4.1.3.1. Point of Contact (POC) Object Example:
 - 4.1.3.2. OrgNOCHandle in Network Object Example:
 - 4.1.4. Maintaining Contact Information in Internet Routing Registries
 - 4.1.5. Maintaining Contact Information in PeeringDB
 - 4.1.6. Company Website
 - 4.2. Global Validation - Facilitating validation of routing information on a global scale
 - 4.2.1. Valid Origin documentation
 - 4.2.1.1. Providing information through the IRR system
 - 4.2.1.1.1. Registering expected announcements in the IRR
 - 4.2.1.2. Providing information through the RPKI system
 - 4.2.1.2.1. RIR Hosted Resource Certification service

What's Next: MANRS Training

Routing security is hard. How can we make it more accessible? The “simple” MANRS Implementation Guide is a 50-page document that assumes a certain level of expertise.

Online training modules

- Based on the MANRS Implementation Guide
- Walks a student through the tutorial with a test at the end
- Working with and looking for partners that are interested in integrating it in their curricula

A hands-on lab on implementing MANRS Actions

- Completing the online modules as a first step in MANRS engineering certification
- Looking for partners



What's Next: MANRS IXP Partnership Programme

There is synergy between MANRS and IXPs

- IXPs form a community with a common operational objective
- MANRS is a reference point with a global presence – useful for building a “safe neighborhood”

How can IXPs contribute?

- Technical measures: Route Server with validation, alerting on unwanted traffic, providing debugging and monitoring tools
- Social measures: MANRS ambassador role, general security awareness and communications
- A development team is working on a set of useful actions to be vetted by the community



LEARN MORE:
www.manrs.org



Thank you.

Andrei Robachevsky

robachevsky@isoc.org

Visit us at
www.internetsociety.org
Follow us
[@internetsociety](https://twitter.com/internetsociety)

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120

