September 2017

AusNOG 2017

7 & 8 September 2017, The Langham, Melbourne.

MANRS

Two years of good MANRS - Improving Global Routing Security and Resilience

Aftab Siddiqui

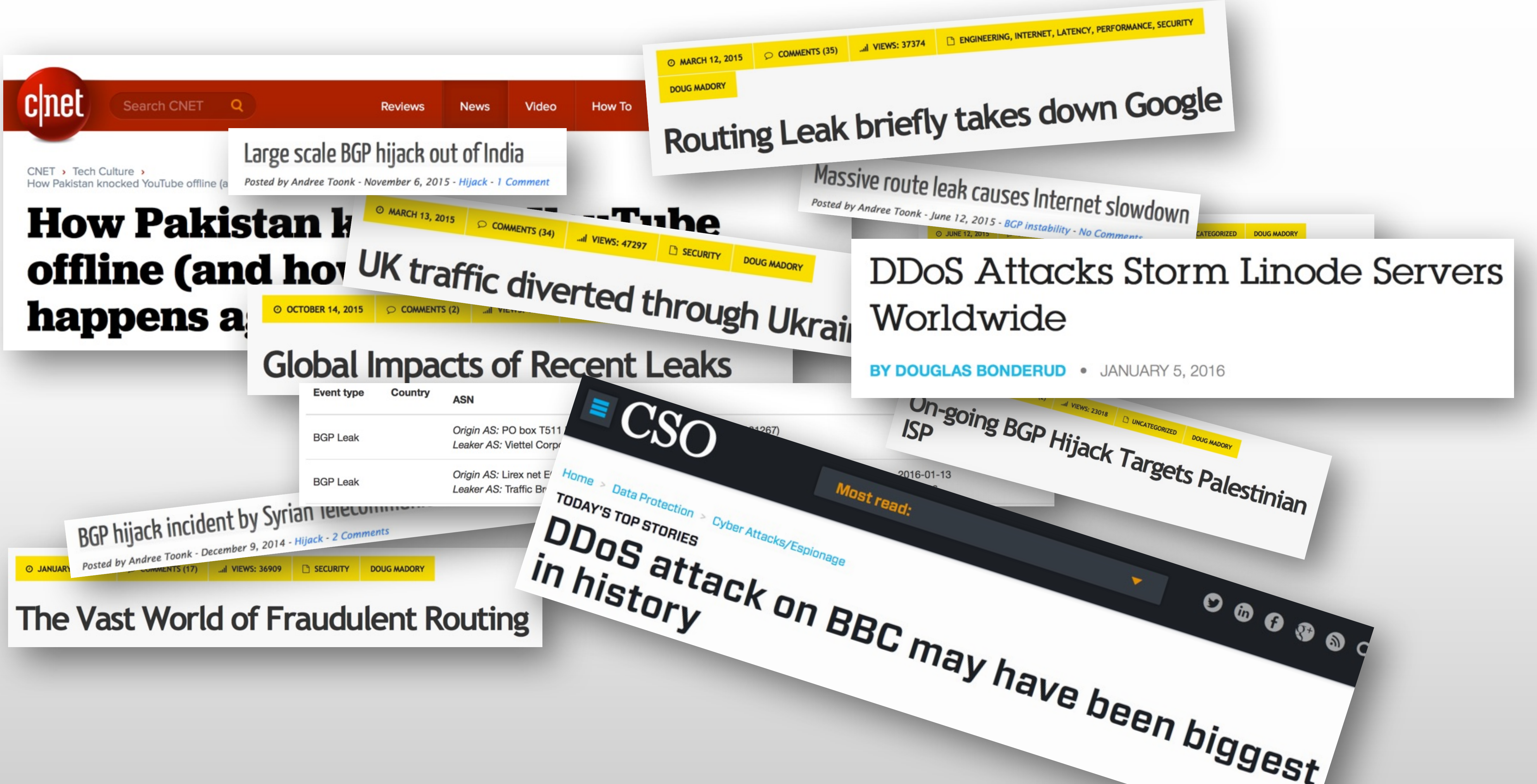
siddiqui@isoc.org

Internet So

MANRS

Internet Routing – what is the problem?

- Internet routing infrastructure is vulnerable
  - Traffic can be hijacked, blackholed or detoured
  - Traffic can be spoofed
  - Fat-fingers and malicious attacks
- BGP is based on trust
  - No built-in validation of the legitimacy of updates



Search CNET

Reviews News Video How To

CNET › Tech Culture ›
How Pakistan knocked YouTube offline (a

How Pakistan k
offline (and ho
happens a

Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

MARCH 12, 2015 · COMMENTS (35) · VIEWS: 37374 · ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY · DOUG MADORY

Routing Leak briefly takes down Google

Massive route leak causes Internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

JUNE 12, 2015 · CATEGORIZED · DOUG MADORY

MARCH 13, 2015 · COMMENTS (34) · VIEWS: 47297 · SECURITY · DOUG MADORY

UK traffic diverted through Ukrai

OCTOBER 14, 2015 · COMMENTS (2)

Global Impacts of Recent Leaks

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

DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016

VIEWS: 23018 · UNCATEGORIZED · DOUG MADORY

On-going BGP Hijack Targets Palestinian ISP

2016-01-13

CSO

Home > Data Protection > Cyber Attacks/Espionage

Most read:

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

BGP hijack incident by Syrian Telecomm

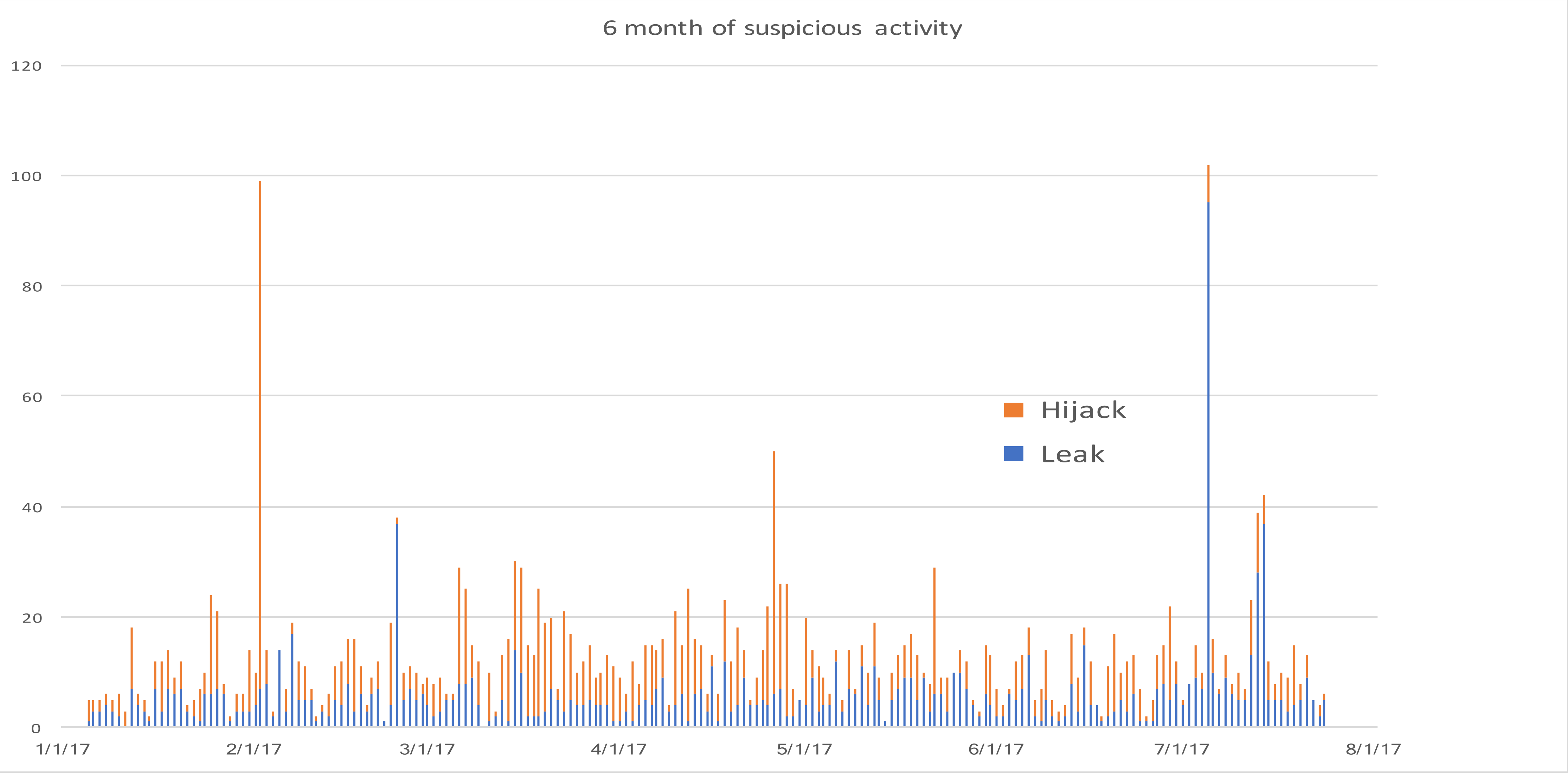
Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

JANUARY · COMMENTS (17) · VIEWS: 36909 · SECURITY · DOUG MADORY

The Vast World of Fraudulent Routing

Not a day without an incident

data source: http://bgpstream.com/

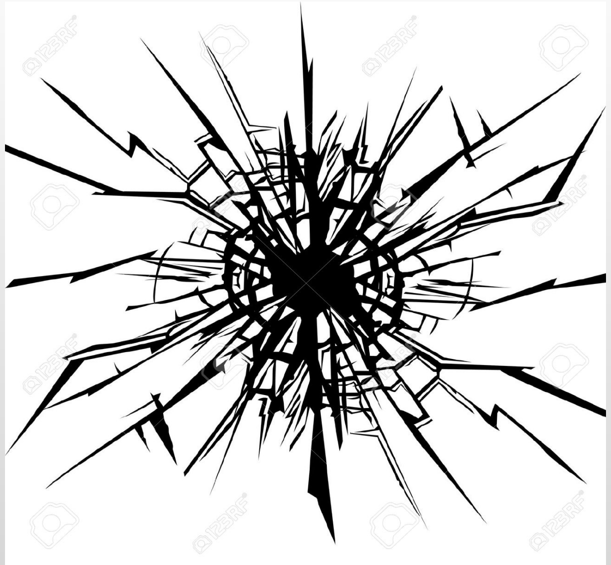


What’s behind these incidents?

- IP prefix hijack
  - AS announces prefix it doesn’t originate
  - AS announces more specific prefix than what may be announced by originating AS
  - Packets end-up being forwarded to a wrong part of Internet
  - Denial-of-Service, traffic interception, or impersonating network or service

- Route leaks
  - Similar to prefix hijacking
  - Usually not malicious and due to misconfigurations
  - But may also aid traffic inspection and reconnaissance

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



Are there solutions?

- Yes!
  - Prefix and AS-PATH filtering, RPKI …
  - BGPSEC under development at the IETF
  - Whois, Routing Registries and Peering databases

- But…
  - Lack of deployment
  - Lack of reliable data

Mutually Agreed Norms for Routing Security (MANRS)

MANRS defines four concrete actions that network operators should implement

- Technology-neutral baseline for global adoption

MANRS builds a visible community of security-minded operators

- Promotes culture of collaborative responsibility

Good MANRS

- **Filtering** – Prevent propagation of incorrect routing information
  - *Own announcements and the customer cone*

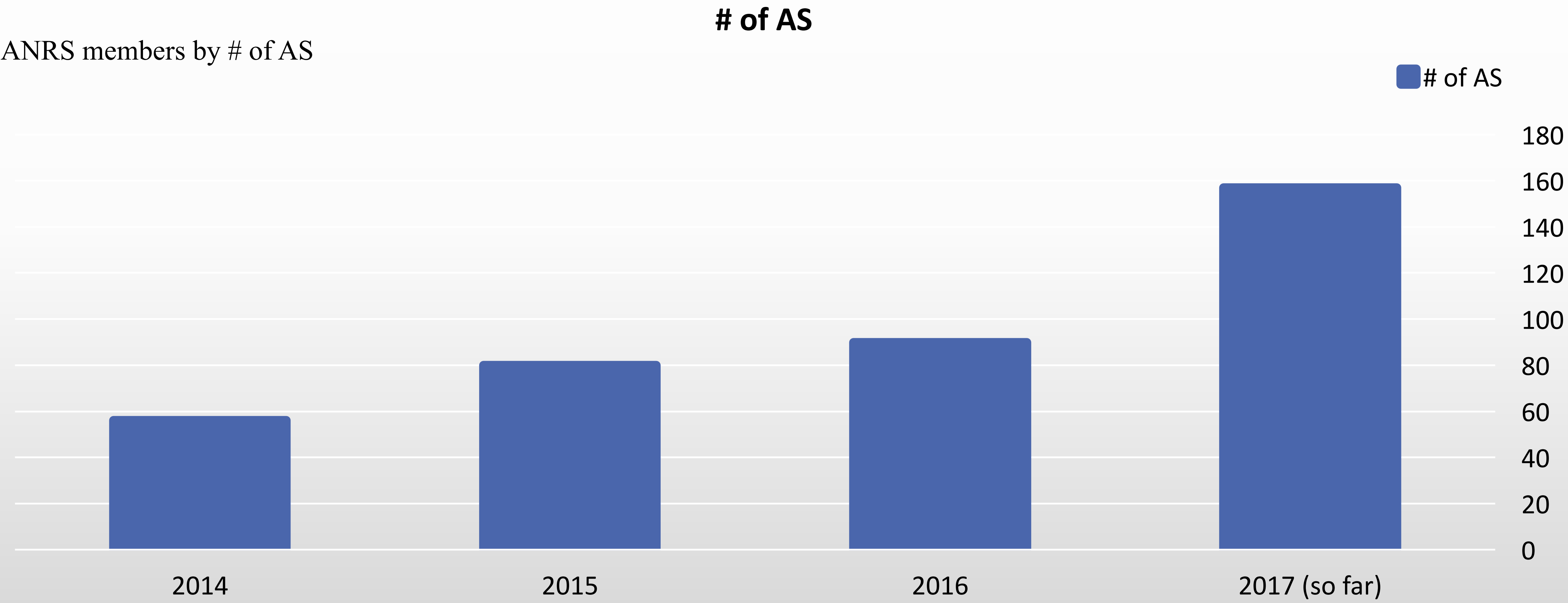
- **Anti-spoofing** – Prevent traffic with spoofed source IP addresses
  - *Single-homed stub customers and own infra*

- **Coordination** – Facilitate global operational communication and coordination between network operators
  - *Up-to-date and responsive public contacts*

- **Global Validation** – Facilitate validation of routing information on a global scale
  - *Publish your data, so others can validate*

Two years of MANRS

MANRS members by # of AS



Increasing gravity by making MANRS a platform for related activities

- Developing better guidance
  - MANRS Best Current Operational Practices (BCOP) document: http://www.routingmanifesto.org/bcop/
- Training/certification programme
  - Based on BCOP document and an online module
- Bringing new types of members on board
  - IXPs

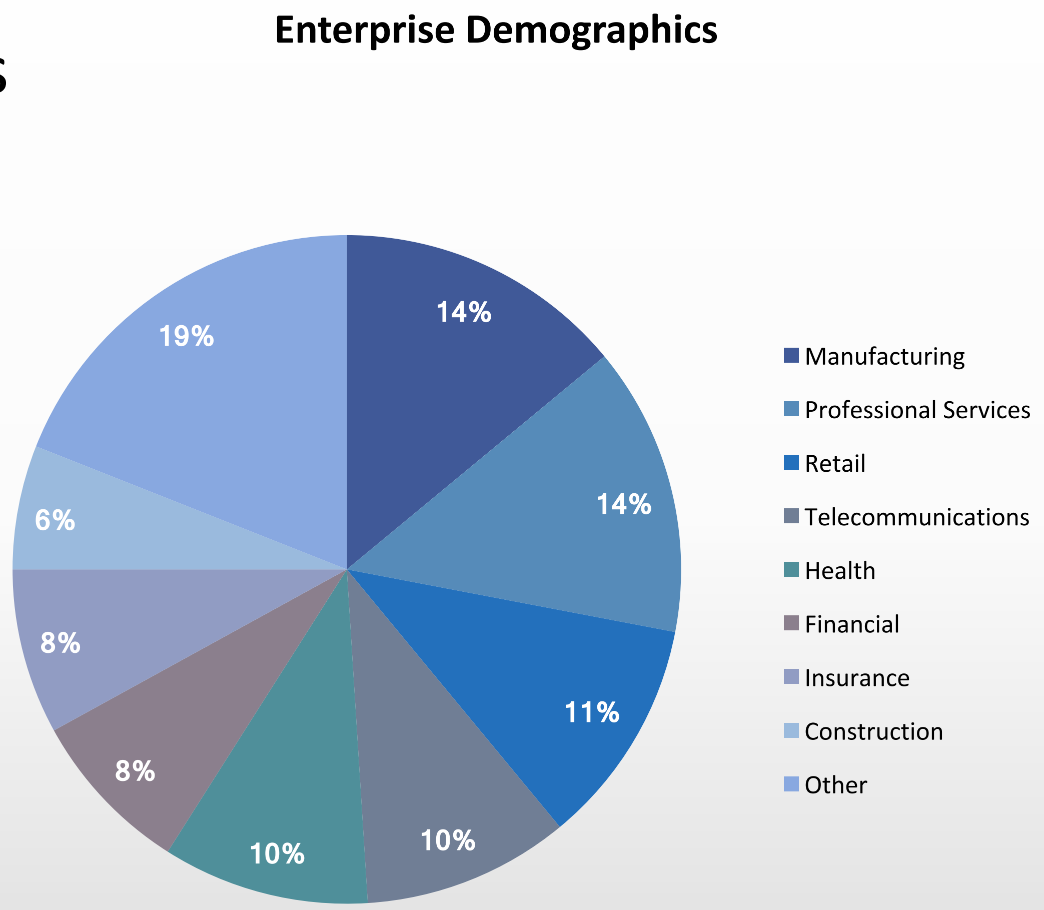
Leveraging market forces and peer pressure

- Developing a better “business case” for MANRS
  - MANRS value proposition for your customers and your own network
- Creating a trusted community
  - A group with a similar attitude towards security

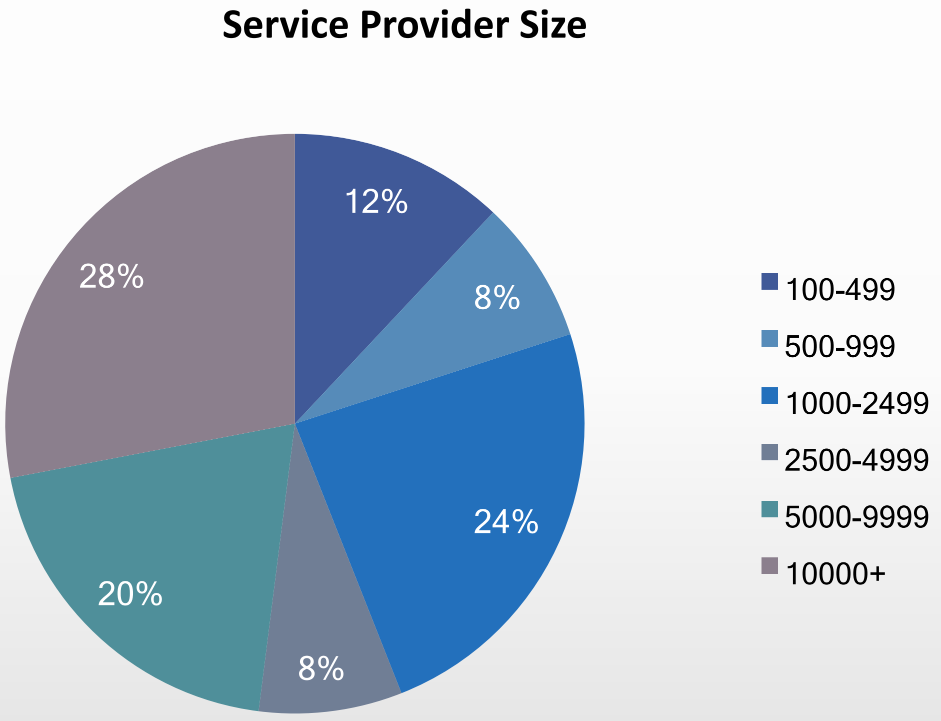
Is there a business case for MANRS?

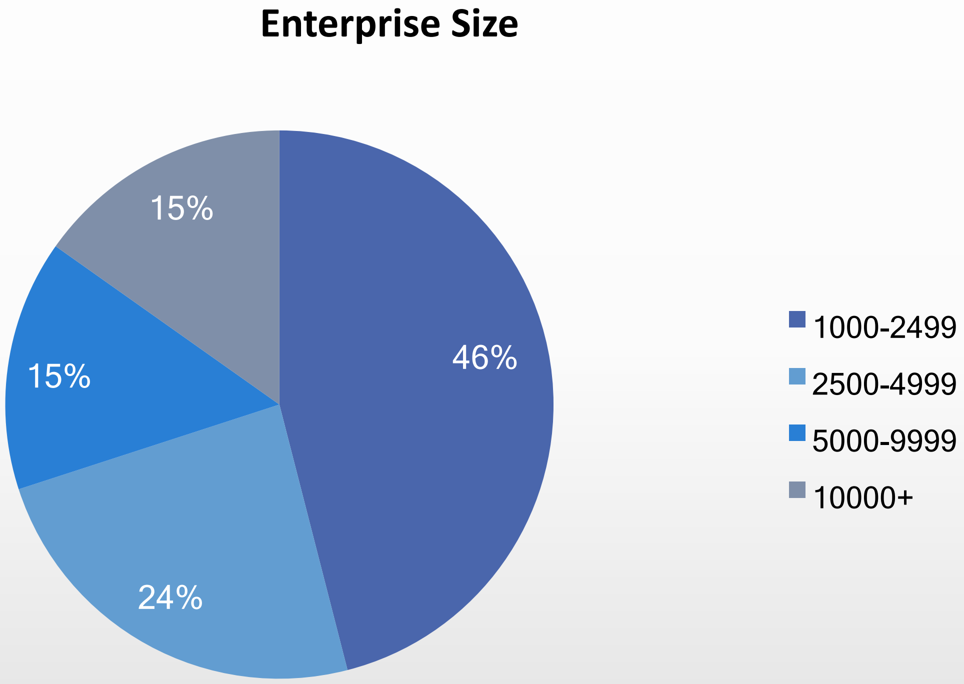
Study Methodology

- Examining perceptions and expectations
  - 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



Demographics

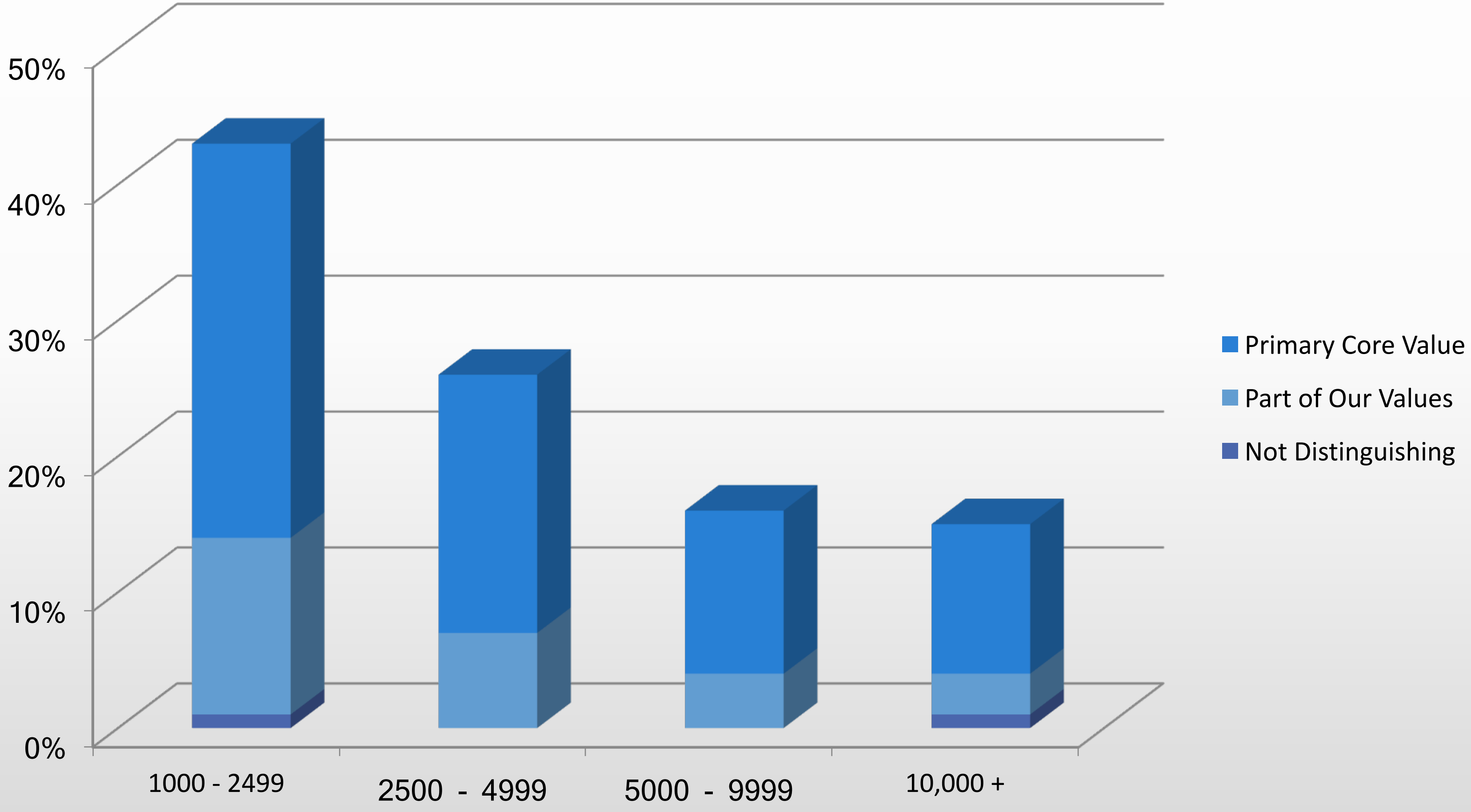




A business case for an enterprise

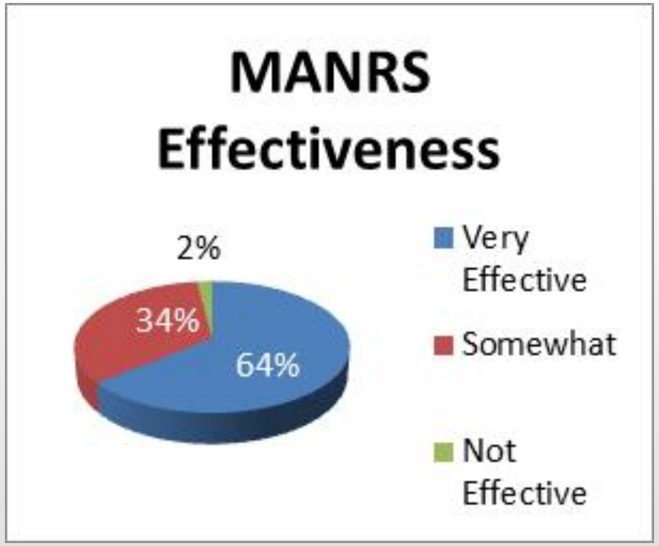
Enterprises Are Concerned About Security

- A core value for a majority

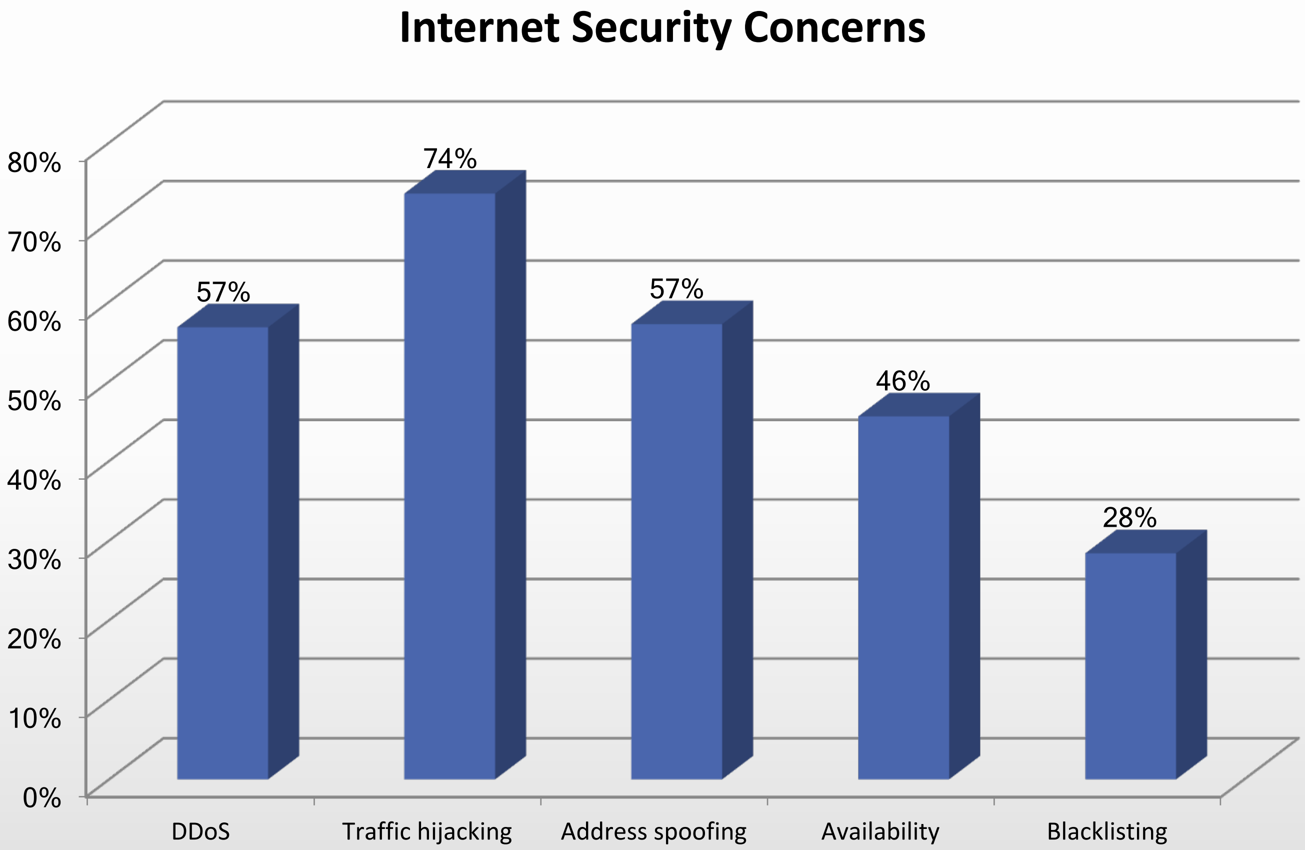


Enterprise Concerns Around Security

- Widely varying concerns across a range of issues

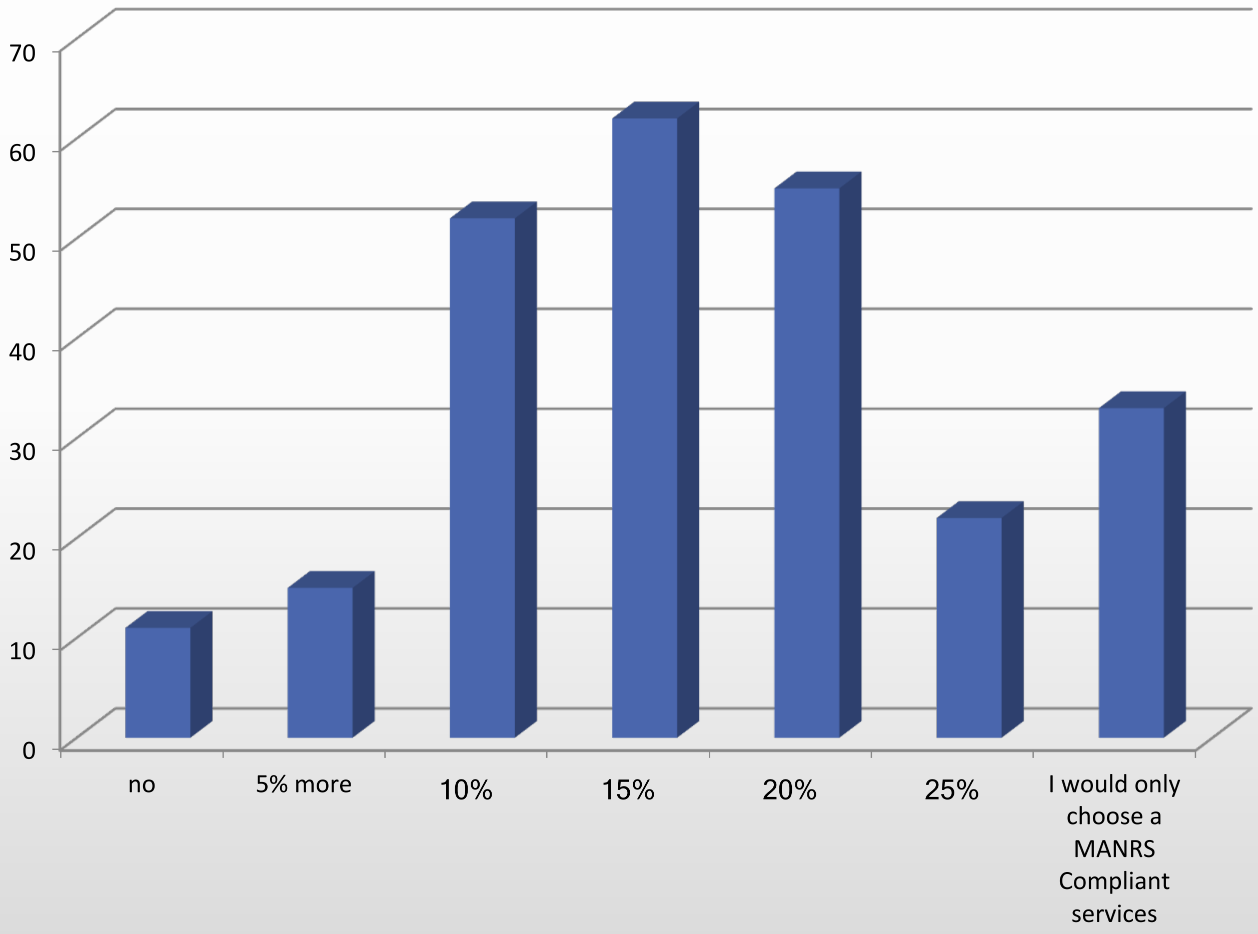


- And confidence that MANRS can help



And Enterprises are Willing to Pay for MANRS

- Significant value on security posture
  - Median premium of 15%
  - 13% would only choose MANRS compliant providers



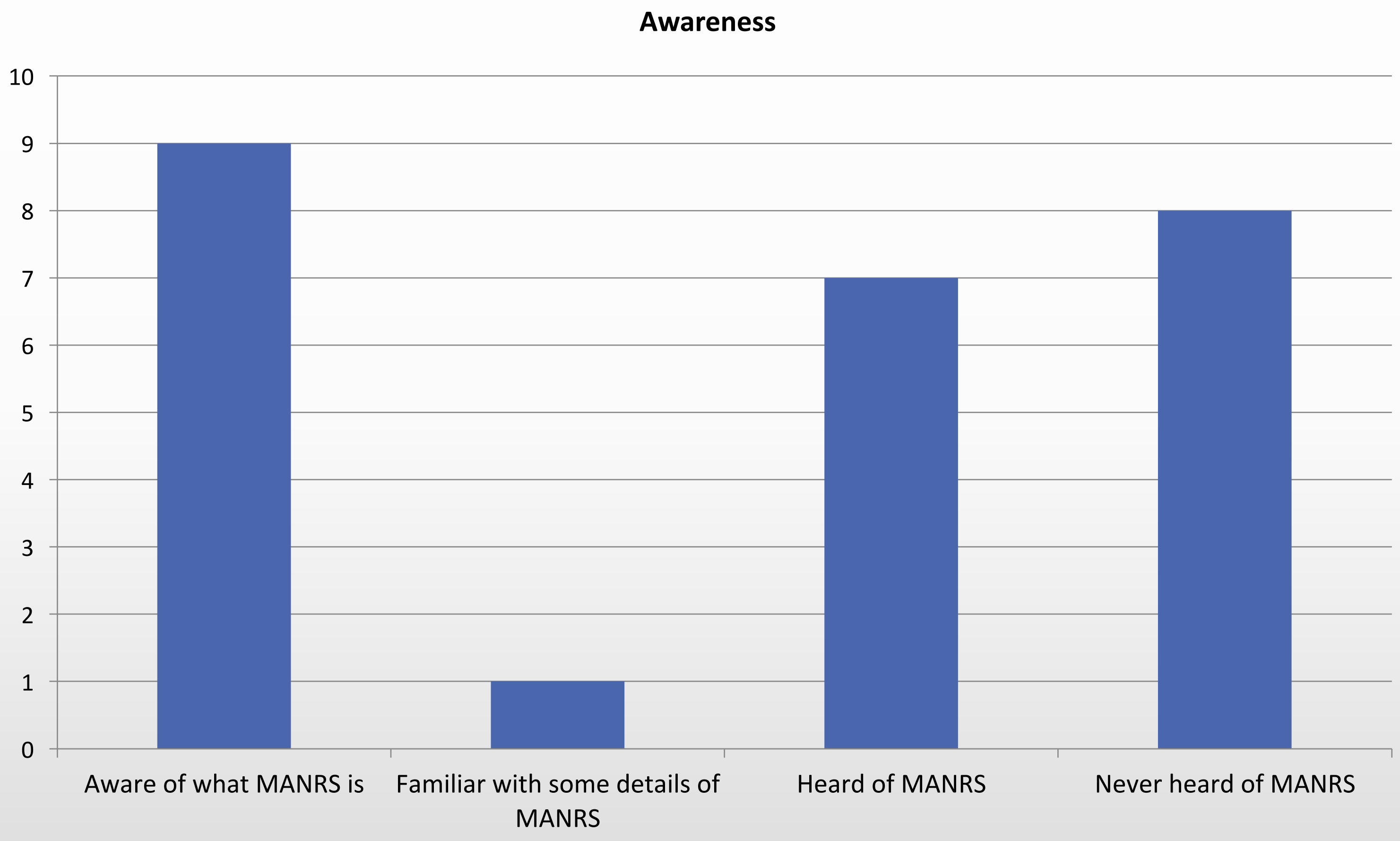
Q: Would you pay a premium for MANRS compliant services?

Enterprise Conclusions

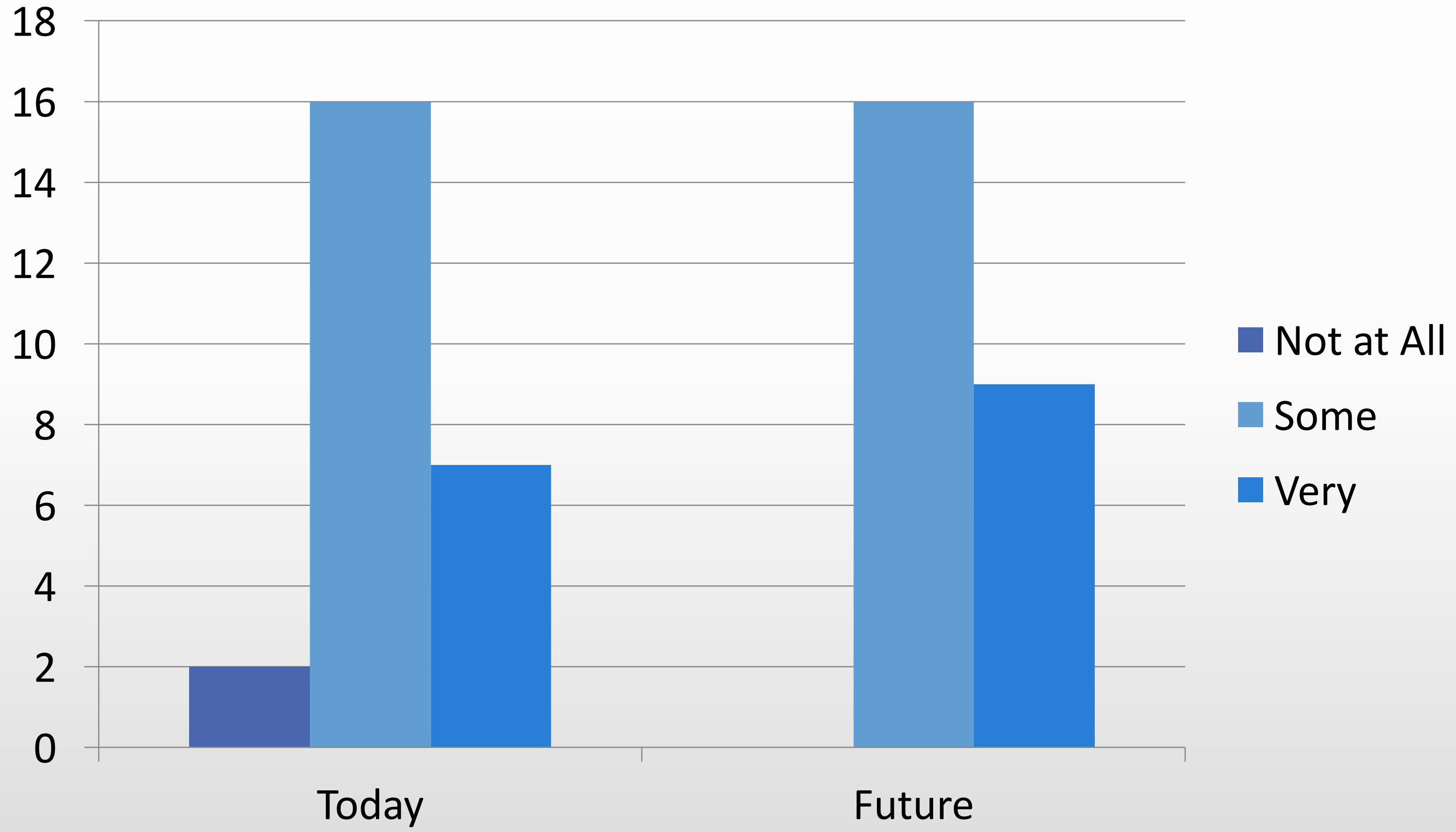
- Great opportunity for service providers
  - While not well known by enterprises (yet), MANRS attributes are highly valued
  - Enterprises care about security and believe MANRS can help
  - Enterprises are willing to put MANRS compliance into RFPs and require it of their service providers

A business case for an ISP

Service Provider Awareness

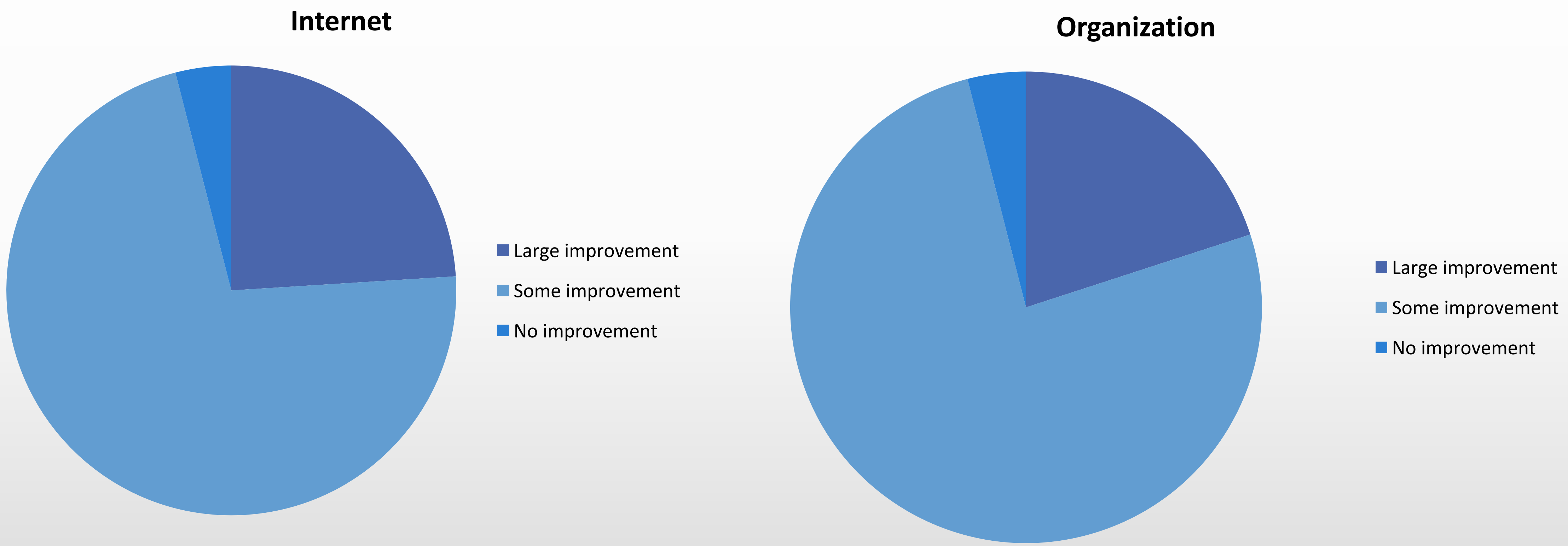


MANRS Effectiveness



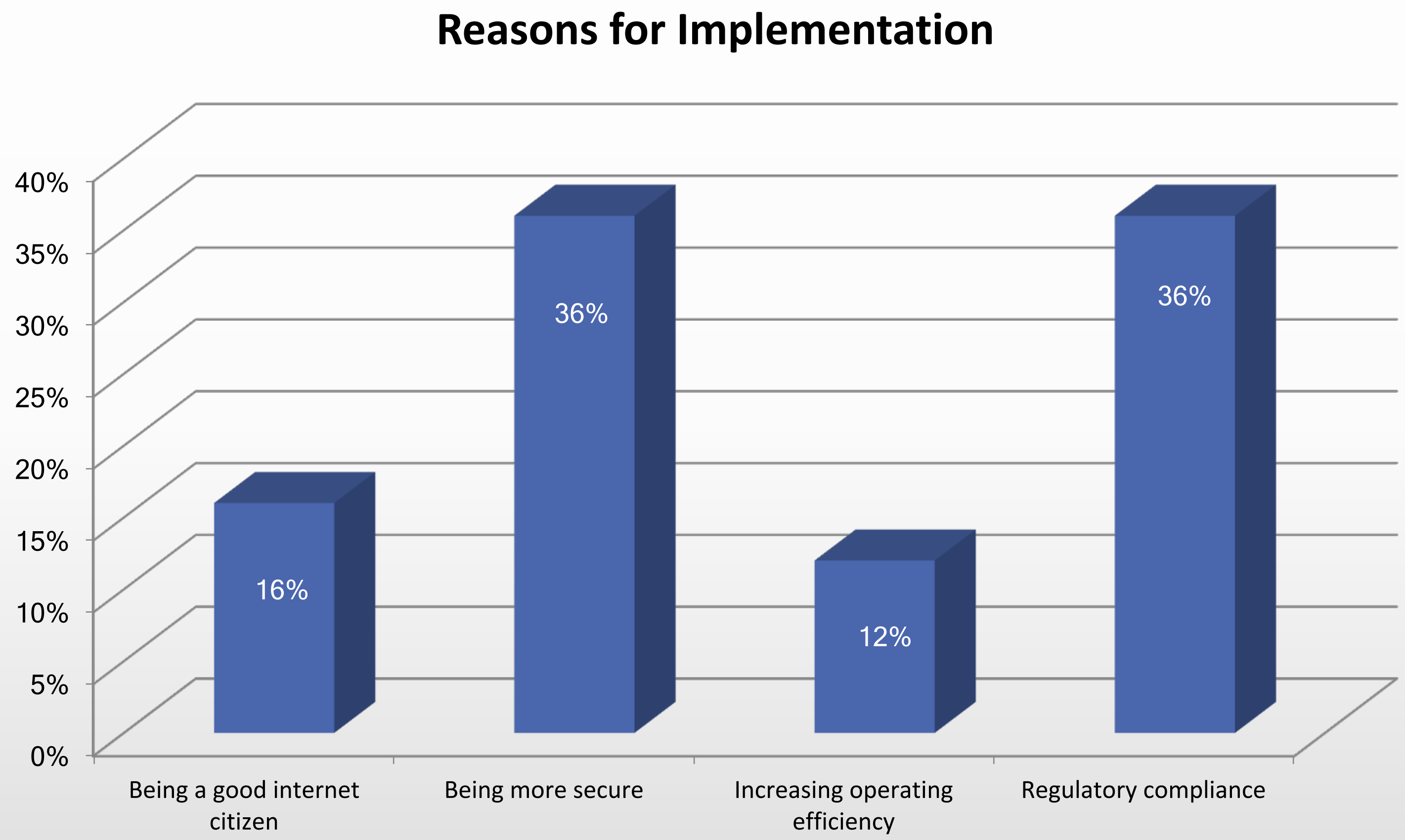
Q: How effective do you think MANRS is/could be in improving Internet security?

MANRS Security Improvements



Q: Do you see MANRS as having a significant effect on improving Internet security/your organization's security?

Service Provider Motivations



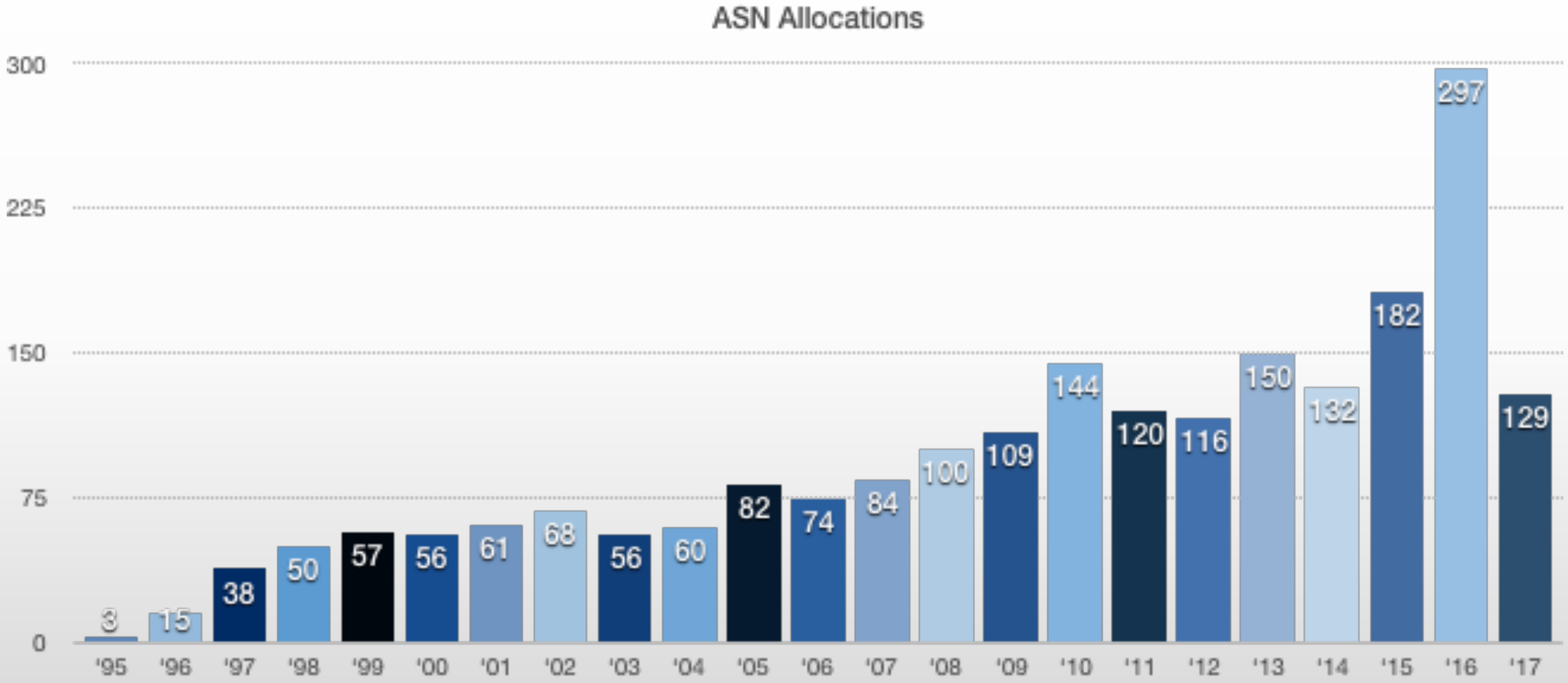
Q: Which aspect of MANRS would provide the greatest reason for implementing for your organization?

Service Provider Conclusions

- Cautious enthusiasm, but market misperceptions
  - Much support for the actions and high expectations for the change MANRS could make on individual organizations and the Internet as a whole, if implemented widely
  - Challenges in decision process
    - Technical teams drive for 64%
    - Technical teams have authority in 4%
  - Limited expectations of enterprise value
    - Implementing MANRS and marketing an increased security posture to enterprises can serve as a business differentiator and translate into increased revenue
    - Possibility for add-on security services to customers based on implementing MANRS actions

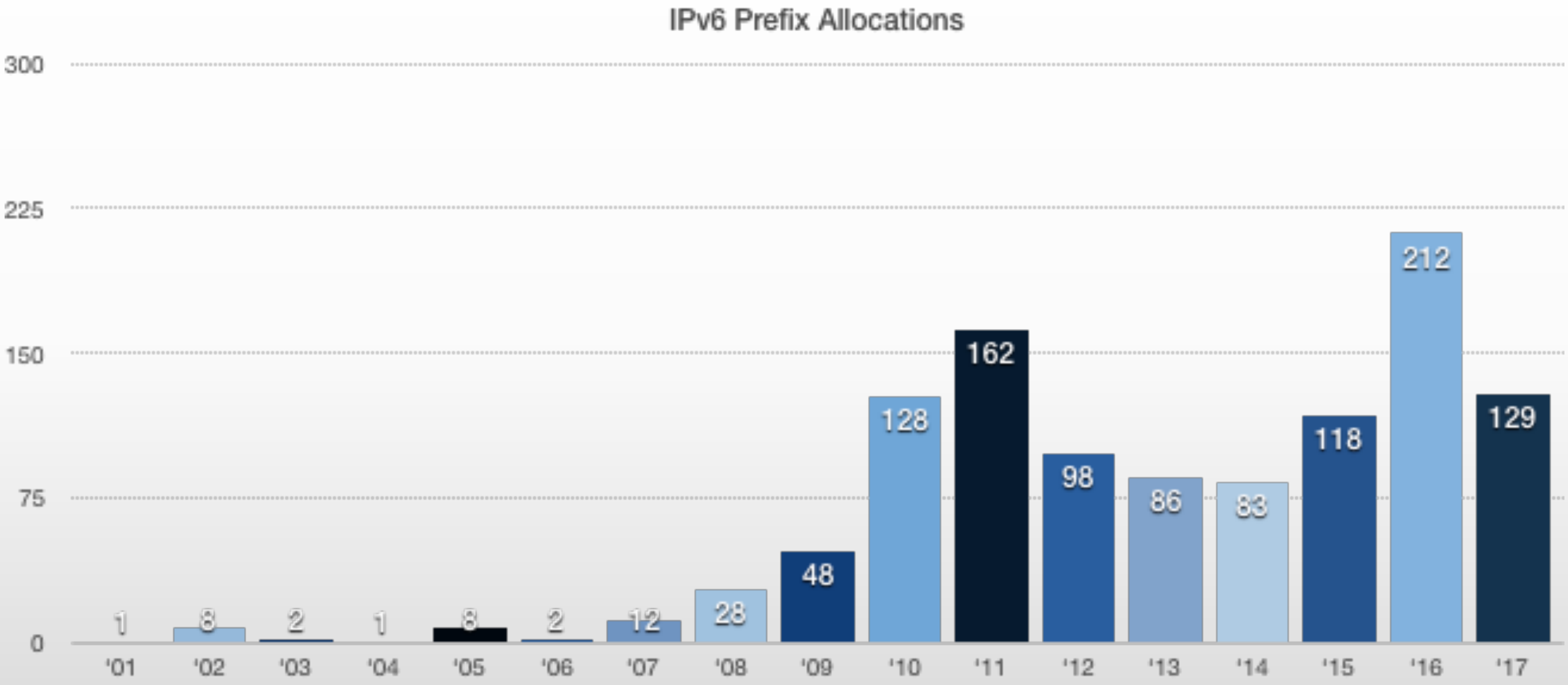
Resource Statistics

No. of ASNs: 2183



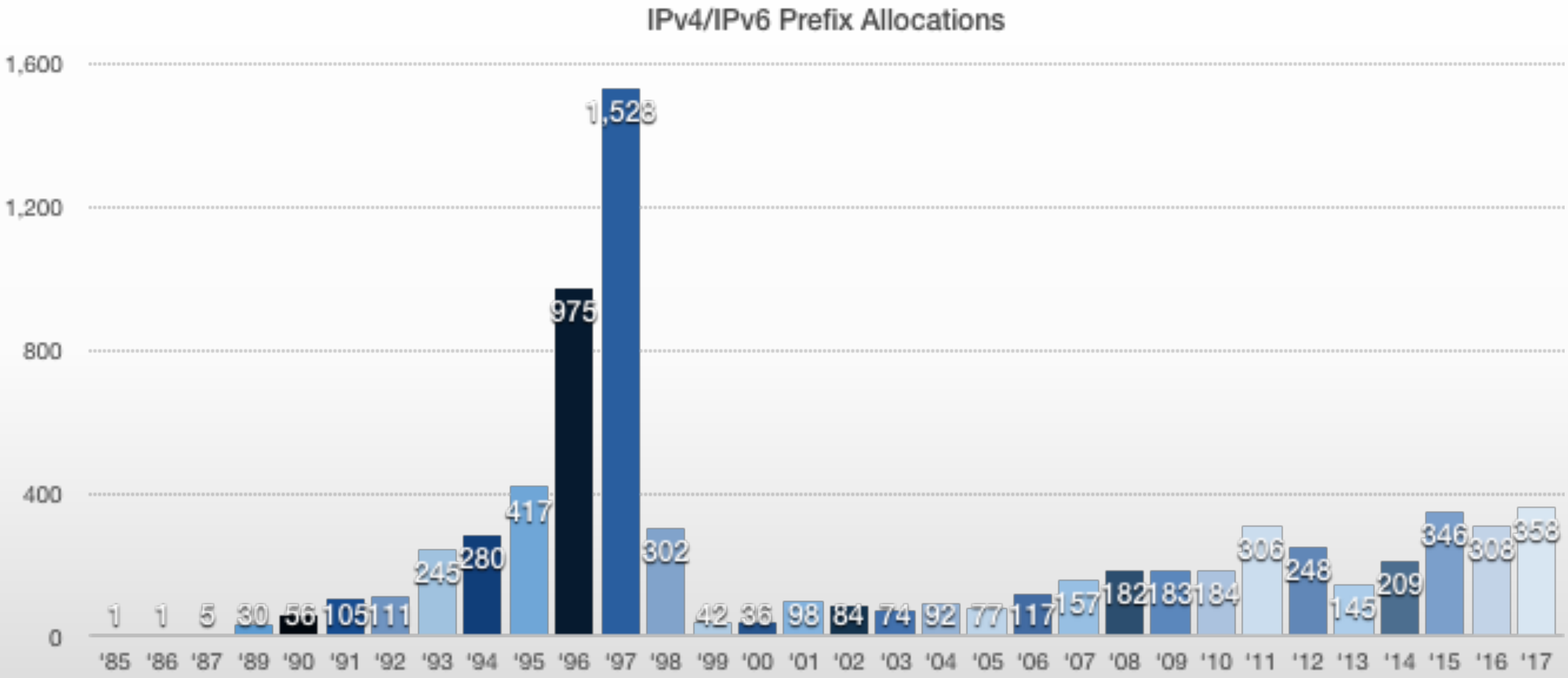
Data Source: http://ftp.apnic.net/apnic/stats/apnic/delegated-apnic-latest

No. of IPv6 Prefixes: 1126



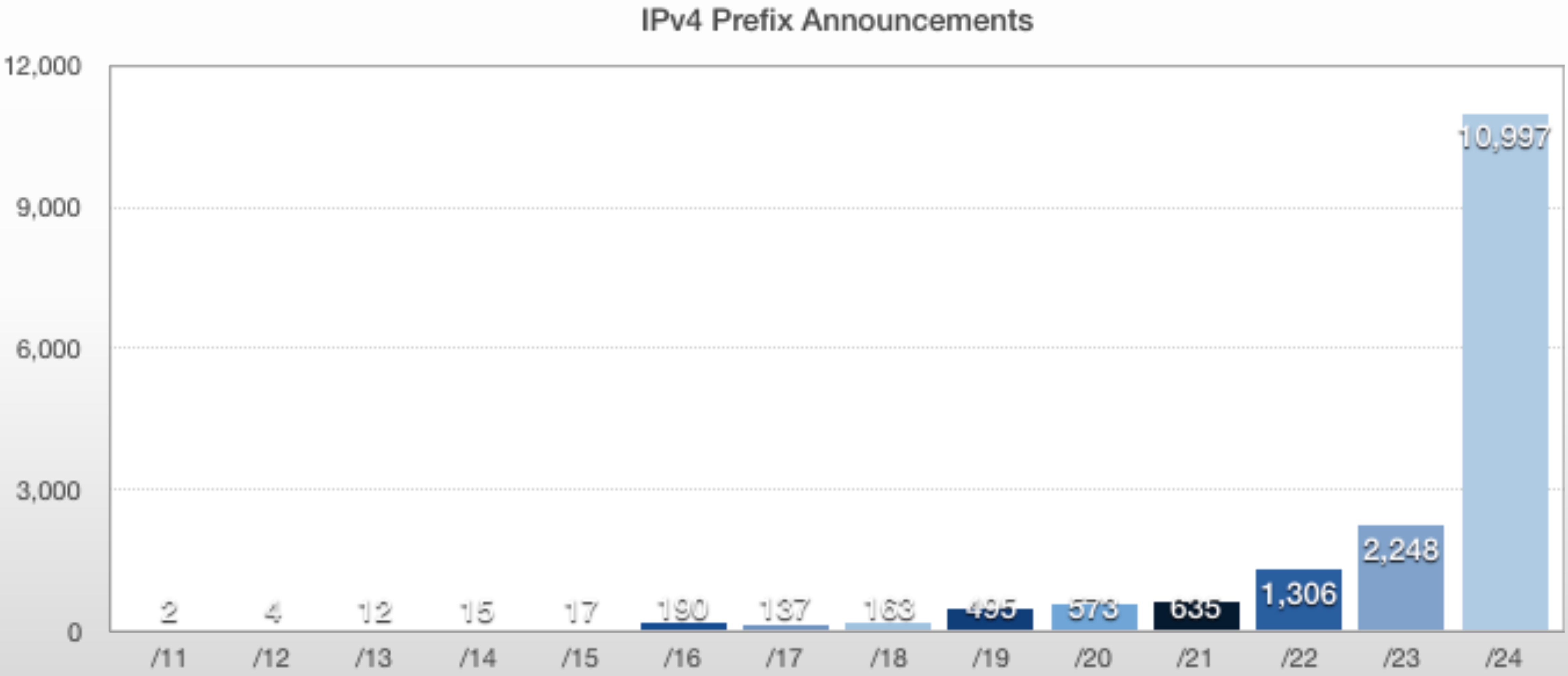
Data Source: http://ftp.apnic.net/apnic/stats/apnic/delegated-apnic-latest

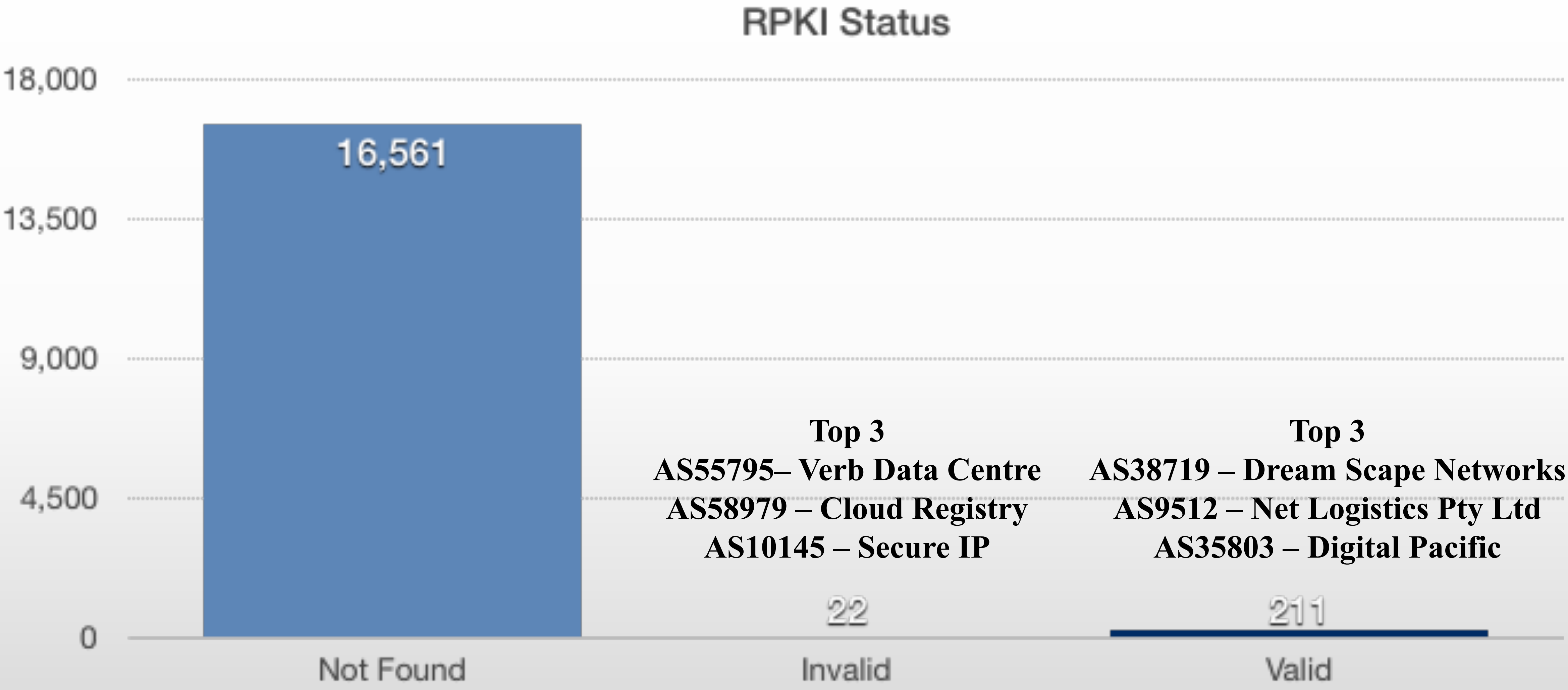
No. of IPv4 Prefixes: 7462



Data Source: http://ftp.apnic.net/apnic/stats/apnic/delegated-apnic-latest

No. of Prefixes Announced: 16794





Top 3
AS55795– Verb Data Centre
AS58979 – Cloud Registry
AS10145 – Secure IP

Top 3
AS38719 – Dream Scape Networks
AS9512 – Net Logistics Pty Ltd
AS35803 – Digital Pacific

Bogus Prefixes/ASNs from Australia

Possible Bogus Prefixes

Prefix	Origin AS	AS Description	Peer AS	Peer AS Desc.
45.124.164.0/22	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
45.124.164.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
45.124.165.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
45.124.166.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
45.124.167.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
103.20.219.0/24	AS55795	VERBDC1-AS-AP Verb Data Centre Pty Ltd, AU	AS17819	Equinix
103.58.216.0/22	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
103.58.216.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
103.58.217.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
103.58.218.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
103.58.219.0/24	AS38803	GOLDENIT-PTY-LTD-AUSTRALIA-AP Goldenit Pty ltd Australia, AU	AS4826	Vocus
119.160.232.0/21	AS132070	INTERVOLVE-BRISBANE-AS-AP Interhost Pacific Pty Ltd t/a Intervolve., AU	-	-
203.89.101.0/24	AS9499	SUPERLOOP-AS-AP SUPERLOOP (AUSTRALIA) PTY LTD, AU	AS24093	BigAir
203.89.103.0/24	AS9499	SUPERLOOP-AS-AP SUPERLOOP (AUSTRALIA) PTY LTD, AU	AS24093	BigAir
203.89.107.0/24	AS9499	SUPERLOOP-AS-AP SUPERLOOP (AUSTRALIA) PTY LTD, AU	AS24093	BigAir
220.152.112.0/21	AS23871	AINS-AS-AP Australia Internet Solutions, AU	AS7474	Optus

http://www.cidr-report.org/as2.0/

Possible Bogus ASNs

AS55481	Announced by	AS1221	ASN-TELSTRA Telstra Pty Ltd, AU
AS64521	Announced by	AS9822	AMNET-AU-AP Amnet IT Services Pty Ltd, AU
AS64627	Announced by	AS23871	AINS-AS-AP Australia Internet Solutions, AU
AS65315	Announced by	AS134188	NTTDATAVTS-AS-AP NTT DATA Victorian Ticketing System Pty Ltd, AU
AS65535	Announced by	AS133178	ACABPS-AS-AP Australian Customs and Border Protection Service, AU
AS4294836336	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294836363	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294836392	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294836409	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294836414	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294836444	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901860	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901861	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901863	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901864	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901865	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901866	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901867	Announced by	AS2764	AAPT AAPT Limited, AU

http://www.cidr-report.org/as2.0/

Possible Bogus ASNs

AS4294901868	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901869	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901870	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901874	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901875	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901876	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901878	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901879	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901880	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901881	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901882	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901884	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901886	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901888	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901889	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901890	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901891	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901892	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901893	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901894	Announced by	AS2764	AAPT AAPT Limited, AU

http://www.cidr-report.org/as2.0/

Possible Bogus ASNs

AS4294901895	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901896	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901897	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901898	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901900	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901901	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901902	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901903	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901904	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901906	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901908	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901909	Announced by	AS2764	AAPT AAPT Limited, AU
AS4294901910	Announced by	AS2764	AAPT AAPT Limited, AU

http://www.cidr-report.org/as2.0/

Spoofer Results

Session	Timestamp	Client Prefix	ASN	NAT	Spoof Private	Spoof Routable	Adjacency Spoofing
228714	2017-05-23 12:47:28	180.214.94.x/24	9268 (OVERTHEWIRE-AS-AP)	no	received	received	/8
160215	2017-03-07 05:01:32	125.63.49.x/24	45570 (NETPRES-AS-AP)	no	received	received	/8
138763	2017-02-02 05:34:04	117.120.47.x/24	4851 (HOSTNETWORKS-AS-AU-AP)	no	**blocked**	blocked	/21
		2402:e400:10xx::/40	4851 (HOSTNETWORKS-AS-AU-AP)	no	received	received	none
134201	2017-01-26 04:18:36	117.120.47.x/24	4851 (HOSTNETWORKS-AS-AU-AP)	no	**blocked**	blocked	/21
		2402:e400:10xx::/40	4851 (HOSTNETWORKS-AS-AU-AP)	no	received	received	none
132112	2017-01-19 03:03:17	117.120.47.x/24	4851 (HOSTNETWORKS-AS-AU-AP)	no	**blocked**	blocked	/21
		2402:e400:10xx::/40	4851 (HOSTNETWORKS-AS-AU-AP)	no	received	received	none
127707	2017-01-12 01:47:47	117.120.47.x/24	4851 (HOSTNETWORKS-AS-AU-AP)	no	**blocked**	blocked	/21
		2402:e400:10xx::/40	4851 (HOSTNETWORKS-AS-AU-AP)	no	received	received	none
123342	2017-01-05 00:32:31	117.120.47.x/24	4851 (HOSTNETWORKS-AS-AU-AP)	no	**blocked**	blocked	/21
		2402:e400:10xx::/40	4851 (HOSTNETWORKS-AS-AU-AP)	no	received	received	none

https://spoofer.caida.org/recent_tests.php?as_include=&country_include=aus&no_block=1

Conclusion

MANRS Adds Value

- Strong motivations for service providers
  - Significant differentiation for enterprise buyers
    - Identifiable value in a vague market
  - Education is required for enterprise
    - Enterprises want to know more
    - Security information has value
    - Questions on regulatory involvement…
  - Additional revenue opportunities for providers
    - Operational information
    - Information security information feeds
    - Sticky services

Please join us to make routing more secure

- Go to https://www.manrs.org/signup/
  - Provide requested information
  - Please provide as much detail on how Actions are implemented as possible
- We may ask questions and ask you to run a few tests
  - Routing “background check”
  - Spoofer https://www.caida.org/projects/spoofer/
- Your answer to “Why did you decide to join?” may be displayed in the testimonials
- Download the logo and use it
- Become an active MANRS participant

Questions?

- Feel free to contact us if you are interested and want to learn more
  - http://www.routingmanifesto.org/contact/
  - Mail: routingmanifesto@isoc.org
- Looking forward to your sign-ups:
  - http://www.routingmanifesto.org/signup/