BLACK & WHITE PAPER

451 Research Advisory

# MANRS Project Study Report

AUGUST 2017

COMMISSIONED BY

Internet Society

## About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners – what they are doing, and why they are doing it.

## About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

© 2017 451 Research, LLC and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

**NEW YORK**
1411 Broadway
New York, NY 10018
+1 212 505 3030

**SAN FRANCISCO**
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

**LONDON**
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 207 426 1050

**BOSTON**
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

# EXECUTIVE SUMMARY

The Mutually Agreed Norms for Routing Security (MANRS) project was founded with the ambitious goal of improving the security and reliability of the global Internet. As MANRS approaches the third anniversary of its founding, a study has been undertaken to better understand the attitudes and perceptions of Internet service providers and the broader enterprise community around the project. This report documents the results of that study and provides advice and perspectives on the state and future of the MANRS project. It includes use cases for service providers and enterprises that outline the benefits of MANRS participation.

The interpretation of the study has yielded some interesting results that are relevant to the project participants and the project board. The key points from the study are:

- While MANRS itself is not well known by enterprises, its attributes are highly valued.
- Enterprises have high expectations for MANRS efforts.
- Enterprise perceptions of MANRS can translate into increased revenue for service providers.
- Existing MANRS actions cover a reasonable set of controls.
- There are options to extend the MANRS actions for some providers.

The study shows that there is considerable unrealized potential with the MANRS project and that enterprise interest should be a strong incentive for more service providers to participate. Market education could be particularly effective in overcoming the operational inertia that many providers face.

## Project Description

This research project was undertaken to gain a deeper understanding of the progress that MANRS has made, including its visibility and perception within enterprise and service-provider communities, and to explore actions that could be taken to increase participation and awareness. Discrete studies were conducted with separate populations of service providers and enterprise IT personnel who are involved in Internet services contracts. The studies identified their awareness of MANRS and delved into their opinions of the various aspects of implementation and the perceived value of the MANRS actions. The study responses were analyzed, and the correlations and divergences between the two groups were assessed. This report details the findings and conclusions that have been made.

Two use cases have been created in addition to this report, one addressing enterprises and one addressing service providers. Each looks into the benefits of greater involvement in MANRS for the specific group and relies on the data that was collected as part of the studies.

## Study Methodology

Achieving a deeper understanding of perceptions in areas as broad as information and routing security can be complex. The study that has been undertaken for this project sought to compare the results from two discrete but interconnected communities. The expectation was that service providers would have some exposure to MANRS, and that the level of understanding was important. For enterprises, the expectation was that there would be more limited exposure, and the more important aspects were the alignment of values around MANRS characteristics. Because of this, while the studies worked from a common base, the question sets used had a different focus for each of the target groups. An independent organization was used to conduct the final studies.

The service-provider study was narrower in scope and looked in more depth than the enterprise study. The question set was tested on an initial group of 10 providers who were known to have an understanding of the MANRS project. It was conducted through open-ended telephone interviews. The results of the initial group interviews were not included in the study, but were used to shape the final question sets for each subsequent group. The initial group was geographically diverse, with representatives from Asia, Europe and North America. The formal study featured telephone interviews with 25 randomly selected service-provider employees who were screened to ensure they had involvement with decisions in routing infrastructure operations and were in management roles within their organizations. This group was almost entirely from North America and had an even distribution of organizational sizes, with a median size of 2,500–4,999 employees.

The enterprise user study was conducted by web form with a randomly selected group of 250 respondents who were screened to ensure they were IT management staff that were involved in the procurement and contracting of Internet services. Company size was limited to a minimum of 1,000 employees in an effort to target those with more significant requirements for Internet services. The respondents were primarily from North America and broadly distributed across industry verticals. Manufacturing and professional services organizations were most strongly represented, with each vertical accounting for 14% of the total panel. Healthcare, telecommunications and retail followed closely behind them, with single-digit percentages for other verticals. Median organizational size was also 2,500–4,999.

The full demographics of the study respondents are available in the study data.

## Results Overview

The studies confirmed our expectations that MANRS visibility had room for improvement with both enterprises and service providers. They also revealed that service providers underestimated the value their customers place on their broad security positioning. One unexpected finding was the extent to which enterprises saw security as a core value for themselves. This may be the result of increasing awareness due to expanded media coverage of security incidents, but could also reflect increasing maturity in IT positioning across enterprises.

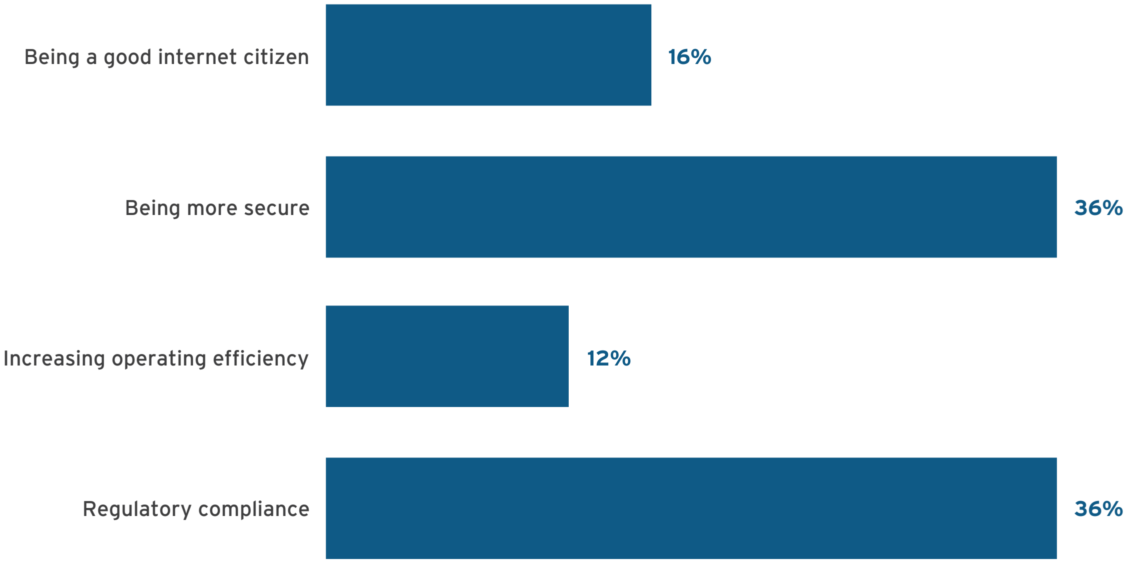
## Service-Provider Study Details

The service-provider study confirmed many of the concerns that had been expressed in the initial assessment. These concerns may not be fully qualified, however, since only a single respondent reported they had implemented most of the MANRS actions, and, as such, the service providers surveyed don't have direct experience in MANRS implementation. This means the perceptions of the survey base are a reasonable representation of the service-provider community that the MANRS project hopes to reach – namely, those that have yet to participate.

Almost one-third of the respondents hadn't heard of MANRS, while slightly more were well aware of the project. That means estimates of implementation efforts are speculative. Interestingly, none of the respondents were concerned that MANRS would increase operational effort or complexity, while over two-thirds (68%) felt that it could decrease them. Quite often, new, untried technologies are perceived as requiring more effort, so this is a positive sign regarding service-provider expectations. That said, just over half (52%) of respondents were moderately concerned about MANRS implementation causing an outage – 24% were not concerned, while an equal number were very concerned, indicating that some operational disruption was expected.

The implications of culpability after adopting MANRS were moderate at 60% of respondents, but 28% expressed no concern at all. This is most likely due to different styles of engagement with customers at various service providers. Those who are already identifying themselves with a security interest had lower levels of concern.

### Figure 1: Reasons for Implementation



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

There was an unsurprising disconnect regarding the decision process around MANRS. While 64% of respondents reported that technical management would drive adoption, only 4% of those teams had the authority to implement it – instead, 80% of service providers would need approval by mid- or high-level management (40% for each). This will present challenges in organizations where the implementation imperatives aren't clearly communicated across the organization.

The motivations for implementation were also misaligned with the enterprise results. While 97% of enterprises were considering including MANRS compliance in an RFP and 13% would consider it for a lockout requirement, service-provider survey results reflected a lack of understanding of that importance. Only 12% of service providers would plan for implementation if a MANRS requirement arrived as part of an RFP. It would spur consideration for 72%, and it would have no impact on 16%. These responses can be seen as speculative, since there has been little to no use of MANRS compliance in provider selection. Our estimation is that the responses would be more greatly skewed toward implementation if there were any experience of MANRS compliance in RFP and tender processes.

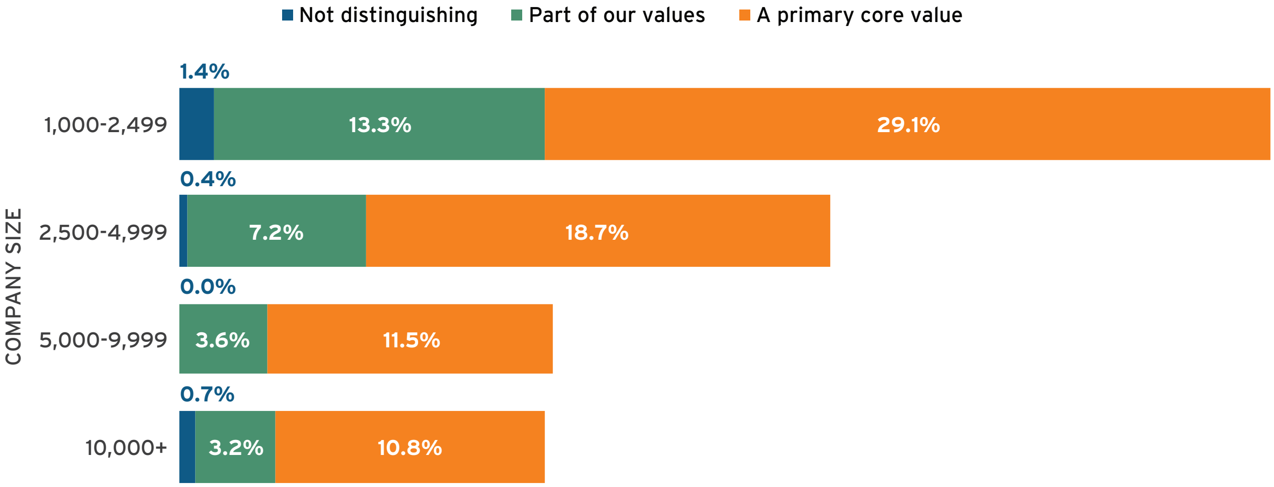
## SERVICE-PROVIDER STUDY IMPACTS

There is cautious enthusiasm for MANRS in the service-provider community. This is heartening in the face of an expectation that customers might not value MANRS. To increase the motivations for implementation, though, there is a knowledge gap that needs to be bridged with education, and there must be solid stories on both sides. MANRS could get enterprises to spend more with service providers, which is a message upper management wants to hear, and enterprises value the security details that the technical teams are keen to promote. Enterprise interest in including MANRS in RFP and tender processes should only increase that potential.

## Enterprise Study Details

The enterprise portion of the study examined security concerns and explored their alignment with MANRS values. A surprisingly large number of enterprise respondents (71%) stated that security was a core value for their organization. Evaluating the breakdown by company size showed that smaller enterprises had an outsized concern about security as part of their primary values. That level of concern persisted across many responses for the enterprise study.

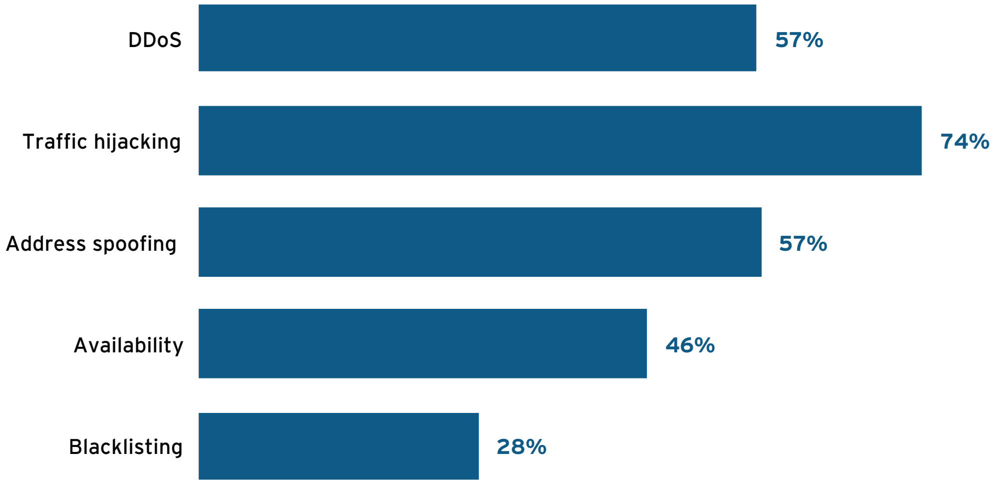
### Figure 2: Importance of Overall Security Posture



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

When the types of security concerns were examined, traffic hijacking led the list. This can be viewed as another confirmation that the respondents' focus on Internet services may be creating a greater awareness of the types of issues that MANRS is looking to address. It bodes well for their expectations.

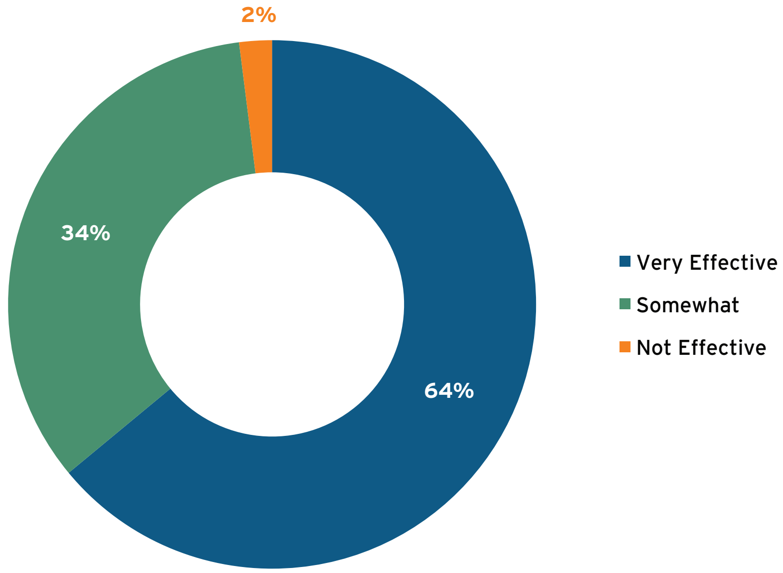
### Figure 3: Internet Security Concerns



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

Alongside those concerns, there was confidence that MANRS actions could be effective in dealing with them. This paralleled a set of positive responses to MANRS values and the expectations expressed in the narrative entries.

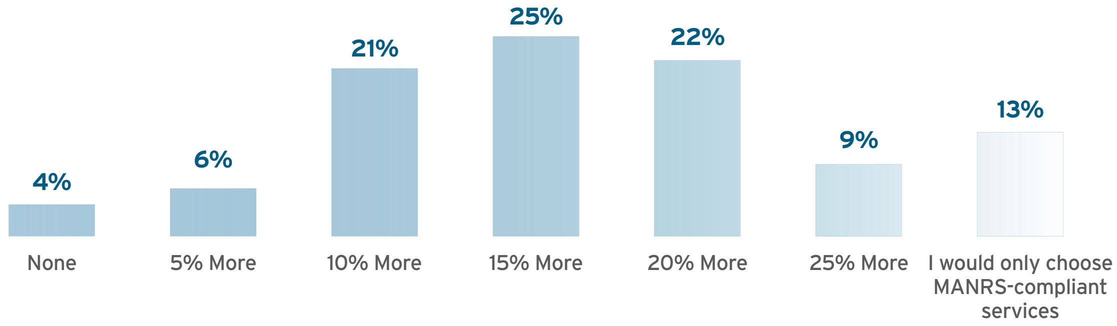
## Figure 4: MANRS Effectiveness



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

Most importantly, enterprises showed a willingness to pay for what they saw as valuable. In identifying what price increase they would support for MANRS compliance, the median value was 15% – an impressive premium for what is often seen as a commodity service.

## Figure 5: Enterprise Pricing Premium for MANRS



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

In addition, 13% indicated that, if available, they would only select a vendor who was MANRS compliant in a competitive situation.

### ENTERPRISE STUDY IMPACTS

The enterprise results indicate there is great opportunity for service providers that participate in MANRS. Enterprise decision-makers are looking for the kinds of values that MANRS confers on participants. There are opportunities for revenue enhancement and competitive improvement that are real and significant. Security is a strong focus area for enterprises, and MANRS can be a mark of trust in a critical part of their IT infrastructure at a time when it is increasingly difficult to differentiate between providers.

## Use Cases

The two use cases for this research project address the benefits of MANRS participation for service providers and enterprise organizations. They are delivered as separate documents and are included here for reference.

## Recommendations

The studies have identified that there is significant potential for additional adoption of the MANRS project as it stands today, as well as options to expand the program for certain segments of the service-provider community. The primary findings of the study can be summarized with the following:

- MANRS awareness in the enterprise could drive service-provider participation.
- Service-provider education around enterprise values could drive participation.
- Some level of regulatory involvement may be needed.

MANRS awareness in the enterprise can be driven via partnerships with participating service providers. Enterprises report that they see service providers as sources of technical authority, and providers gain direct benefits in competitive positioning as part of that promotion. There are additional paths through peer organizations for enterprises, such as user groups and online communities. These are also avenues that could be pursued in partnership with service providers. Security-focused forums have the greatest potential, such as:

- ISACA – A nonprofit that offers security and governance certification and community.
- RSA Conference – Security-focused conference where MANRS sessions could be proposed.
- (ISC)2 – A security certification nonprofit that also runs security conferences.
- InfraGard – A US coordinating organization sponsored by the Federal Bureau of Investigation that addresses infrastructure protection.

It will be important to further educate service providers on the level of value that enterprises see in MANRS. There is a clear misalignment here, and the differentiation that MANRS provides in the eyes of enterprise decision-makers works in the providers' favor. Given the smaller size of the community, direct promotion can be effective, as well as targeted events. Operators groups and provider-specific conferences could include:

- NANOG, RIPE, AfNOG, APRICOT and other operators groups
- HostingCon – Annual conference focused on service providers

Both service providers and enterprises identified that some level of regulatory involvement would be a strong driver for MANRS adoption. This is an area where we would recommend caution, since the nature and direction of response in governmental interactions can be difficult to manage. An effective path would be to work with auditors and industry organizations to promote activities that align with governmental imperatives. Efforts from the US National Institute of Standards (NIST) and the EU Agency for Network and Information Security (ENISA) have produced recommendations for improving enterprise security. The task of interpreting and implementing these recommendations often falls to auditors and security services companies. Working to include MANRS in their practices could be a practical means of leveraging the priorities of the regulatory mandates without the risk of direct government action. The ISACA COBIT framework is another possibility. There may also be paths with organizations such as the Payment Card Industry Security Standards Council, but these are less directly relevant to MANRS target audience.

The future of MANRS can include a number of options for the expansion of its mandate. The existing MANRS actions fit well with the scope of responsibilities for Internet service providers. As more providers begin to offer enhanced security services, MANRS could offer guidance in those areas. Service providers are looking to address growing demand from enterprise customers in managed security services. *The 451 Research Voice of the Enterprise (VotE) Information Security study from Q1 2017* indicated that security information and event management (SIEM) projects have risen to the second spot among enterprise 'top five' projects for the first time, tied with endpoint security and only slightly behind security awareness initiatives. That's a strong indication of the priority that enterprises are placing on operational security management. Service providers can offer advisory consulting and managed services to address these demands.

In this study, enterprises identified concerns about traffic integrity as a high priority. Traffic routing, interception and hijacking was reported as the leading security concern (at 74%, with DDoS and address spoofing tying for second at 57% each), while route validation was the leading MANRS value (32%) in a separate question. That concern could extend to other areas of infrastructure integrity. MANRS could identify technologies such as namespace security, which is being addressed with DNSSEC. While service providers rely on registrars for DNSSEC implementation, they often have close working relationships and could provide implementation services to enterprises looking to implement DNSSEC. This could enhance the trusted security advisor role that service providers have begun to assume already.

MANRS could also assist in defining the framework of another revenue opportunity for service providers. Many enterprises are incorporating intelligence feeds into their operations. Enterprises are looking to improve their situational awareness and are interested in operational information that can be fed to SIEM systems. The information and event streams that MANRS actions could generate have value to enterprises. Anti-spoofing and route validation controls often generate log messages that could be delivered as an intelligence feed. The MANRS project could define a standard format for these intelligence feeds to aid service providers in integrating them with their enterprise customers. This could be an effort made in collaboration with other organizations that are creating formats for security information exchange. STIX, Cybox and TAXII are finding application with a number of enterprises today, and would be useful starting points. Creating monetizable services as part of MANRS could be one more reason to participate.

While there have been challenges in creating a dramatic increase in MANRS adoption, the studies have shown there is solid alignment between the motivations of service providers and the aspirations of enterprises. With additional effort, bringing these two together could create a bright future for MANRS.

## About the Author

Eric Hanselman is the Chief Analyst at 451 Research. He has extensive, hands-on understanding of a broad range of IT subject areas, with direct experience in the areas of networks, virtualization, security and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines. The convergence of forces across the technology landscape is creating tectonic shifts in the industry, including SDN/NFV, hyperconvergence and the Internet of Things (IoT). Eric helps 451 Research's clients navigate these turbulent waters and determine their impacts and how they can best capitalize on them.

For more than 20 years, Eric has worked with segment leaders in a spectrum of technologies, most recently as CTO of Leostream Corporation, a virtualization management provider. Prior to that, Eric delivered security solutions for IBM and Internet Security Systems. At Wellfleet/Bay Networks, Sitara Networks and NEC, he was involved in the introduction of many new technologies ranging from high-performance image analysis to rollouts for IPv6. Eric holds a patent in image compression systems. He is also a member of the Institute of Electrical and Electronics Engineers (IEEE), a Certified Information Systems Security Professional (CISSP) and a VMware Certified Professional (VCP), and he is a frequent speaker at leading industry conferences. He majored in chemistry at Reed College.

# Appendix I: Service Providers – Security Brings Better Business to the Table

## OVERVIEW

It can be challenging for Internet service providers to differentiate themselves in the market today. Customers are often confused about capabilities and performance differentiation between providers, and it can be difficult to clearly express the value that a provider offers. Concrete distinctions are possible in the area of security, which has well established value with enterprises and can significantly impact customer procurement and decision processes. The Mutually Agreed Norms for Routing Security (MANRS) project can provide a mark of security proficiency and community involvement for those providers that are able to participate. That distinction can add competitive value to a provider and can also enhance operational effectiveness. A new study from 451 Research has detailed what that value is and how service providers can put it to work.

## ENTERPRISE VALUE

As enterprises look to select infrastructure partners, they are juggling a collection of requirements that can be difficult to manage. Where they have trouble determining the value of competing aspects of various providers' offerings, their focus often lands on pricing. To move the decision point beyond price alone, providers need to have qualities that can be easily identified and can differentiate them. The 451 Research study showed that the security posture of a service provider is important to enterprises and that MANRS participation is something that has value. While MANRS isn't well known by enterprises, the ideas that the project represents are held in high regard and come with real value to enterprise buyers.

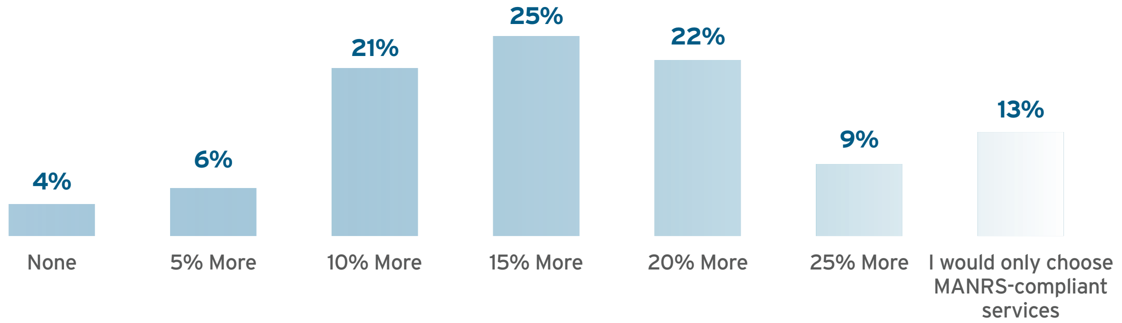
The study included a brief introduction to the project and then asked respondents how they valued what MANRS participation offered and which of the project directives and outcomes were most valuable to them. The first of these valuations was an assessment of how much more they would be willing to spend, if anything, for services from a provider that was a MANRS participant. The median value of the price premium was 15% – a considerable valuation for what's considered a commodity service by many buyers. In addition, 33% of respondents said they would use MANRS participation as an exclusive criterion for vendor selection, if it were available. A full 97% were interested in putting MANRS participation in RFP and tender requirements.

This valuation means that MANRS participation can convey a set of benefits for service providers:

- Improved competitive positioning in the RFP and tender process
- Increased customer retention and lower churn
- Opportunities for value-added services

All of this is in addition to the internal benefits that service providers can achieve with MANRS. Service providers can improve their operational efficiency by establishing better communications paths with their peers. They also have the potential to improve security operations by identifying problems with clients and peers earlier, and there is the added value of contributing to the overall security of the Internet community.

Figure 1: Enterprise Pricing Premium for MANRS



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

## MONETIZING MANRS

There are a number of ways in which service providers can put the value of MANRS participation to work for them:

- Include MANRS in proposals
- Publicize MANRS values to customers
- Offer value-added services

Capitalizing directly on the value of MANRS with increased prices is problematic. The reality of most markets is that pricing comparisons will occur regardless of other aspects of a buying decision. Where MANRS participation can be useful is in reducing levels of discounting required to win contracts. Participation in MANRS can be used to increase the likelihood of selection in a competitive process. It can be used as a means to eliminate competitors who are not qualified. The study results have shown that enterprises are enthusiastic about including MANRS as a selection criterion. Additional analysis has shown that improvements in competitive position and reductions in necessary discounts could add as much as 7% to longer-term revenue.

Customers value MANRS participation, and service providers can leverage that by publicizing their involvement. By including information and branding in marketing and communications to customers and the broader market, service providers can establish a strong impression in an area that customers see as valuable. Publicizing MANRS can refresh the understanding customers have that their providers have valuable capabilities and can reduce the likelihood that they would consider switching vendors. That customer bond can be strengthened with security-focused communications and community building. The 451 Research study also showed that being part of a larger community that is working toward improving the security of the Internet is another aspect of MANRS that's important to customers.

Service providers can gain additional revenue by adding MANRS-derived services to their portfolio. Anti-spoofing controls that log activity can be used to generate periodic reports for customers. These reports can be part of an intelligence feed that alerts customers to misconfigurations or potential attacks. This type of service can be inexpensive to operate, if appropriately automated, and can provide additional customer binding, in addition to generating revenue.

## CONCLUSIONS

For service providers, there are considerable benefits to participating in the MANRS project. It can increase their value to customers and potentially increase revenue. The MANRS directives are a useful guide to increasing operational efficiency while contributing to the improvement of the security of the Internet community. The combination of customer impact and internal benefit should be sufficient motivation for providers to become part of this growing community.

# Appendix II: Enterprises – Joining a Community for Greater Security

## OVERVIEW

Enterprises face many challenges in running their IT infrastructure, and one of the most significant is the selection of service providers. Assessing provider capabilities and performance can be a complex process. One factor that can aide in this decision is a provider's participation in the Mutually Agreed Norms for Routing Security (MANRS) project. MANRS is a collaborative project that focuses on concrete steps to enhance the security posture of participants and thereby contribute to the overall security of the Internet community. In working with a service provider that is part of the MANRS project, enterprises can establish themselves within the vanguard of those with a security-forward position and join the larger Internet community that is working to improve security and reliability.

## THE MANRS PROJECT GOALS

The MANRS project seeks to improve the security and reliability of the global Internet by standardizing the controls and operating principles used by network operators. It lays out a set of four actions that participants put to work as part of their operations and their interactions with others. Collectively, these efforts aim to curb accidental or intentional activities that can damage Internet reliability. The four actions are:

- Route Filtering – Preventing the propagation of incorrect routing information.
- Anti-spoofing – Preventing traffic with spoofed source IP addresses.
- Coordination – Facilitating global operational communication and coordination between network operators.
- Global Validation – Facilitating validation of routing information on a global scale.

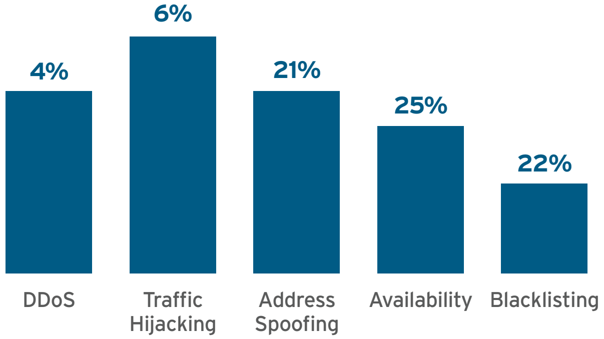
Together these actions can help prevent problems and speed resolution when problems occur. Service providers that are MANRS participants have made a commitment to be part of this effort. One of the challenges of the Internet's structure is that it requires larger community efforts such as this in order to be effective. This effort can help in reducing perennial problems, such as traffic rerouting (detouring), denial-of-service attacks (DDoS) and traffic hijacking.

## THE MANRS STUDY

In an effort to evaluate and assess the MANRS project and its impact on enterprises and service providers, 451 Research undertook an expansive study, the results of which provide useful peer benchmarking data on the importance and impact of the project for enterprises. Over 70% of study respondents identified that their information security posture was a primary core value to their organization. A big part of any enterprise security environments is their connection to the Internet and the partners they select to deliver it, making MANRS an important qualifier.

The study also explored Internet security concerns for enterprises and sought to quantify how enterprises expected to address them. The greatest concern was traffic hijacking, a problem that has often been in the news, and one that has customer satisfaction implications beyond its security implications.

### Figure 1: Internet Security Concerns

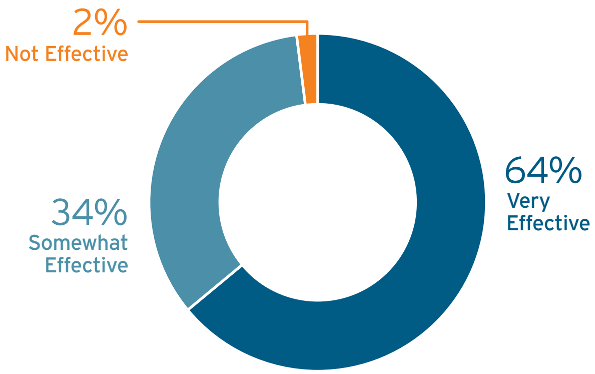


*Source: 451 Research study: MANRS Perception and Action, July, 2017*

The next two most important concerns have an intrinsic link. While denial-of-service attacks are a concern, address spoofing – the technique that can be used to cloak the origins of DDoS attacks – received an equal measure of concern among study respondents. The MANRS project seeks to address the causes of these concerns through its four actions.

The study also evaluated the responding organizations' thoughts about how effective the MANRS project would be at combating the problems that concerned them. Almost the entire respondent pool reported they felt that, over time, the project would be an aid in addressing Internet security concerns. Almost two-thirds felt it would be very effective.

Figure 2: MANRS Effectiveness



*Source: 451 Research study: MANRS Perception and Action, July, 2017*

## LEVERAGING MANRS FOR ENTERPRISE

One of the primary benefits of the MANRS project for enterprises is the indication that it gives for the attitude and initiative of service providers around operational security. The typical enterprise expends significant effort in selecting IT infrastructure partners, but effective selection criteria can be hard to come by. Service providers that are participating in MANRS have made an effort to improve their security posture, and are working with a larger community to reduce threats to Internet security and stability. MANRS participation can be a reasonable selection metric and can be included in RFP, tender and purchasing processes to improve the understanding of a provider's capabilities. In the 451 Research study, 97% of respondents indicated they would consider including MANRS participation in their selection process.

The MANRS project also provides a means for organizations to join a larger community that's concerned with security. This can help organizations looking to collaborate on addressing concerns.  It can be a means to identify ecosystem partners with whom enterprises can join forces to create a stronger foundation for security. In regulated industries, MANRS links can be an additional factor for auditors to consider when assessing the overall security posture of an organization.

MANRS can also strengthen an enterprise's bottom line. As the 451 Research study showed, most organizations are concerned about security, and being part of the MANRS community can strengthen enterprise security credentials. It communicates an enterprise's security investment to its customers. MANRS involvement can be included in marketing materials and could be part of a larger brand statement.

While the MANRS project is targeted at service providers, any organization that has peering arrangements that involve BGP can also become part of the community. Incorporating the MANRS actions into IT operations can add maturity and increase operational efficiency.

## CONCLUSIONS

The MANRS project offers a number of benefits for enterprises that are directly attainable. There should be careful consideration given to MANRS participation, not only by an enterprise's service providers, but potentially for the organization itself. The wider Internet community can benefit from the greater security awareness that the project offers, and enterprises play an important role here. Enterprises that join the MANRS community can improve their security posture, as well as their business.

# Appendix III

## RFP LANGUAGE FOR MANRS SELECTION

The following is sample language that could be used by enterprises interested in making MANRS compliance part of a Request for Proposal process in selecting Internet service providers. This is an example only, and is not legal advice. Appropriate legal counsel should always be consulted in the preparation of any RFP document.

### Eligibility Requirements for Proposing Organizations

1. Proposing organization's MANRS compliance

> XXXX supports the broader Internet community efforts to improve resilience and security. All proposing organizations shall have been participants in and compliant with the Mutually Agreed Norms for Routing Security project (*https://www.manrs.org*) for at least the 30 days preceding proposal submission. Proposing organizations will maintain compliance throughout the term of the contract and will notify XXXX if, at any time, compliance lapses. Notification must be through the contacts specified in the contract and must be in the form of written communication. Compliance will be determined by the implementation of at least the minimum set of Expected Actions defined by the MANRS project. Lapses in compliance will be considered material breach of any contract in force.