How can IT executives improve global routing security?

Information for CIOs, CTOs and CISOs

Today, the Internet plays an essential role in our increasingly digital societies around the world. From banking to education, health to logistics, just about every sector relies on Internet-based applications and services to function.

Our increased dependence on digital technologies brings with it growing concerns around Internet security. While there are many dimensions to Internet security, it's critical we secure the key building blocks of the Internet's infrastructure.

The Internet's routing system enables data to flow from one point to another. Ensuring that this data flows correctly to its intended recipient, is the foundation of Internet network security.

Thousands of Internet routing incidents occur every year, leading to economic harm by:

- making key services unreachable
- disrupting e-commerce
- allowing malicious actors to spy on users and with it, the potential to compromise systems.

While existing security measures can help address many of these routing incidents, the solutions they provide are often limited. The interconnected nature of networks means that many solutions only work when other networks make the same improvements. **We need collective action to make real change.**

As an executive, you are a critical decision-maker. You have an important role to play in establishing an effective network security posture that ultimately strengthens and protects your enterprise as well as the Internet itself.

What is MANRS?

The Mutually Agreed Norms for Routing Security (MANRS) is a community-driven initiative supported by Internet Society. MANRS provides a set of best practices based on existing norms for network operators to improve the security of the global Internet routing system.

By choosing service providers who are MANRS-compliant (and joining MANRS if you operate a network), your enterprise can both improve its security and help encourage other providers to improve their infrastructure.

MANRS defines four simple but concrete actions:

- Border gateway protocol (BGP) filtering;
- Anti-spoofing;
- Coordination; and,
- Global validation.

By implementing these actions, network operators can greatly improve Internet security and reliability. Two of the steps are preventative and help address the technical causes behind common routing incidents. The other steps take advantage of globally accessible information to help limit the impact of such incidents and decrease the likelihood of future incidents.

The MANRS actions define outcomes rather than specific methods. This allows implementation to change with technology and helps establish MANRS actions as best practice.

Alongside routing incidents, MANRS seeks to address ecosystem challenges in the global routing system.

MANRS improves economic incentives for routing security by allowing network operators to demonstrate their commitment to:

- Security – by securing core Internet infrastructure for greater global Internet security.
- Customers – by ensuring the services they provide adhere to routing security best practices.
- Competitors – by ensuring routing security incidents don't have a cascading effect on other network operators.
- Policymakers – by ensuring a robust and resilient national Internet infrastructure in support of the larger cybersecurity agenda.

An independent study by 451 Research[1], commissioned by the Internet Society, found that traffic routing, hijacking and interception were the leading security concern for enterprises. Distributed denial of service (DDoS) attacks and address spoofing came in second.

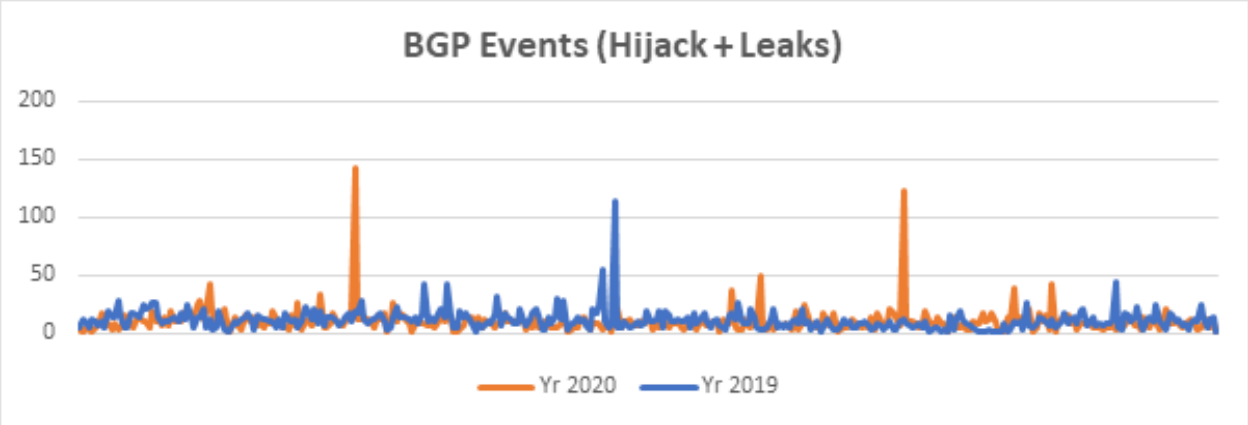
94% of enterprises said that they'd be willing to pay more for a vendor who was a MANRS member in a competitive situation.

This highlights the importance of MANRS implementation as an indicator of a network operator's sound security practices.

1 MANRS project study report: https://www.manrs.org/wp-content/uploads/2017/10/MANRS-451-Study-Report.pdf

Why does MANRS matter for enterprises?

In 2020, there were a total of 3,873 major network incidents that involved border gateway protocol (BGP) related attacks. Of these, 64% were hijacks and the rest were route leaks.



In 2019, there were 4,232 major network incidents that involved BGP, of which:

- 3.8% of all networks were affected by a routing incident
- 2% of all networks were responsible for the 4,232 routing security incidents.

These incidents can:

- create a serious strain on infrastructure
- result in dropped traffic
- allow for unauthorized inspection of traffic
- be used to perform Denial of Service (DoS) attacks.

In July 2020, there were two significant routing incidents in the global BGP routing system[2], impacting more than 1,500 networks worldwide. This highlighted the need for network operators to implement good routing security practices. These incidents impacted major North American network providers including TWC, Rogers and Charter, among others[3].

As a company leader, you can help your enterprise tackle routing security threats effectively by evaluating your Internet service providers (ISPs), content delivery networks (CDNs), and cloud hosting providers to make sure they follow security best practices.

How can MANRS help your organization?

1. **Ensure business continuity and prevent reputational damage:** Every enterprise should know whether their providers implement Internet routing best practices as part of their business continuity program. MANRS actions offer your enterprise an effective way to prevent network security mishaps that can cause significant reputational damage to any business.

2. **Security as a competitive advantage:** Implementing MANRS actions allows your business to communicate to customers that you're serious about your network infrastructure's security. This can serve as a critical differentiator for your organization.

3. **Qualify vendors or partners:** MANRS can help your enterprise's leadership to choose an appropriate network or cloud operations partner without having to undertake an extensive or complex assessment process. Multiple key vendors are already MANRS-compliant, which significantly simplifies the process of auditing their security capabilities.

4. **Alignment of infrastructure security across divisions:** Various elements of an enterprise's IT infrastructure may have their own security practices. Vulnerability in any one of them could pose a serious risk to your company. MANRS principles can serve as a useful guide if you're looking to align your entire network infrastructure under common standards.

5. **Threat intelligence:** You may be looking to improve your enterprise's situational awareness and be interested in incorporating intelligence feeds into your operations. The information and event streams that MANRS actions can generate will therefore hold value for your enterprise.

6. **A checklist for auditing infrastructure robustness:** You recognize the threat of network security issues to your company but, without MANRS actions in place, you may lack an effective and efficient way to audit your core network's preparedness. The MANRS checklist provides an easy means to assess the robustness of your enterprise's core network infrastructure.

7. **Access to an advanced knowledge base:** MANRS give you access to a large community focused on addressing security issues. This can help your organization to build a stronger foundation for security through collaborations.

Given the significant impact of routing incidents on critical networks, we need to give high priority to protecting and improving our network infrastructure. However, research shows a general lack of understanding of the fact that simple steps can dramatically reduce such incidents.

Some of the measures outlined above aren't entirely new and some organizations may be working to integrate such measures in the near future. To ensure a healthier and more robust network infrastructure, we must prioritize the measures highlighted in this document, and back their implementation with adequate resources.

- Find out more about MANRS: manrs.org
- Read about the Internet Society's work: internetsociety.org