Best Practices Briefing

Network Refresh and Lifecycle Management for Enhanced Security and Reliabillity

Managing technology assets through their lifecycles is one of the most difficult challenges of any IT organization. The network is arguably the most complex and critical IT environment to maintain due to its constantly changing nature and the number of business functions dependent upon it. Modern networks must be able to scale without disruption while also supporting new devices and business requirements. Since changes can impact a wide range of stakeholders, network changes and upgrades are often delayed and minimized unless a problem occurs. When tactical problems must be addressed, refresh and lifecycle projects can fall down the priority list. The end result, technical debt accumulates, and it is common to have assets that are reaching end of life or end of support.

Other important but repetitive tasks, such as patching and asset inventory management, fall behind as the tyranny of the urgent consumes the team's attention. It is hard to keep staff engaged in mundane and thankless activities. Additionally, most enterprise automation projects fail to achieve the desired results. Security risk grows and accelerates as a result. The risk is compounded as hardware reaches its end-of-support phase as patches are less frequent or simply do not exist to address new threats. In addition to security risk, these dynamics also impact performance and reliability of the business operations the network supports.

With the growing sophistication of cyber threats and the constant need for high-performance networking, organizations must adopt a proactive approach to network refresh and lifecycle management. This briefing outlines how to establish a robust lifecycle program ensuring your cyber risk is minimized, your network is resilient, and your overall cost of operations is lower.

DISCUSSION FRAMEWORK:

1. Introduction: The Need for Lifecycle Management

- Why organizations are largely reactive regarding life cycle management reducing efficiency, reliability and security.
- Increasing challenges in network operations as significant percentage of assets reach end of sale/end of support.
- How many key business initiatives today are growing demands on network speed and design.

2. Best Practices for Network Refresh

- Key business and technical indicators that a network refresh is needed.
- Critical Success factors for budgeting, planning, and executing a successful network refresh.
- Exploring options: Upgrades versus overhauls and how to choose.
- The significance of configuration compliance in secure and efficient network design and operations.
- The importance of having and effective Configuration Management Database (CMDB) to track assets, ensure compliance, and streamline the refresh processes.

3. Implementing a Lifecycle Management Program

- Steps to establish a lifecycle program, from inception to maintenance.
- Toolsets and policies for tracking hardware status.
- Importance of aligning your lifecycle program with vendor support cycles.
- Considerations around cabling infrastructure, including its role in networking, best practices for upgrades, and the need for regular assessments to ensure optimal performance and ease of troubleshooting.
- Integrating carrier services management into your network lifecycle program.

EXPECTED OUTCOMES:

The goal of this briefing is to collaborate with your team around the following:

- A proven methodology to assess the current state of your network infrastructure.
- A structured approach to planning and executing a network refresh.
- Best practices to establish a sustainable lifecycle management program.
- Actionable steps to ensure that outdated or end-of-support hardware is phased out safely and efficiently.

RECOMMENDED PARTICIPANTS:

CIOs, IT Leadership, Network Architects, Network Administrators, Network Operations Leadership, Security Officers, and anyone involved in the management and oversight of enterprise networking.

Expected time: 90 minutes