Five Costly Common Network Mistakes to Avoid

With today's healthcare organizations critically reliant on Internet access to provide patient care, health IT teams are rejecting the traditional self-management model in favor of managed services. Why? Because tasking already time-strapped technology teams with overseeing their organization's network can have severe financial ramifications and put your patients' welfare at risk.

1 Healthcare organizations that manage their own networks have to allocate expensive internal IT resources to outage recovery efforts and ongoing maintenance such as security patches, firmware management, and day-to-day issues.

Most healthcare providers don't have the capital or resources to staff the amount of experienced IT personnel needed to manage their complex networks in-house.

As health IT teams explore connectivity service options, they should consider the cost-saving benefits and increased efficiencies of having your network's design, installation, maintenance, monitoring, and support all managed through one experienced provider. Using a professional third party to perform these ongoing tasks not only augments internal IT teams with certified, expert-level support engineers 24x7x365, it streamlines your budget and frees up internal IT resources to focus on your critical initiatives that fulfill strategic business objectives. In fact, a recent industry survey found a stunning 96% of respondents indicated managed services cut their IT costs[1].

2 Healthcare organizations are prime targets for external attack vectors, such as DDoS attacks, which can trigger organization-wide outages. Most internal IT teams are ill-equipped for this eventuality.

Network attacks not only cripple your infrastructure, they are also costly data from the "IT Security Risks Survey 2017" showed a single DDoS attack can set small and medium-sized businesses back an average of $120,000[2].

With costly attacks on the rise, health IT teams need to prioritize and invest in enterprise-grade monitoring and attack mitigation across their networks. Experienced managed service providers can deploy advanced monitoring that enables the carrier's operations center to track, detect, and mitigate network attacks before they inflict damage. Should an attack occur, some providers can even deploy black hole route filtering to quarantine attack traffic and push threats back into the Internet and away from your network.

3 The cost of downtime grows exponentially as over-utilized IT resources attempt to balance troubleshooting and carrier-management workloads during a crisis situation.

Network downtime impacts your ability to provide patient care and hurts your bottom line– the 2019 ITIC Global Server Hardware, Server OS Reliability Survey found a single hour of downtime cost 98% of organizations at least $100,000[3]. In crisis situations, IT teams that maintain their own networks are forced to handle communications with multiple carriers who may not have the dedicated technical resources to quickly and efficiently resolve the outage.

To mitigate this, health IT teams need a dedicated service provider who will rapidly tackle troubleshooting and urgently oversee carrier management on the customer's behalf, no matter how many underlying carriers there are. Service providers who also monitor an organization's network can address outages before they're even aware there's an issue, minimizing or even preventing costly downtime altogether and saving them precious capital and resources.

4 Insufficiently managed networks can produce unstable Internet connections that disrupt critical in-person and virtual patient care services, such as video telemedicine sessions.

Virtual care services like telehealth and telemedicine are only successful if the underlying Internet connection is stable, reliable, and strong. Even small percentages of packet loss can disrupt streaming sessions with pixelated picture reception and unreliable voice quality.

Health IT teams need to actively optimize their Internet connections across the organization. Managed service providers can design custom networks based on a customer's specific needs that provide dedicated bandwidth, utilize private Internet networks, and guaranteed upload and download speeds, ensuring a reliable connection for real-time services such as voice over IP (VoIP) and video.

5 Poorly designed networks create lag and delay access to critical systems during peak operational hours.

In a recent industry survey, 31% of respondents said Internet speed and network outages at work were the biggest recurring technology problem[4].

Health IT teams must ensure their network is designed to handle high-capacity operations, especially during peak hours. Managed service providers can engineer a network that eliminates lag delays, giving organizations peace of mind that their cloud-based applications, platforms, operations, and workflows will be fully supported by a robust, dependable, scalable, and secure Internet infrastructure.

Citations:

[1] https://www.channelinsider.com/c/a/Commentary/Do-Managed-Services-Really-Save-Money-608662
[2] https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/
[3] https://www.randgroup.com/insights/cost-of-business-downtime/
[4] https://www.whitehatvirtual.com/what-is-the-real-cost-of-inefficient-it/