THREE COMMON NETWORK MISTAKES

Some network mistakes turn up over and over again—these mistakes cost organizations money, time, and even loyal customers. What these mistakes all have in common is that they mainly reflect a lack of planning. A network that runs smoothly and delivers top performance with minimal downtime takes thought, organization, an awareness of current technology, and a plan.

Here we present three common pitfalls. If you pay attention, you don't have to fall into them, too.

1. Non-standard construction

Because data centers are larger and more complex than ever, "seat-of-the-pants" construction doesn't really work well anymore for any network much larger than a home network. "Guesstimating" can eventually lead to all kinds of problems ranging from overheating to inadequate power to lost data.

To standardize best-practice network construction, in 2005 the Telecommunications Industry Association (TIA) published the TIA-942 standard that set requirements for network architecture, system redundancy, security, file backup, hosting, and power management, as well as a number of other procedures. TIA-942 covers not just the network itself but also supplemental services. Over half the standard covers matters such as electrical systems, HVAC, fire detection and suppression, and building construction. The standard defines four tiers of data centers, with Tier 1 being a simple server room and Tier 4 being a mission-critical data center with high security and redundancy.

TIA-942 helps to ensure consistency and produces networks with high reliability, expandability, and scalability. Because TIA-942 is intended to optimize network performance, a sure-fire way to sub-optimal network performance is to ignore the standard and creatively cut corners. Unfortunately, many installers do cut corners—either to cut costs or sometimes because they don't know any better.

When having a data center built, insist that the contractor build to TIA-942 standards. Have your data center independently audited and certified. This precaution could save you from future demons such as power disturbances, overheating, and downtime.

2. Neglecting physical security

If anyone can wander into your server room, if you have network ports in public spaces, or if your building access control is substandard, you have a huge hole in your network security. Unrestricted physical

access to a network is a much larger security threat than is generally appreciated because, if a person has physical access to a device, there is almost always a way to take control of it or to get data out of it. The fastest way into a network is not through the firewall, but through a USB port on an unattended workstation. Your most dangerous information thief may not be a faraway hacker, but one of the cleaning staff inside your building.

This is why it's important to secure your hardware—a lost laptop, an open USB port, or a simple network tap can be a conduit for quick and devastating data loss that no firewall can prevent. Today's digital printer/copiers store copies of pages, so it's essential to scrub their memories before they leave your premises when they reach the end of their service life. Think also about the paper generated and make sure that sensitive printouts are destroyed before they're discarded.

There are many ways to ensure the physical security of your network, from simple port locks to sophisticated remote monitoring systems. At minimum, doors and cabinets should be kept locked and laptop computers secured. Biometric locks add an extra layer of security. Video surveillance has become so practical and inexpensive that there's no reason not to use it in secure areas.

3. Insufficient technical support

In the middle of a busy business day, the network goes down and your support staff is either nowhere to be found or unable to deal with the problem.

Even the most perfect, well-planned network will eventually have difficulties leading to downtime. It's the nature of beast that downtime always occurs at the most critical and inconvenient times and especially over holiday weekends. That's why—if your network is vital to your operation—you need to have an experienced tech available 24/7.
Small businesses in particular often don't have enough support staff or have insufficiently trained support staff—too many small companies still rely on a staff member who's "good with computers" but has no real training. This worked to some extent in the days when computers were a lot simpler, but today's dense, high-speed network environment requires a lot more expertise.

The tech support problem can usually be worked around by contracting with a service that provides network support and is always on call. There are other advantages to working with a network services company. For instance, they can often also manage network installation and act as partners who are knowledgeable about current network technology and can make the network more efficient and cost effective.

Although a network is virtually indispensable in today's business environment, there are many ways to inadvertently sabotage it, creating unnecessary expense, frustration, and downtime. The best way to avoid the many network pitfalls is through careful planning, meticulous organization, and a willingness to ask for professional help when it's called for. This is by no means a comprehensive list. What would you consider to be the top networking mistakes? The failure to standardize? Not educating network users?

Source : https://bboxblog.wordpress.com/2013/02/05/three-common-network-mistakes/