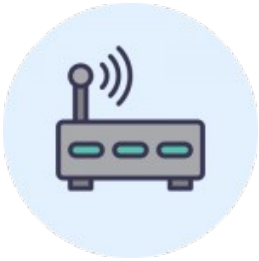
Doc 1: How to choose network hardware in a business

The backbone of your network is your hardware. All of the communications of your network flow through your routers and switches. When these items aren't communicating at levels that you require, business is affected. Very often, a negatively impacted network has financial ramifications.

If you are building a network from scratch, purchasing the network hardware that best fits your business needs will set your network infrastructure up for success. If you are considering making hardware changes to an existing network, you need to be able to prioritize your hardware upgrade needs. This prioritization process must reflect the needs of your network.

Routers



Your router is where your internal network meets the outside world. It is an integral piece of your network. All traffic destined for the outside world must travel through your routing equipment. There are many different things to consider while choosing the best router for your business.

Class Level

Will a consumer or small office router work for your business? Or do you need a more expensive product that offers more features? Cutting costs where you can is often a good idea, but is this the spot to do it? Here are some things you consider in regards to router classes:

- Maximum throughput. What speed capabilities does your business need?

- Level of support. What kind of support package does your router's manufacturer offer?

- Configurability. Consumer routers come with a lower level of configuration options than enterprise-class routers.

Security Options

Your network's security is of the highest importance. While almost all routers come with at least a basic level of security options and features, it's important to know that your router's features will meet your needs. Following are some offerings to look for.

- Content Filtering. You may want to be able to control and monitor the websites that your employees are visiting.
- Intrusion Prevention and Gateway Antivirus
- Firewall

Switches

While all traffic to and from the outside world goes through your router, all local communications are handled by network switches. They are truly the backbone of your network. It's important to know how manageable you need your switches to be, and the speeds and number of ports that you will require.

Management Features

There are two basic levels of management features for network switches: managed and unmanaged. There are a few different reasons why you might choose one or the other.
- Complexity. Unmanaged switches are simple; there is no configuration needed.
- Cost. Managed switches can be expensive, at least double the cost of an unmanaged switch.
- Configurability. If your network needs to utilize VLAN technology, you will need a managed switch.

Speeds

When shopping for switches, one oft-touted specification is link speed. There are three speed classifications to consider, and only one that you should really be shopping for most of the time.

Security Considerations

Because your wireless network naturally increases the vulnerability of your infrastructure, security must be taken extremely seriously. Here are a number of suggestions for securing your wireless network.
- Security keys. All networks with corporate-level access must be encrypted and force users to use a key to authenticate.
- Network segmentation. Your guest network should be separated from your corporate network. MAC address filtering. Administrators can use MAC address filtering on corporate networks to provide additional verification for devices to connect.

Doc 2: Different types of threats a business may receive

1 - Phishing Attacks

The biggest, most damaging and most widespread threat facing small businesses are phishing attacks. Phishing accounts for 90% of all breaches that organizations face, they've grown 65% over the last year, and they account for over $12 billion in business losses. Phishing attacks occur when an attacker pretends to be a trusted contact, and entices a user to click a malicious link, download a malicious file, or give them access to sensitive information, account details or credentials.

Phishing attacks have grown much more sophisticated in recent years, with attackers becoming more convincing in pretending to be legitimate business contacts. There has also been a rise in Business Email Compromise, which involves bad actors using phishing campagins to steal business email account passwords from high level executives, and then using these accounts to fraudulently request payments from employees.

Part of what makes phishing attacks so damaging is that they're very difficult to combat

2 - Malware Attacks

Malware is the second big threat facing small businesses. It encompasses a variety of cyber threats such as trojans and viruses. It's a varied term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.

These attacks are particularly damaging for small businesses because they can cripple devices, which requires expensive repairs or replacements to fix. They can also give attackers a back door to access data, which can put customers and employees at risk.

3 - Ransomware

Ransomware is one of the most common cyber-attacks, hitting thousands of businesses every year. They've grown more common recently, as they are one of the most lucrative forms of attacks. Ransomware involves encrypting company data so that it cannot be used or accessed, and then forcing the company to pay a ransom to unlock the data. This leaves businesses with a tough choice – to pay the ransom and potentially lose huge sums of money, or cripple their services with a loss of data.

4 - Weak Passwords

Another big threat facing small businesses is employees using weak or easily guessed passwords. Many small businesses use multiple cloud based services, that require different accounts. These services often can contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts, can cause this data to become compromised. Small businesses are often at risk from compromises that come from employees using weak passwords, due to an overall lack of awareness about the damage they can cause. An average of 19% of enterprise professionals use easily guessed passwords or share passwords across accounts according to a recent report.

5 - Insider Threats

The final major threat facing small businesses is the insider threat. An insider threat is a risk to an organization that is caused by the actions of employees, former employees, business contractors or associates. These actors can access critical data about your company, and they can case harmful effects through greed or malice, or simply through ignorance and carelessness. A 2017 Verizon report found that 25% of breaches in 2017 were caused by insider threats. This is a growing problem and can put employees and customers at risk, or cause the company financial damage.

Doc 3: How to fix the different problems

Across the board, human error is one of the biggest threats to data security. When employees do not know what the secure practices are, or do not realize the importance of following them, it places your business at risk across multiple fronts.

Solution: Educate your team about security threats and best practices.

Regularly train your employees in proper security procedures, and make the case for why it is important. Make sure they know what to do if they notice something suspicious, or if they become aware of a security lapse. Enforce best practices and demonstrate that they are important to the company.

Even with a firewall in place, viruses and malware do sometimes get through. In fact, even when security software is installed, users sometimes turn it off or change its settings if they feel like it's too intrusive.

Solution: Install anti-malware software.

Anti-malware software is designed to identify and remove anything malicious that gets on your computer. Make sure your anti-malware software isn't just running, but is also up to date and that the security settings are at the right levels.

Poor passwords are a never-ending problem for IT security. The number of users who leave their login information at a default setting ("admin") and choose passwords that are easy to guess is staggeringly high. These human errors are some of the most common root causes for security breach and data theft.

Solution: Enable two-factor authentication.

While many users seem to be immune to calls to choose stronger passwords, two-factor authentication can add an extra layer of security independent from poor passwords.

You may have significant security protocols in place for your office equipment, but what happens if that data is moved to a private computer? Corporate data hacks sometimes occur when an employee's personal computer is compromised, and the leak spreads to the rest of the organization. Similarly, employees accessing corporate networks through insecure networks can also lead to a breach.

Solution: Have a mobile and personal device policy.

There are two ways to handle this problem: Either provide employees with laptops and mobile devices and prohibit file sharing off these devices, or require employees to harden any personal devices they may use to access your corporate network. Also be sure to instruct users on how to access the Internet securely when they're working remotely.