Network Infrastructure for Business

A business' network infrastructure is the backbone on which it operates. It is tied into everything from sales, finance, operations, logistics, and more. Each of these pillars of your business have a degree of reliance on technology to keep it stable, and these pillars are directly related to the outcomes you want to achieve. For example, improving productivity, improving efficiency, increasing profits, and lowering risks are all dependant on how you manage and maintain your network infrastructure.

What businesses tend to struggle with is these pillars may become too large and complex to manage on their own. Here are some tips to help you get through the complexity of managing and maintaining your network. These tips will help you focus on managing and maintaining your business:

Identify

Create a catalogue for all your network systems and applications. This catalogue should clearly identify every physical device and software platform in your organization including its make, model, version, date of purchase, and warranty status. The items on this list should include:

- **Network hardware** – a list of servers, switches, routers, etc.
- **Network software** – a list of operating systems, email, CRM, etc.
- **Network services** – a list of IP addresses, wireless protocols, etc.
- **Network diagram** – a detailed 'blueprint' that will help administrators manage your network

Standardize

Having a standardized approach to IT will help you quickly troubleshoot common problems. IT infrastructure can quickly become a tangled web if not maintained properly. This can be costly.

You can do this by applying the following across your network:

- **Standardized hardware** – Avoid having a mix of hardware manufacturers and maintain the same manufacturer across the board. For example, you decide the pros and cons of having all Dell vs all Lenovo vs all HP computers. The same can be said for networking equipment (Cisco vs. Aruba, etc).
- **Standardized operating systems** – The operating systems and firmware for all your network hardware should be the same as well. For example, you will want to decide on whether having Windows 7 or Windows 10, Server 2013 or Server 2016 will work best for you. This can vary as you may have software in your environment that is not compatible with the latest versions.
- **Standardized applications** – You will want to ensure all your applications, such as Microsoft Office, are the same version. For example, you should have either Office 2013 or 2016 on the network, not a mix of both. This applies to business management systems, email, etc.

- **Checklists** – have a guide to ensure every time you setup a new system, whether hardware or software, you achieve the same results. This can save a lot of time and guesswork for new or untrained staff.

Protect

Make sure all your network users are made aware of common threats such as phishing, email spoofing and ransomware. Good network protection always starts with educating its users. This will save you a lot of time, money and potential grief.

After you have identified your network's current state, review it for vulnerabilities relating to both your infrastructure and processes. After you know where the gaps are, develop a plan on what needs to be done to seal them.

You can approach this:

- **Current state** – document what threats you are most susceptible to in your network's current state

- **Research** – threats are always evolving, so ensure you and your staff are aware of them and know what to do in the event of an attack

- **Plan** – put together an action plan to address any vulnerabilities you have identified

- **Implement** – put your protection plan into action and frequently test it

- **Attack yourself** – frequent penetration tests and vulnerability scans will help you benchmark your readiness for an attack. As threats are constantly evolving, you will need to know how vulnerable your network is to them and how to protect yourself.

- **Plan for the worst** – a good disaster recovery plan will help you minimize any monetary impact to your business caused by a disaster event such as theft, flood, fire, ransomware and more.

Improve

Once you have identified, standardized and protected your network infrastructure, make a concentrated effort to continuously improve it. As your network is all encompassing, you will need to focus on the people and processes it effects and not just the technology.

Here are a few tips to get you started:

- **Research** – Know your industry trends to identify what systems need to be in place for your business to remain competitive.

- **Train** - Keep adding new skillsets to your operation related to IT such as software development and other technical skills. The more IT related skills you and your staff have, the more you will be able to improve both technical and business operations.

- **IT Roadmap** – A good IT Roadmap is an integral part of any business and will serve as a guide on how technology will help your overall strategy. This will also provide you with financial and logistical information on what is required to continuously improve your network infrastructure.

These are just a few high-level strategies to get you started. A strong network infrastructure is critical to creating a stable business environment. Having a stable environment is critical to a businesses bottom line.

If you have any questions, contact AlphaKOR to discuss how you can lower costs, lower risks, improve productivity and increase revenue for your business through a strong network infrastructure.

Frank Abbruzzese
President
AlphaKOR Group