Small Business Network Security Recommendations

Small business network security importance cannot be understated. This is as true in the Chicago metro area as it is throughout the rest of the nation. The fact is that an unsettling majority of small businesses have networks that are improperly secured – or worse, not secured at all. It can be easy for business owners to treat network security as an amorphous blob that they simply do not have the time to worry about. But this is a dangerous mentality that exposes the business to unnecessary risk.

Rapid Growth – A Network Security Nightmare?

Small business owners know that, while a positive sign, rapid growth presents problems. Adding headcount fast or expanding to additional locations puts pressure on nearly every facet of a business. Unfortunately, this all too often leads to businesses neglecting to put the proper network security protocols in place to support their growth successfully. In the past, the technology available made these scenarios a true nightmare for SMBs. It was often prohibitively expensive, functionally limited and inordinately difficult to manage.

Thankfully, the small business network security landscape has improved greatly since then. Modern technologies like Cisco's Meraki line of network security appliances solve the classic problems by being surprisingly affordable, feature rich and easily managed. By combining this with solid network security principles, small businesses can protect themselves in the short term and set themselves up for long-term success.

Three Network Security Recommendations for Small Businesses

1. **Properly configured firewall(s):** Every business location should have a properly configured firewall. It is not enough to just have a firewall in place without first verifying that it is set up to effectively protect the business. It is better to be restrictive by blocking all traffic by default and only specifically allowing traffic into the network as necessary. Examples of necessary traffic could include web browsing, email and VoIP phone systems.

2. **Granular employee permissions:** Every employee should have granularly assigned permissions on the network. These may be set up and grouped by department or job description, or they may be set up on an individual basis. Much like with firewalls, it is also better to be restrictive with these permissions by blocking access to network resources by default and only specifically allowing access to them as necessary. Examples of necessary resources could include specific software, servers or shared files that are needed by the employee to perform their core job functions.
3. **Thorough documentation:** Every network security policy and procedure should be thoroughly documented, redundantly backed up and easily accessible to the relevant parties. The old IT proverb is that if files do not exist in at least three different places, they do not exist at all. Examples of backup locations could include a local file server or NAS device, cloud storage and even a paper file.

Cisco Meraki Makes Network Security a Breeze

The above three network security recommendations represent the bare minimum for small businesses – the "low-hanging fruit," so to speak. But to create a strong long-term integrated IT strategy, small businesses need more. This is where Cisco Meraki comes into play. Their network security appliances augment these basic practices with meaningful reporting and analytics, mobile device access control, antivirus scanning, content filtering and multifactor authentication. In effect, they give small businesses every enterprise-grade tool they need to secure their networks with industry standard best practices. At the same time, they do so with the ease of use that would usually only be found in consumer-grade equipment.

Ready to protect your small business with enterprise-grade network security? Click here to learn more about how Cisco Meraki can help you.