Small and Medium Business Cyber Secuirty Checklist

□ Access Control

Physical security of your company's data starts with knowing who can and should access it. Employees tend to handle different types of data, depending on which department they work in, if their role is customer facing, etc. Knowing who has access to what workstations is important in logging information and tracing problems to their source. It's also a key element of making sure that your data is safe from disgruntled or former employees.

□ Data Organization

Having your data safe is one thing; having it in the right place in your network is another. Data needs to be organized to keep permissions organized. If all your company's data finds its way to a folder on a hard drive, the permissions to that folder cannot be used as an effective tool for protecting it, especially from a malicious user or a successful phishing campaign.

□ Network Protection

Network protection is an umbrella term for keeping your network safe, but some core principles go a long way to securing your network. 1) Use password management solutions to ensure strong password authentication where (or if) you need it. 2) Implement multi-factor authentication anywhere it's possible to. 3) Use modern firewalls and antivirus scanning to ensure that your network is not vulnerable in real-time, as well as respond to threats as they happen.4) Employ disk encryption as a last line of defense against data exfiltration.

□ Software Security

Up-to-date software is more secure than older software. When vulnerabilities are published and patched by software companies, it often means that threat actors have already been using the vulnerability to attack and gain access to workstations and infrastructure that use that software. The only way to make sure that you aren't vulnerable to these attacks is to patch software when it's available.

□Usable Backups

Having a backup solution is necessary for withstanding natural disasters, employee error and accidental deletion, hardware failures, etc., but just making a backup doesn't mean that the job is finished. Having timely backups (and for a lot of companies, that means daily backups) is necessary, but your team also needs to inspect and test the backups to make sure that they work. Plenty of ransomware attacks expose companies who made their backups, but don't have a plan for restoring from the backups once they're made.

□Uptime Maximization

Maximizing your uptime means planning for the unplanned. A solution that gets you running immediately when things go sideways can keep your bottom line from being affected. While having redundant infrastructure keeps your uptime and availability high, implementing a redundant system has to be framed as a security issue, since having a second set of infrastructure or software for emergency use means that all of your security concerns are doubled.

□ Write Good, Clear Policy

Once you've got a secure and usable network, you can help keep it secure by thinking about how the network should be used by employees. You might not, for instance, want to have employees connect to your network with their personal mobile devices, since it makes your attack surface larger. Being clear about this can help you avoid attacks originating from unexpected threats and helps your security team focus on what's most important to your business.

□Employee Knowledge

Having all of these policies and practices in place has to go hand in hand with employee training. Let employees from all of your departments know how to be a security asset for your company, and make sure that they understand the policies they're expected to abide by. Periodic training and assessment on your company's security regime is the only way to trust that your company is securing its data and following best practices.