# 10 Steps for Ensuring Cyber Security for Small Business

PATRICIA LOTICH

It is difficult to turn on the news and not hear a report about a cybercrime stealing valuable customer and business data. It doesn't seem that long ago when working off-site or at home required loading information onto a floppy drive and transporting work projects from one computer to another.

Fast forward to today and most businesses operate in the cloud and VPN networks. Employees have become accustomed to the freedom of virtual work and enjoy the ease of firing up the laptop or smartphone to conduct business. This new phenomenon makes work seamless and provides organizations with the advantage of accomplishing tasks even while employees are away from the office.

However, every business has sensitive data that needs to be protected. Your employees are the first line of protection and need to be aware of their responsibility in keeping company data safe and secure. According to the Cyber Security Breaches Survey 2018, 43% of businesses were a victim of a cybersecurity breach in the last 12 months.

It can be difficult keeping that data safe when it is estimated that 25% of employees use the same password for all of their accounts and 81% of those don't password-protect their smartphones or computers.

A survey by CoalFire suggests that 47% of employees do not use a password on smartphones or mobile devices that access sensitive company computer files. The survey also reports that 84% of employees surveyed say they use the same device for work and personal use, and that 50% of the companies these employees represent don't have a policy in place for mobile device usage.

## The findings of this survey are alarming:

- 84% of employees use the same devices for work and personal use.
- 47% state that they don't use passcodes on their cell phones.
- 36% report that they reuse the same password.
- 51% reported that their company did not have the capability of wiping out data from devices that were lost or stolen.
- 24% reported using a password management system.
- 60% are writing passwords on paper, 11% save passwords on an encrypted document on computer and 7% report having passwords saved on a document on their desktop.
- 49% of IT departments do no communication or training on cyber security.

These statistics are alarming, and every business owner should pay attention to the potential risk for a security breach of sensitive company data.

# How to Protect A Small Business from Cyber Security Threats?

## 1. Write Cyber Security Policy

The first step is determining what is and what isn't appropriate for your particular organization. Gather key leadership and your IT representative and write policies and procedures that protect your organization. This policy should include when it is appropriate to use personal mobile devices, password protection protocols, and steps that need to be taken in the event of a lost or stolen device.

## 2. Require Strong Passwords

Most of us agree that using strong passwords is a major pain. We like to work from memory and strong passwords eliminate that option. However, we have learned that using the same password, or easy to remember passwords are a hacker's dream.

Using unsafe passwords is like sleeping with your doors unlocked. You just never know who will test that door and try to get in. Pick a password manager for your company and require employees to use safe password practices and require employees to change passwords every three months. Lastpass and Google both provide password storage and protection. Do some research and pick one that makes the most sense for your organization.

Then, communicate expectations to employees, train them on how to use password storage software, and then hold them accountable for following company guidelines.

## 3. Train Employees on Cyber Security

Employees come to work and want to do a good job and most employees are not thinking about cybersecurity. Spend some time training employees about the unique risks of cybersecurity and how it can result in significant liability and harm to your business.

The goal of the training is to communicate the employee's responsibility for helping the organization protect itself. This training should include sharing cyber policies, best practices for password creation, and practical ways to store password information.

## 4. Secure Wi-Fi Networks

Protect your Wi-Fi by hiding and encrypting the network name and use a strong password on the router. If necessary, provide a separate Wi-Fi access for customers that does not have access to your business network.

## 5. Limit Data Access

Be aware of which employees have access to data. Never allow only one person to have access and limit access to a need-to-have. For example, the accounting clerk may need

access to credit card processing data but may not need access to employee personal data. Know who has access and maintain strong controls over that access.

## 6. Perform Regular Data Backups

Most businesses use a level of cloud storage. And while these storage systems are safe, they can have failures. Make it a policy to backup all computers and files on a regular basis and keep that data locked.

Store copies of that data either locally or in the cloud. For instance, someone should have responsibility to back up the network at a certain time of day on a particular day of the week.

## 7. Use Security Software

Hackers are constantly looking for cracks in your system. Use security software that helps to protect your business from viruses or malware. Set software to run an update regularly and to alert you to any possible threats.

## 8. Update Software

A big mistake, organizations make is not updating software when updates are available. These updates are important because it blocks vulnerabilities from outdated software.

## 9. Conduct an Audit of Mobile Devices

Conduct an audit for what personal devices employees are using to conduct business and review password protection practices. Keep records of devices that are in use and require employees to update the information when new devices are used.

## 10. Hold Employees Accountable

Your data is only as safe as employees work to protect it. Incorporate data security practices into a performance management process to enable the organization to influence positive cybersecurity practices. Most employees have a vested interest in the organization they work for and care about its success.

Taking the time to plan and educate employees on cybersecurity issues can allow your organization to partner with employees in safeguarding critical business data.