Practical Cybersecurity Tech
for Small Business

Tim Foley
CISSP, CISM, CRISC, CCSK

Tim Foley joined Dataprise in 2011 and currently serves as the Director of Information Security. He is a proven thought leader who brings with him over 15 years of industry experience, with a focus on Information Security and Program Development. Dataprise supports clients in Florida and along the East Coast of the US.

As a small business owner, you've spent years building your business. You've invested your time and your tears building a brand that you can be proud of. While your business may be considered small, in the eyes of a cyber-attacker, it may not be as small as it seems.

When asked about cybersecurity and putting safeguards in place, the overwhelming majority of Small and Medium Business (SMB) owners acknowledge that security is something they should be concerned with, but very few are actively taking preventative security measures. Many SMB owners I talk to simply believe that the likelihood of an attack on their business isn't very high.

Historically, small business owners were far more concerned with understanding how the internet could work for them and how they could use it to expand their business outside the local area. The idea of investing in preventative security was a distant afterthought.

But an attack on an SMB is not as unlikely as it seems. In fact, according to Symantec, nearly half of all cyberattacks are committed against small businesses. In many ways, an SMB makes for a more ideal target for an attacker. Why?

Most Cyberattacks aren't Sophisticated

The vast majority of cyberattacks aren't carried about by well-organized groups of hackers. Attackers are typically individuals simply looking to exploit an existing vulnerability or weakness.

Your Information is Valuable

Don't be fooled, regardless of size, every business has data that's important and that data makes them a target. In today's security climate, data has become the new currency, and no matter the size of your business, that data has value.

You're an Easier Target

Many large enterprises are increasing their security budgets and stepping up their level of protection. This is making them increasingly difficult to breach. An SMB on the other hand, does not typically have the technologies, budget, or in-house expertise solely dedicated to security.

Your Business Relies on Being Online

Whether it be for online marketing, social media promotion, running your e-commerce store, or simply having a constant online presence, your business is dependent on being connected at all times. Downtime for your business is detrimental.

What protects your business one week, may not work the next.

You're Not Staying Up-to-Date

It's important to know that information security is not a destination, but an evolution. Simply implementing a firewall or an anti-virus will not deter an attacker for long. As security technologies become more sophisticated, so do attackers.

AMERICA'S SBDC FLORIDA

→ FloridaSBDC.org

floridasbdc.org/cybersecurity

Helping Businesses Grow & Succeed

So what steps can a small business take to make its systems and digital infrastructure more secure?

Here are some practical steps that you can take to help protect you and your business. These basics of security should be non-negotiable for every SMB.

Awareness and Assessment

It's important to realize that you are a target. Every SMB owner should assess what (data) information is potentially valuable to an attacker. Knowing what information is at risk can help you understand who may want to access that information and how you can better protect it.

Do the Little Things

As mentioned, most attacks aren't sophisticated in nature. Instituting even very basic measures of security will help deter the vast majority of attacks. As your business grows, it becomes easier to add additional layers of security for more advanced protection once the simple foundation is laid.

Get Help

The information security landscape is complicated and constantly changing. As a small business owner, your primary focus should be on your core business. Therefore, outsourcing your security to a managed security service provider (MSSP) may be the best option for you.

Get the *Right* Help

Not all MSSPs are created equal. A good MSSP should be available when you are, and should complement, not complicate, your business. It is important for an MSSP to know your business and how it operates so that they can effectively protect the data that is most important to you.

Too often when talking with SMB owners, I hear that information security is an IT problem. This is something I strongly disagree with. I think information security is more than an IT problem, it is a business resilience problem.

A resilient business understands that they must be prepared against attacks, both known and unknown. Whether it be the latest cyberattack, or a new competitor moving in across the street. A resilient business is one that hopes for the best, but prepares for the worst. And because of this, a resilient business is ultimately one that is able to stand out amongst its competitors and is better able to service their customers.

Small Business Cyber Self-Assessment Checklist:

☐ **Password Protection**
- Implement a strong password policy for corporate resources
- Reset passwords every 90 days, at least
- Do Not use Shared Logins to access corporate information/ machines
- Use multi-factor authentication, where possible

☐ **Endpoint Protection**
- Ensure licensed and up to date Anti-Virus on every machine
- Patch the Operating System on a monthly basis with critical patches
- Keep Line of Business Software applications up-to-date

☐ **Perimeter Protection**
- Have a business grade Firewall (Not rented or shared)
- Secure your Corporate wireless network with a strong password (WPA2)
- Have a separate network for Guests, especially wireless

☐ **End User Protection**
- Provide User Security Awareness training to employees at least annually
- Ensure that users have only the access (building access, network access, etc) they require to perform their job function, and not more

☐ **Backups**
- Keep daily backups of all critical data
- Store full backups at an offsite location, once per month

☐ **General Best Practices**
- Keep an inventory of all corporate Assets (laptops, tablets, mobile phones, etc)
- Separate Personal and Business accounts wherever possible (ie. Social media, etc)

Good security is within reach of any organization. Use this checklist as a basic guide, and if you require assistance with any of the above, find a trustworthy partner organization that you can trust to help you with the implementation.