SMALL BUSINESS CYBERSECURITY BASICS

simpleplanit

CONTENTS

INTRODUCTION

There are a number of things that you should do to protect yourself, your business and your clients. We have broken these things down into two categories: Basic and Advanced. The Basics are things that every business should have in place and are simply best practices. The Advanced, are services that businesses that have more than 25 employees, or are in regulated industries, should strongly consider putting in place. While all of these services would benefit smaller organizations as well, the cost may not be justifiable.

This guide is designed for small business owners and leaders. This is not a "Do-It-Yourself" guide, but rather a guide to outline what you should have in place and to give you some things to consider as you look to hire the right security expert when the time comes. This will also help you to prioritize things as you look to stay within your annual security budget.

As for budget, here's a quick guideline that you can use to establish your security budget. It's suggested that small businesses should spend around 7 percent of their overall revenue on IT systems and services. You then take a percentage of this amount and allocate it to security services. We've seen percentages range from 5 percent all the way up to 20 percent. It really depends on the nature of your business and your overall risk tolerance. The lower the risk tolerance, the higher the cost.

DON'T DO IT YOURSELF

If you are not a security expert, then find someone who can help. The risk of mismanaging your security solution is far too great and the consequences are far too high. We encourage you to partner with an individual consultant or security company. Here are some key takeaways when looking for help:

1. It is better to look for someone who is not affiliated with any specific vendor (i.e. a security professional that represents a hardware/software company). You don't want someone who is solely focused on selling you a product.
2. Look for a consultant or company that specializes in security.
3. Not every IT person is a security expert, so make sure they have some security credentials. You can find the classification of every top security credential here: https://adobe.ly/34dHV7e

   (***Quick Tip*** – Follow the Blue line to see if they're a security Expert or a Novice)

NOT EVERY BUSINESS IS THE SAME

The level of risk tolerance and acceptance will vary from business to business. The amount of money you invest in security is directly related to the level of risk you're willing to accept, as well as the likelihood of a breach. So, before you decide on the budget that will determine how you're going to secure your business, you should consider the following:

1. What are the critical apps or assets that if breached, could cause catastrophic damages to your business?
2. How comfortable is the business with downtime, revenue loss and data loss?
3. Who has access to business-critical assets, apps, and information, and what will happen if they get hacked? What do your vendors have access to?
4. Does anyone have access to business apps or data from home or remotely?
5. Are there regulations the business must comply with such as PCI, HIPAA, NIST or GDPR?

It's also important to understand that you cannot go from 0% to 100% overnight. It's a gradual process, so start by addressing the biggest risks to your business first.

With all that said, let's begin!

BASIC SECURITY

Regardless of your company's size or the industry that you're in, here is everything that a business should have in place to protect themselves. Now depending on your business, some of these items may be more important than others, but we have not listed them in any specific order.

1. **Data Backups –** Backups are extremely important and are a must-have. This is especially important in the event a hacker uses ransomware to lock you out of your files. Make sure the backups are located off-site and not connected to your network. This way if your business is hacked, the hackers won't have access to them. These backups should also be password protected. You should also consider how much data you can afford to lose. Having more frequent backups reduces the amount of potential data lost, but that will significantly impact your cost.

2. **Disaster Recovery/Business Continuity (DR/BC) Plans –** Small businesses can't afford to have downtime. Studies show that even one minute of downtime can cost between $137 and $427. DR/BC plans help businesses quickly failover to their backup systems and data in case of an emergency and reduce downtime. Disaster recovery management involves keeping a copy of all critical systems and data so that you can easily move over to using them to quickly resume operations after a disaster strikes.

3. **Security Awareness Training –** Educate your employees about cyber threats! This must be done on a continuous basis. If employees are not constantly trained, then the risk of them being a victim of an attack increases dramatically. Develop a culture within your organization where they're looking out for suspicious emails and practicing how to avoid becoming a target.

4. **Multi-Factor Authentication –** Enable Multi-factor authentication wherever possible. This means that you will need to enter a code that is sent to your mobile device whenever you log into apps like your online accounting. This protection adds another layer of security in the event your password is stolen. A lot of applications have this built into them, but there are also 3rd party programs that you can incorporate.

5. **Computer Access Control –** Lock down your computers to ensure employees only have permissions necessary for them to do their job. For example, they should not have permission to install applications or admin privileges. Also verify that only the applications that are absolutely necessary are installed.

6. **Firewall (Commercial Grade) –** Obtain a commercial grade firewall and have it configured properly. This will limit who can access your business from the outside world and will help control how data exits your business.

7. **Inventory and Patch Management –** This will allow you to know what is installed and ensures all apps, computers, and POS systems are updated and patched to the latest versions. Unpatched computers and apps are open doors for hackers…so do your best to make sure they are always up to date.

8. **Password Policies –** Establish a policy that requires complex passwords or phrases. Most security experts will tell you that your password should be at least 12 characters long. We believe that number should be 15, but the longer the password the better. Also make sure employees do not access computers with Admin credentials and employees should never share passwords.

******BONUS*** Here is a Password Policy Template that you can use for your business***

9. **Termination Policies –** Make sure terminated employee's credentials are immediately deactivated. You must ensure that they don't have access to business systems and emails anymore.

10. **Health Check and Vulnerability Scanning –** This should be performed once a quarter and will basically check for any issues with applications or computers on the network that may be open doors for hackers. Hackers are also using vulnerability scanning on your network to try to get in, so you need to be ahead of them.

11. **Anti-Virus Software –** Install and use this software on all computing devices. Don't simply rely on the free antivirus that comes loaded on your machine when you purchase it. This should go without saying, but please make sure that it stays up to date. Outdated anti-virus software won't do you any good.

12**. Vendor Compliance –** If you need to comply with regulations such as PCI, then process your credit card transactions using a vendor that complies with this regulation. If you're regulated by HIPAA, make sure that you have your BAA's in place that require your vendors to have adequate safeguards in place to protect your data.

13. **Website Whitelisting –** Because visiting infected websites is often a main vector of attack for hackers, it makes sense to whitelist the websites your business uses for its operations. Whitelisting involves only allowing employees access to websites that have been added to the list of approved sites, all other sites are blocked.

14. **Virtual private network (VPN) –** This is used when accessing office files remotely. A VPN will ensure that if anyone hijacks your connection, they will not be able to see or access the data you are sending over the network (i.e. the password you are using to log in to different apps etc).

ADVANCED SECURITY

The advance security section is made up of ongoing monitoring services. These things are often referred to as “Managed Security Services”. These items will typically be offered as a monthly service and will monitor your network for security issues and hacking attempts. Here are some of the services that you may want to consider including as part of your cybersecurity solution:

1. **Managed Security Information and Event Management System (SIEM) –** Almost every application and device will produce a log that tells you everything that it has done. A SIEM aggregates all of that data so that a security professional is able to see everything that is going on within your environment (both cloud and on premise). When monitored in real-time, this solution will allow you to respond to security incidents in a matter of minutes and seconds. The faster you're able to respond to a security incident, the better chance you have of minimizing the possible damage and impact.

2. **Penetration Testing –** After you have the basics covered, you may want to hire a company that will attempt to hack your organization. This will give you an idea of how well you are protected against cyberattacks and what else can be done to better protect your business.

3. **Monthly Email Phishing Testing with Reporting –** Email continues to be the highest entry point into businesses for cybercriminals. Routine simulated phishing has been proven to minimize the risk of end-users falling victim to these malicious types of attacks.

4. **Dark Web Scanning –** Find a service that does deep dark web scans and not just scanning of the main databases. This service should monitor multiple dark web channels looking for any information about your business. This will allow you to change any compromised credentials in your environment before they can be used to launch an attack against you.

5. **Data Loss Protection (DLP) Software –** DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

WHAT IF THINGS DON'T GO AS PLANNED?

An incident response plan is basically a plan for what to do if your business gets hacked. How you respond to each incident depends on what has happened. For example, if all of your computers were locked by a hacker demanding payment to unlock them, you may take different actions if you have a clean backup and can restore everything versus not having a backup at all. Or what if your customers' credit card information was stolen? Then an incident response plan would guide you to who you need to notify and what actions you need to take in order to put an end to the breach and be compliant. To expedite your response efforts, you may find it valuable to have simple flowcharts pre-prepared and contact lists of people and organizations that you're required to contact in the event of a breach.

It's important to work through these suggestions with whomever is responsible for securing your network. Make sure that your incident response plan is easy to read and is reviewed/rehearsed at least once a year...you never know when you may need to use it.