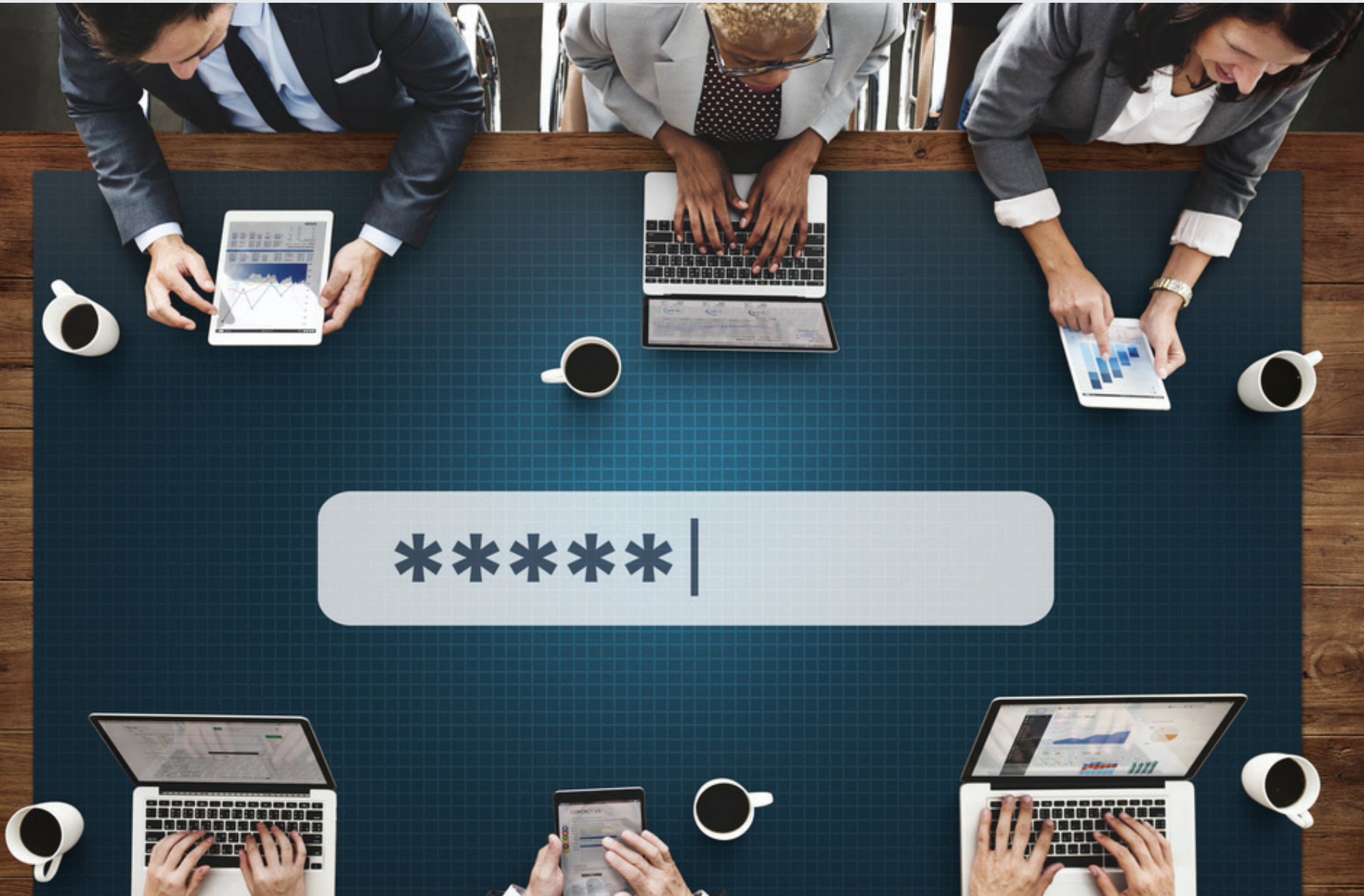




# THE ULTIMATE CYBERSECURITY GUIDE

\*\*\*\*\* |



## INTRODUCTION

Even though large enterprises usually dominate the cybersecurity headlines, small and medium sized businesses (SMBs) are often at much greater risk of an attack. Most SMBs don't take a systematic approach to security, relying on the false assumption that they don't have valuable information to steal and can fly under the radar. They often don't have the resources or the time required to implement a sufficient strategy to thwart would-be hackers.

Hackers know this, making SMBs an easy mark!

**Most SMBs don't take a systematic approach to security making them an easy mark for hackers**

Hackers use several tactics to gain access to a network; exploiting security gaps in software, orchestrating brute force attacks (trial and error techniques to guess passwords), or engaging in social engineering (tricking employees into providing access to corporate networks).

We have long passed the days of bogus emails with horrible grammar and rampant misspellings. Hackers have graduated to very complex attacks that can get the best of some of the most


vigilant organizations. Small businesses need to be prepared for all types of assaults.

According to a 2016 Ponemon study, half of SMB's reported having a data breach that involved customer or employee information in the 12 month period ending June 2016. The average cost of these breaches is much higher than most SMBs can afford and remain in business. Victimized companies lost an average of \$879,582 due to damage or theft of IT assets as well as incurred \$955,429 in extra costs due to disruption of normal operations.

**Half of SMBs in the U.S. reported having a data breach in the 12 month period ending June 2016**

## COMMON MISTAKES

Fending off these threats is no easy task and SMB's are committing many of the same errors. Some of the most common include:

- 
1. Not educating employees about good security practice and co-opting employees into security responsibilities.
  2. Not having a backup or disaster recovery process.
  3. Poor or no access control of physical hardware.
  4. Bad password policies.
  5. Not enforcing security policies.

Perhaps the biggest error SMB's make, and one that could help businesses avoid many of the other mistakes on the list, is the lack of a comprehensive security plan.

## THE ULTIMATE CYBERSECURITY CHECKLIST

To help SMBs avoid some of these blunders, we have created a checklist to help guide you in creating and implementing a comprehensive cybersecurity plan.

## 1) COLLECT DATA AND ESTABLISH A BASELINE

The first step to creating a robust plan is to inventory your technology assets and assess your current policies.

### Create a device inventory



Have you created a list that documents all company computers and devices? In order to create a comprehensive plan, you must be able to account for all devices that have access to company data. Labeling each device and creating a naming scheme are good tips for generating a device inventory. Are employee-owned devices such as smartphones or tablets accessing the corporate network? If so, note these devices in your inventory.

### Create a software inventory

Have you documented software versions and security level patches for each device? Record the type and version of operating systems and application software running on each device. Verify whether each device has security software such as firewall, anti-malware, and anti-virus software installed. Check mobile devices for device management software that supports encryption and remote wipe. Also, record what security patches have been installed.

### Review acceptable use policies



Do you have an acceptable use policy documented and is it sufficient? You need to have rules around what employees can and cannot do on company devices and networks, including Internet usage, email usage, software installation policies, downloading attachments and use of personal devices to access company data.

### Review password policies



Do you have a password policy documented and is it sufficient? You need to have rules governing password strength such as

the number of characters, uppercase, lowercase, duration, etc. And don't forget about requiring passwords to access all those mobile devices!

### Review data access policies

Do you have a data access policy documented and is it sufficient? You need to define the responsibilities and roles of people who have access to company data, as well as how you plan to enable contractors or partners to access company files.

### Backup and Disaster Recovery



Do you have a way to back up data regularly? As a minimum, you should have an on-site solution for rapid recovery and an off-site solution in case of a catastrophic event. Check your backup power and fire suppression systems as well. Determine how quickly you need to be working if a disaster occurs and check those Recovery Time Objectives against your current backup/restore capability. Be sure to look for a solution that meets your exact needs - they are not all the same.

### Secure access to physical structure

Do you have a way to control access to physical structures? You should limit access to physical structures such as server rooms or data centers to only authorized employees.

### Review Wi-Fi network policy

Last but not least! Is your Wi-Fi secure and is it hidden from the outside world?



## 2) DOCUMENT A PLAN

Now that you have a better understanding of your assets and some of your security vulnerabilities, you need to draft a comprehensive security plan.

Try to draft policies that are not overreaching or difficult to understand, and reflect current practices within your firm. The key is to create policies that makes employee compliance easy and everyone in the organization can support. If you create policies that are overly complex or disrupt current business processes, the likelihood that employees will comply is low.

### Draft an acceptable use policy



Keep it simple and to the point so there is no confusion of what is acceptable and what is not. Also, make sure that you have a way to enforce the policy. Having employees sign compliance agreements is a common tactic.

An acceptable use document is also a good way to protect yourself from liability in the event employees use company equipment for illegal activity. If you decide to allow employees to connect their personal devices to your network, ensure that you have appropriate BYOD security infrastructure in place. Also, consider employees' usage of social media. Are they sharing information that could lead to a data breach if it falls into the wrong hands?

### Document a password policy



Requiring employees to use strong passwords is critically important. "Password123" or "admin" should not be an acceptable password. A Verizon study found that 63% of data breaches are due to weak, stolen or default passwords. You may want to consider including two-factor authentication as part of your policy. This typically involves sending an SMS to a mobile device with a onetime pin that can be used as a second authenticator

in addition to a password. Also, consider implementing password management applications to help employees keep track of complex unique passwords.

### Draft a data access policy



Establishing clear rules regarding how to handle data is critical in modern business information systems, as data is now located in more diverse places than ever before.. Think about who needs access to what data to fulfill their role and limit access to only that data. Sensitive information should only be available to employees who must have access to it to do their job.

### Create, Test and Revise Your Plan

Every business has specialized disaster recovery and business continuity requirements. Cookie-cutter solutions are rare in business continuity planning.

You need to determine what data requires backups, how many different versions of that data you need to retain, how long you must retain it, and the speed at which you need to recover in an emergency. Make sure you have backup data stored off-site in encrypted form.

Once the backup system is in place, you need to test it regularly. A backup that's not been tested is almost as bad as no backup at all. You should also test your organization's entire response to an emergency. Practice how your employees will continue business operations if they cannot get to the office.

Finally, take the lessons that you learned from your tests and apply them to your plan. Do this on an annual basis, and you'll have the makings of an excellent business continuity planning cycle.

### Create an education plan

One of the most important pieces of any security plan is to create a security-minded culture in your organization. Employees that take responsibility for the protection of company data will be much more vigilant. This begins with education and communication. Scheduling training sessions to teach employees best practices should be a central part of your blueprint.

Among other things, these sessions should cover: how to create strong passwords, how to identify questionable emails, and how to avoid troublesome websites. You should discuss popular social engineering tactics such as:

- Phishing - where a cybercriminal impersonates an authority
- Baiting - where victims are enticed to download malicious software in exchange for something of value
- Tailgating - where attackers will ask employees to hold a security door for them or request to quickly borrow their laptop

Creating and administering cybersecurity quizzes can also be a good tool for measuring your employees understanding of threats and best practices.

### Document a response plan

Should you have a data breach do you know what to do? How will you secure your network and protect data from further damage? How will you inform customers if their personal information is compromised? When attacks occur, a quick, organized response can reduce the extent and severity of data loss.

## 3) IMPLEMENTATION

### Kickoff meeting

The best way to start the implementation of your cybersecurity strategy is with a kickoff meeting. In this meeting, you can make security policies available to employees and you can direct employees to sign off on acceptable use policies.

### Assign responsibilities



To ensure that your company complies with stated policies and procedures, certain responsibilities need to be assigned to specific individuals. Someone needs to be accountable for keeping the firm up to date on cybersecurity trends, threats and security patches. You may want to assign two people to this job to create some redundancy. To ensure that your employees comply with set policies, spot checks should be executed and assigning an individual to randomly check device for compliance is a prudent compliance measure.

### Software installation and configuration



Each endpoint should be loaded with a firewall, malware and antivirus software. These applications should be set to auto update to ensure new security patches and enhancement are automatically implemented. If you have a BYOD policy, make sure you have appropriated BYOD security software implemented on employee devices. Also, ensure settings on Wi-Fi routers are set so the network name is not broadcast to the outside world.

### Plan and run employee education seminars



These meetings don't need to be long but employees must understand the importance of taking responsibility for safeguarding company data.

## 4) REPEAT



IT changes rapidly and the security landscape changes especially fast. At least once a year, you should review your IT security plans, policies and procedures, and incorporate new technologies, devices and security threats.

## CONCLUSION

Understanding the steps required to make your data secure is a must for SMBs. However, the time required and the nuanced expertise needed to create a detailed plan and execute it is a challenge for almost every organization. Ntiva has the expertise and the resources to help you come up with the right strategy for your business.

### Assessment

We can help you plan, execute and monitor your entire cybersecurity strategy. We start by performing a complete risk assessment to identify security threats, measure your level of preparedness and recommend and prioritize investments.

### Implementation



Once a plan is in place, we can implement appropriate cybersecurity technologies such as antispam, antivirus and antimalware software; email encryption, archiving and compliance; back up systems; and patching..

The next step is to create a backup and recovery strategy, deploying automatic backup software that can manage the backup of end-points as well copying your entire infrastructure to a secure location.

Have mobile devices? We can implement MDM software to ensure mobile devices are secure and BYOD policies are safely enabled.

### About Ntiva

Ntiva is a trusted Managed IT and Cloud services provider that offers IT services and support to businesses of all types, building and maintaining infrastructure, securing networks, and providing strategic technology expertise. Our team of world-class talent genuinely cares about the relationships we build and understands that response and precision are fundamental keys to a successful partnership. Ntiva's ultimate objective is to help our clients leverage their technology investments to improve their overall business performance.

### Ongoing Monitoring and Management



Ntiva tailors plans to provide continuous and proactive monitoring and management of your entire IT infrastructure, preventing threats from occurring before they even happen and/or mitigating attacks before they do serious damage.

For more information on how Ntiva can help you with your cybersecurity strategy from a one-time consultation to regular recurring reviews, send us an email at [info@ntiva.com](mailto:info@ntiva.com) or call 888-996-8482.