TitanFile

# 5 Simple Ways Small and Medium Businesses can Improve Online Security

# Introduction

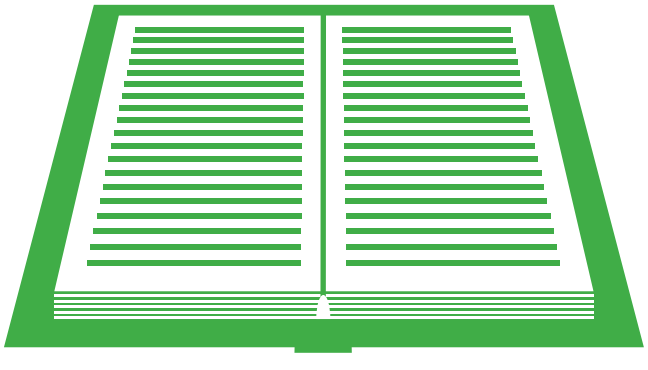
Cyber threats. Data breaches. Hackers. Police investigations. Sounds a little like the plot line of the latest Hollywood thriller, doesn't it? Unfortunately it's a scenario that's becoming all too familiar to small and medium business (SMB) owners.

A quick Internet search of 'security breach' will turn up thousands of results. Chances are the top returns are going to be about major companies who have fallen victim to an online attack. Zappos. Wyndham Hotels. Sony. Large health care organizations aren't immune either. It's not often that SMBs are mentioned, an interesting omission considering the very real threat of cyber attacks on that demographic.

## Why does it matter?

Too many SMBs don't take the necessary precautions to protect their business – leaving their customers vulnerable. While large businesses can bounce back from a breach, that's not always the case with their smaller counterparts. Large settlements, high forensic analysis costs and untold damage to a business's reputation can take a very real toll. There are many reasons SMBs shirk their online security duties. Perhaps there's a lack of managerial buy-in. At others, time or money could be an issue – maybe it's both. Some businesses naively think they're already doing everything they can to protect themselves.

Whatever the reason for not being proactive with online security, now is the time to make some changes. Set your business apart from its competition by being an organization that's focused on protecting sensitive information. Become a champion to your customers by letting them know that you value their business enough to take every step necessary to safeguard their private details. Having a vested interest in security means you have a real interest in providing the best service to your customers – and there are no losers when it comes to reputations built on consumer satisfaction.



## What is this ebook going to offer you?

This ebook will help get you on the right track to security success – and provide you with tips to stay there. We've outlined five simple steps that can help protect both your business and customers from being the next victims of digital crime.

Breaches can occur at any business that stores data in an electronic form. That includes retail stores who take customer contact information for returns, to courier companies that are logging addresses and credit card numbers for delivery. With security breaches on the rise, it's time to get active in protecting your business and your customers. Read on for five ways your business can improve its security procedures. At the end of the ebook, you'll find a checklist of the steps you can take to improve the security at your SMB.

# Chapter 1: Understand the Risks

Every day we engage in risky behavior. Take driving on a busy highway, for instance. Cars are moving at high speeds, and while you might be certain you're being safe, you can't place guarantees on the actions of other vehicles on the road. But that doesn't mean you don't take the necessary precautions to protect yourself. You wear a seatbelt. You never text and drive. You avoid speeding.

## Shouldn't you take the same precautions with your business?

It's not enough to just understand the risks. You have to internalize them, and take the steps required to protect yourself. Many SMBs don't understand the risks associated with running a business in the digital age. Business owners are led to believe that breaches only happen to multinational corporations, not small companies that cater to local audiences. Thanks to their lower profiles, small businesses don't consider themselves a target for cybercrimes or hackers.

In actuality, a quick online search demonstrates that breaches on SMBs are occurring with greater frequency – Visa reports that an estimated 95% of data breaches occur at SMBs. Cyber criminals understand that small businesses typically do not have the same strong security standards in place as their bigger counterparts, and as such are easier targets. This puts your business, and the customers it serves, in danger of becoming another statistic on the evening news.

### Recognize Internal Threats

*When you're working at a small business, it's only natural that you're going to be familiar with all of the employees. You might have coffee with them in the mornings, or share the same lunch break. While it might be hard to believe that these trusted individuals would consider compromising the security of your business, you owe it to your customers to consider the possibility.*

Think small and medium sized businesses are safe from security risks? Think again. Here are some eye-opening stats:

- **Just over one third of businesses have a privacy policy that employees must comply with when handling sensitive customer or employee information.**
- **Less than half of SMBs believe that a data breach would have a real impact on their business.**
- **Only 31% of SMB owners consider their business to be 'very safe' in the face of various online threats.**
- **83% of businesses surveyed do not have a written cybersecurity plan.**
- **Less than half of small businesses terminate the online accounts of employees who have left their organization.**

*Source: 2012 NCSA/Symantec National Small Business Study*

If you're the owner of a SMB, now is the time to take charge. You're taking a great first step by arming yourself with the data required to make important and informed decisions. If you're reading this as a staff member of a small business who's looking to affect change in the workplace, take this material, and your concerns, to the business owner. Protect yourself before you're stuck in a crisis.

The next step to that is performing due diligence on your security systems.

## Security Step One:

Take the time to understand the risks that could impact your business – surveying industry trends and past breaches will help you prepare for the future.

# Chapter 2: Perform Security due Diligence

With a seemingly never ending stream of software patches and security upgrades required, it can seem like a lot to keep up with all of the security protocols needed to keep your business safe. Do you take the time weekly to ensure that your security systems are up to date? If you do, you're in the minority. Leaving security systems unpatched is like leaving your business' front door wide open. You don't let just anyone access your cash register, so take the same stance with your confidential data.

That's why small businesses are often an attractive target for online criminals. Although they might not have the same high-profile presence as larger organizations, their defenses are often lower – allowing for easier penetration. When you've got a small budget and an even smaller IT team it can be hard to ensure that all of the resources necessary for security are in place. That's why it's important that you're extra diligent in protecting the equipment you've already got.

Many businesses do not take the time required to update their Point of Sale (POS) or the hardware that it's attached to. According to the "Retail Reputations: A Risky Business" survey from McAfee, 38% of retailers are still running a legacy version of Microsoft Windows. Other businesses are running old or secondhand hardware, which could lead to various vulnerabilities and compatibility issues with newer security software and applications.

Ensure that any third party providers you work with are accountable to regulations and compliance standards in their own industries. Although it may seem tempting to just click 'I Agree,' closely read all terms of service agreements. This will help you understand the details of your responsibility in regards to data breaches and other issues that could impact your private information, as it is either stored by the third party, or is passing through their system – like a credit card processor. If the third party is not compliant with regulations such as the Payment Card Industry Security Standard (PCI DSS), you could be stuck paying customer damages' if your business is the victim of an attack.

## Living in the Cloud

*For many SMBs, cloud services are the best option. Cloud applications are often more cost effective and do not require the same complicated maintenance of onsite applications. Cloud systems are always up to date, and you can expect the experts in charge of the platform to implement the security regulations required to keep your records safe and secure.*

When you're working with an online provider – credit card, POS, cloud storage – understand their terms of service and security conditions. While appearing to be a lot of confusing terms and legal jargon, it's this information that could save you in the future. Don't be afraid to ask questions – if they're a reputable organization they should feel comfortable answering anything you need to know. Do not hesitate to get insight from an unbiased third party if required.

**Security Step Two:**
Save yourself from security heartbreak and make time each week to ensure your systems are up-to-date.

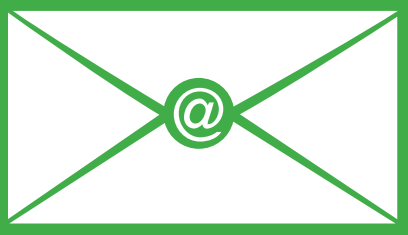
# Chapter 3: Train your Employees

In tough economic times it can be hard to justify the additional expense of training. But if it saves your business from compromising the privacy of your customers, it's worth it.

In workplaces around the world, an increasing number of employees are using the Internet to complete daily tasks. Whether the roles of your employees requires them to engage in communication with customers, conduct business-related research, maintain corporate accounts and profiles online or an assortment of other tasks, the Internet is one of the most common tools employees are using to be successful at their jobs. Unfortunately training on safe Internet usage is not increasing at the same rate.

According to the 2012 NCSA/Symantec National Small Business Study, only 29% of SMBs provide their staff with training on how to keep their computers secure. Just like with your favorite sports team, you're only as strong as your weakest link. The same goes for online security. If you have one employee who is downloading unauthorized material or using an email account that doesn't have a virus scan in place, you run the risk of infecting your whole organization.

That's why it's important to create a culture of training. Ensure that your employees have the skills they need to protect themselves and the interests of your business. The first step to providing training for your employees is recognizing what areas are the most important to your business. Are you concerned with the physical security of your POS or employee workstations? Maybe you're more interested in password protection and understanding wireless security. After you've recognized the areas most important to your business, investigate the resources available to you.



## Informational Emails

*Short informational emails are a great way to share manageable nuggets of information with staff on a regular basis. They serve as little reminders to keep everyone focused on security while completing their daily tasks. If password security is an important topic at your business, consider running a whole series on password protection. On the next page you'll find two examples of email templates to share with your staff on the theme of password security – for a more personalized touch, modify these templates with information that's relevant to your organization.*

Training doesn't have to be limited to a traditional one-day workshop. Knowledge sharing comes in many forms, including webinars, newsletters, formalized in-class training sessions and lunch and learns. Find the format that works best for you. Try out different methods of training, and see what gets the most response from your employees. Once you've found the format that works best, you can tailor sessions to really target the needs of your organization.

Email Template 1:


## Did you know *password* is the most common password?

*Strong passwords are important, but if you look at a list of the most common passwords you'll notice that many people don't put much thought into the process. Strong passwords are required to protect important business details, including client and payment information. When creating a password, consider the following:*

- *Passwords should be longer than 6 characters*
- *Passwords should contain a mixture of lower case and capital letters, as well as numbers and symbols when possible*
- *Do not use passwords closely associated with your personal life. These include birthdays, phone numbers, family members, etc.*

Email Template 1:

## When sharing isn't caring: Password protection

*Now that you've created a more secure password, it's important to give it adequate protection. Commit your password to memory and avoid writing it down. Do not share your password with others. You wouldn't share the key code access to your home with a stranger on the street, right? Think of passwords in the same fashion. They are responsible for protecting information that is highly valuable to our business – sales contracts, customer contacts and payment details.*

*If you're responsible for creating and sharing passwords with others for shared applications, ensure that the passwords are never delivered via email. Instead, share the passwords face to face, or by telephone if necessary.*

Security training will create a greater feeling of transparency in your daily business. Employees will recognize the steps they need to take to keep themselves and their work materials safe. They will feel more comfortable asking questions and reporting any strange activity, including online incidents and questionable emails.

**Security Step Three:**
Understand the education gaps of your business and plan sessions that provide the security training required to protect your assets.

# Chapter 4:
# Create a Security Policy

If your company has staff members that access the Internet, you need a security policy. To avoid any confusion as to what is and is not acceptable use for company devices, it's important that you clearly lay out what is expected of your employees. Just like human resource policies that dictate dress codes and standards on office conduct, security policies provide employees with guidance on best practices and expectations.

These policies are more than words on paper – if implemented correctly they provide your employees with the guidelines they need to make safe online decisions. While many employees, especially recent grads and others that fall into the category of a digital native, are comfortable using the Internet and are aware of best practices, other employees with limited experience could be a potential liability.

When it comes to developing a security policy for your business, it's important to remember that there is no one size fits all solution. Security policies take different forms across various industries, organizations and even departments. Different staff members may have different clearance levels when it comes to access privileges, so they may be governed by stricter regulations. What is important is that you include the details that you believe are the most pertinent to your business. Here are some areas that you should consider including in your security policy. Keep in mind these are just suggestions, and should be tailored to the needs and goals of your business.

- **Present guidelines to all employees on acceptable use of company equipment.** Are company machines permitted for at home use? Detail your expectations.
- **Be clear on email guidelines.** While almost all employees will be comfortable and familiar with email use, do not hesitate to include best practices on the downloading of attachments, phishing schemes, personal email usage and any other areas you deem relevant to your business.
- **Implement password quality parameters.** The proliferation of online services means there's an increasing amount of passwords to create and remember. The trouble is, with so many passwords, users may find themselves getting lax on password security. Reusing passwords, choosing passwords that are easy to remember – and not so difficult to crack – are common problems. Provide your employees with password best practices to help protect their information, and by extension your bottom line.

- **Explicitly outline privacy best practices.** If employees are sharing confidential information, make it clear which tools they should be using. Email does not always provide security and consumer grade file sharing can be vulnerable to outside attacks. Also ensure that staff members are well versed on the importance of not sharing their passwords with co-workers or outside parties.
- **Downloading guidelines.** Be explicit on what's permitted to be downloaded – include a list of applications and programs that are commonly used. On the same token, if there are other applications that are forbidden it's important that you outline those as well. Consider including a process on what to do if an employee is interested in downloading anything that isn't included on the list.
- **What happens if you don't follow the rules?** It's important to conclude your policy with a breakdown of the consequences for any infractions. Employees must know there are repercussions in place for non-compliance.

### What about mobile devices?

*If your business issues mobile devices to its employees, don't neglect to include this in your security policy. If your workplace practices BYOD (Bring Your Own Device) you might even want to formulate a separate policy on that as well. Wondering what to include there? We've got a blog post that will help you* **get started on a BYOD policy for your organization (reading a print copy?** *Visit bit.ly/tfbyodblog).*

Once you've completed your security policy, take the time to introduce it to your employees. Staff members need to understand not only what the policy requires of them, but also the importance of the security policy and how it relates to your corporate mission and values. Schedule time to go through the policy either in a group or one on one setting, ensuring that all employees have ample time to ask questions and voice any concerns. Employees must understand the role they play in preserving the security and integrity of your business.

Your security policy should be written in plain language so that it is accessible to all employees. Include clear examples and lists that make concepts easier to understand. If applicable, use anecdotes, either factual or fictional, that include your organization so that staff are left with examples that are relatable to their role in the company. Consider making both electronic and print versions of your security policy available to staff so that they can easily access a copy from anywhere.

Most importantly, always remind your staff they are an integral component of your security policy and that you value their efforts.

## Security Step Four:

Don't delay on creating a security policy for your business. By providing your employees with guidelines and best practices on Internet use, you're setting your organization up for a safer future.

# Chapter 5:
# Hire Expert Help

You've taken all the steps to implement sound security practices at your business. You understand the risks surrounding negligence of security, and recognize the negative impacts poor practices could have on you and your customers. But sometimes you might require a little outside help.

As a business owner are you responsible for the cybersecurity management of your organization? In many cases, SMB owners are burdened with having to understand and implement security solutions. You wouldn't expect your plumber to be able to perform the same tasks as your accountant, so why do you put yourself in a position that requires you to do jobs that you haven't had training in?

Your company may have an IT expert on payroll, but do they have the time or skills required to dedicate themselves to your security needs? Consider hiring outside help. Security consultants can test for vulnerabilities in your systems, and offer advice on how to ensure you're following the most stringent industry guidelines. Ultimately, they'll be able to provide sound advice on which steps to take towards protecting your security, and the privacy of your customers.

**Support in the Cloud**

*Involving an external security expert doesn't have to be complicated. If you're using cloud services, support teams can provide you with the security you require at a price that is already included in your monthly fee.*

**Security Step Five:**
Recognize the areas you need help with, and seek out an expert. It's okay to ask for help. Your business is your livelihood, so it's important to take the required steps to protect it from online attacks. Seeking the professional opinion of service providers and outside consultants can help ensure you have all of your bases covered.

# Conclusion

Now you know what's required to get your SMB on the path to security success. We know that we don't have to tell you twice that when a small-medium business closes its doors the entire community is negatively impacted. Jobs are lost, the economy feels negative implications, and the overall morale of the area takes a downturn. The costs of cybercrime can push small medium businesses to bankruptcy – arm yourself with the right tools so you don't become a statistic.

Security is a top down pursuit. Executive buy-in is essential. If you're the owner of your business, model safe online behaviors for your employees. If you're an employee, share this document and your personal thoughts on security with the owner and/or manager of the business to enact real change.

Taking the time to read this ebook demonstrates your commitment to the success of your business through security. Congratulations on taking the first steps to protecting yourself and your customers.

## Learn more

There are many steps that organizations can take to enhance their online security. If you're interested in learning about how secure file sharing can benefit your business and protect your confidential information, contact TitanFile. We'd love to discuss our platform, its collaborative abilities and the impact it could have on your organization. If you're looking for a source for security, privacy and collaboration news, be sure to visit our blog at www.titanfile.com/blog. You can also find us some other places online, including:

Visit us online: www.titanfile.com
Follow us on Twitter: www.twitter.com/titanfileinc
Like us on Facebook: www.facebook.com/titanfile

## About TitanFile

TitanFile was founded in 2010 with a goal of democratizing security. We do this by providing organizations of all sizes with a secure file-sharing platform that permits the protected document exchange, while still encouraging collaboration. Our secure collaboration Channels allow real-time conversation, inspiring subscribers to work together on important projects.

Author: Martha Gallagher
Designer: Matt Dupuis

# Five Simple Steps for SMB Security Checklist

You've read the ebook and now you're set to start implementing security at your workplace. We've done the legwork and created your to-do-list for you. Simply print this sheet and start checking items off as you work your way to security success.

## Understand the Risk

- [ ] Keep up to date on security news
- [ ] Understand common security issues and how they can impact your business
- [ ] Recognize the areas of your business that require improvements to security protocols

## Perform Security Due Diligence

- [ ] Ensure all of your security software and hardware applications are up to date
- [ ] Do your homework when dealing with third-party providers. Only choose solutions that are adherent to industry regulations

## Train your Employees

- [ ] Begin developing a training plan for your employees
- [ ] Poll your staff to see if there are any security items they'd like to know more about
- [ ] Decide which training format works best for your staff
- [ ] Create an internal newsletter, or add a new section to yours, that includes security tips and tricks

## Create a Security Policy

- [ ] Decide which areas require the most focus in your security policy
- [ ] Actively promote your policy to all staff members

## Hire Expert Help

- [ ] Recognize your problem areas and bring in help to troubleshoot solutions
- [ ] Using cloud solutions? Involve your service provider to better understand their security protocols

Interested in learning more about how TitanFile can help your SMB improve its security? **Contact us today to learn more.**

www.titanfile.com
+ 1 855 315-6012 | sales@titanfile.com