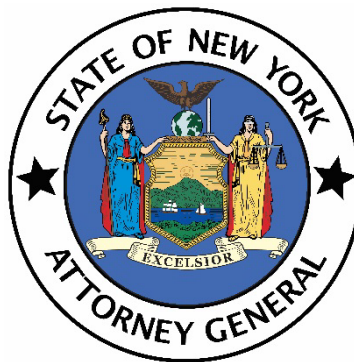

SMALL BUSINESS GUIDE TO CYBERSECURITY IN NEW YORK STATE



From the Office of
New York Attorney General Barbara D. Underwood

Dear Fellow New Yorker,

It seems that not a day goes by without news of another data breach. Tens of millions of records containing New Yorkers' personal information have been disclosed by some of the nation's most well-known companies. As a small business owner or manager, you may think this will never happen to you, but attacks on small and mid-size companies are growing rapidly and can have a major impact on business operations. Indeed, the majority of the breach notifications my office receives each year involve breaches affecting fewer than 100 people. Studies indicate that at least half of confirmed data breaches targeted small businesses, and as many as 60% of those businesses went out of business within six months of the cyber-attack.ⁱ Despite this ever-present threat, only 50% of small and medium businesses in the U.S. have secure company email to prevent "phishing" attacks, and only 10% of such businesses have taken basic steps to protect customer information.ⁱⁱ Clearly, there is good reason to develop strong security measures to protect your customers and your business operations.

No business is too small to be subject to an attack, and many internet attacks have no particular target. An attacker may simply send a large broadcast that takes advantage of any unprotected system it finds as a staging point. The attacker can then launch an attack on the infected computer or other computers. Without a data security plan and essential protections, like strong passwords and anti-virus software, you not only place your business at risk, but potentially expose your customers and other businesses as well.

It is critical to take certain steps to protect your company, your employees, and your customers from a data breach. If you use the internet to do business—even just to browse the web or use web-based email, you are vulnerable. This guide takes you through the process of developing a sound cybersecurity plan with minimal frustration and cost. Following the practices recommended in this guide will decrease your vulnerability and make your business safer.

Sincerely,

Barbara D. Underwood

What's At Stake If I'm Breached?

- **Your reputation:** Customers and other businesses may not trust you and may avoid conducting business with you.
- **Your business:** You might lose access to information you need to run your business. You might lose money if attackers use ransomware or steal your company's financial account information. You might need to halt operations to replace software and devices, resulting in lost time and revenue. After the attack, you might be at a competitive disadvantage as you work to regain customer trust and rebuild the ability to operate.
- **Investigatory Costs:** Regardless of whether you investigate the incident yourself or hire a professional, you will need to spend time and money to figure out what happened, when and how it happened, why you were vulnerable to the attack, and who was affected. You will also be required to notify employees, affected consumers, and government agencies—including the Office of the Attorney General—of the breach. If you are unprepared, these costs will multiply.
- **Legal Costs:** If you haven't taken reasonable precautions, or you did not provide notice to the affected consumers, breaches of sensitive data can create civil liability, both from individuals who had their data compromised and from law enforcement.

**IN 2016, HACKERS
BREACHED HALF OF ALL
U.S. SMALL BUSINESSES**

**OVER HALF OF
ATTACKED COMPANIES
GO OUT OF BUSINESS
WITHIN SIX MONTHS**

What Can I Do?

You don't have to spend a great deal of time or money to implement a good data security system. All you need is a plan that includes (i) consideration of what sensitive information you collect, (ii) how you keep it secure, and (iii) what steps you will take in case of a breach. The plan should also include training your employees and checking on them periodically to ensure they are carrying out your data security policies. Depending on the size and type of business you operate, you could combine annual training with a periodic e-mail reminder about data security, or you could periodically address data security at meetings or company retreats.

How Do I Keep My Customers' Information Secure?

In this guide,¹ we will explain how to implement the following 10 steps to keep your customers' information safe and secure:

1. Use Strong Passwords And Change Them Regularly
2. Use Anti-Virus Programs and Firewalls
3. Delete Old Files and Accounts
4. Limit Access to Sensitive Data
5. Be Cautious with Email Attachments, Links, and Downloads
6. Back Up Files/Folders/Software
7. Establish Network Security/Access Control
8. Establish Physical Access Controls for Computer Equipment
9. Keep Your Software Up to Date With the Latest Security Fixes
10. Get Help When Needed

¹ While this guide is intended to help you adopt better data security, it is not intended to offer legal advice. If in doubt, please consult with an attorney.

Password Managers:

How many online accounts does your business have? 5? 10? More? Do you remember all the passwords for them or do you use the same password? If it's the latter, and your password gets breached, all your accounts are at risk. Using a unique, strong password for every site is essential and a password manager software program can help. The typical password manager installs as a browser plug-in to automate the authentication process. When you log in to a secure site, it offers to save your credentials. When you return to that site, it offers to automatically fill it in.

STEP 1: USE STRONG PASSWORDS AND CHANGE THEM REGULARLY

Passwords are the first line of defense against an attacker. Thus, it is important to adopt a thoughtful password policy for your organization.

A good password policy:

- ✓ Uses long passphrases with uncommon words. They are easier to remember and harder to crack.
- ✓ Does not include the user's name, birthday, pet's or child's names, or anything that can be easily guessed.
- ✓ Does not use the default password on the account. Change the password that may have come standard with a software package.
- ✓ Never re-use the same password for two or more accounts.

Be aware that computer intruders use trial-and-error (or "brute force") techniques to discover passwords. By

bombarding a login program with all the words in a dictionary (which takes only a few minutes), intruders may "discover" the password. If they know something about you, such as your spouse's name, the kind of car you drive, or your interests, intruders can narrow the range of possible passwords and gain quick access. Consider a policy that suspends or disables accounts after repeated login attempts and be sure to choose software and service providers that utilize this security feature.

Want more tips? The U.S. Federal Trade Commission (FTC) provides useful information and offers advice on creating strong passwords.

STEP 2: INSTALL AND MAINTAIN ANTI-VIRUS/FIREWALL PROGRAMS

Much like the flu virus, a computer virus spreads from computer to computer, replicating itself and weakening the "immune system" of your computer. They come in all shapes and sizes – they can allow outsiders access to your computer, expose your personal files, render your computer unusable, and more. Protect yourself from these threats by installing anti-virus programs and firewalls.

Anti-virus programs are able to scan the contents of the files you download to determine whether they pose a risk. Many computers include anti-virus software, sometimes on a “trial basis,” and

KEY TERMINOLOGY

ENCRYPTION: the process of converting information or data into a code, especially to prevent unauthorized access.

PHISHING: a type of social engineering attack to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

SSL (Secure Sockets Layer): the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private.

there are many commercial options that won't break the bank. Install the software on each machine your employees use. Always update the program and allow it to perform system scans when prompted.

Firewalls are like a bouncer for your network; they scan the traffic coming into your computer and deny access to potential threats, such as communications to your computer from an unexpected foreign computer. Security professionals can install system firewalls at a relatively low cost.

Together, these protections can avoid problems before they start and keep your business running smoothly.

STEP 3: DELETE OLD FILES AND ACCOUNTS

Hackers can't steal sensitive information if it's not there. To limit the risks from an attack, delete customer or employee information files you no longer need. Unfortunately, dragging the files to the “Recycle Bin,” and selecting “Empty Recycle Bin” is not enough—the file will remain on the hard drive, at least until it is “overwritten.” You need specialized software to completely erase these files from your system's memory. Visit your operating system provider's website for free or low-cost options they recommend. Remember, only keep the information you absolutely need to run your business.

You should also promptly delete accounts for recently departed employees. Otherwise, anyone with access – such as a disgruntled former employee or his or her friend or family member – can steal your information. It's like changing the locks when your roommate moves out. Deleting old files and accounts also frees up more memory resources, so your computer will operate faster.

STEP 4: LIMIT ACCESS TO SENSITIVE DATA

Carefully manage which users are allowed access to sensitive files. For example, you may want to prohibit access to employee tax files to all but one or a select few employees who need such access in order to do their jobs. Educate employees to use care in sharing sensitive and confidential information, especially if it's health care or financial information, where additional

federal laws could apply. When possible, make sure that highly sensitive information is not stored on any computer that multiple employees use.

SENDING SENSITIVE INFORMATION OVER THE INTERNET:

If you send sensitive information over the internet, you should encrypt it first. Look for “https://” in the address bar when transferring sensitive information through a browser. It stands for Hyper Text Transfer Protocol Secure. The “S” at the end of HTTPS stands for “Secure.” It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

For highly sensitive information like social security numbers, consider implementing encryption. Encryption transforms information from one form (readable text) to another (“encrypted,” or scrambled text). The encrypted text appears to be gibberish and remains so for people who don’t have the formulas (encryption transformation scheme and decryption keys) to translate the encrypted text back into readable text. There are a number of low-cost encryption tools available to encrypt files on your desktop computer. You can also use your computer’s

IN FOCUS: “NO CLICK” LIST

system settings to enable BitLocker (Microsoft) or FileVault (OsX).

STEP 5: BE CAUTIOUS WITH EMAIL ATTACHMENTS AND DOWNLOADS

Watch out for one of the most common methods of getting a virus and providing an attacker with access to your computer network – attachments and links sent through email.

Make it a rule to not open email from anyone you don’t know. When in doubt, contact the sender by a separate email or phone call to see if they intended to send you an email. Train employees to identify these threats, and, if possible, test employees from time to time.

Do not open an email or link if:


- ✓ You do not recognize the sender
- ✓ Subject line is blank or has nonsense characters
- ✓ Message claims you have won something or must log in to an account
- ✓ Message requests you change a password by submitting your current password
- ✓ Message contains misspellings or awkward grammar
- ✓ Messages asks you to update or fix errors with an account you don’t use

Here is an example of what a phishing scam in an email message might look like as well as some red flags:

What to Look for with Scam E-mail

FROM: security@realbankorcompany.com
TO: You

SUBJECT: Verify your account NOW

 **REAL COMPANY NAME**
CUSTOMER SERVICE

Dear Customer,
A potential issue has been detected in regards to your **checkings** account. Please follow the link below and log-in to authenticate your account and reach customers service to resolve and restore access to your account.
It is critical you do this within 48 hours or your account may be suspended.

<http://scam.realbank123>

VERIFY MY ACCOUNT

Attachment: Security and safety at Bank Name.exe (9 MB)

Always look at the “from” field. Be aware that even this can be spoofed.

Check with the company directly if you are suspicious, or second-guessing the sender, based on the logo, fonts or heading. Also, be on alert if you don’t actually have an account with the company.

Spelling and grammar mistakes are a big red flag.

A threat or sense of urgency to spring you into immediate action is another red flag.

Hover (or ‘tap and hold’ on phones) over links to check they are actually directing you to the right site.

Never open or download anything that you are not 100% confident is from a safe source. Be extra vigilant about .exe files.

Cybercriminals often use web addresses that resemble the names of well-known companies but are slightly altered, such as “google.com” or “micsft.com.”

STEP 6: BACK UP ALL FILES/SOFTWARE

Be prepared for the unexpected. Maybe a customer spills a drink on your hardware, your software has some sort of fatal glitch, or an old computer finally gives out and you are suddenly left without access to your software and your files. Creating a backup of all of your files gives you an insurance policy.

Use an external hard drive, a secure cloud computing service, or ideally both to back up your files. Do this regularly to put yourself at ease about actions outside your control. And be sure to protect your backup files too, either by using hard-drives that are encrypted and password protected, or cloud-services that offer a high level of security and strong password protection.

STEP 7: ESTABLISH NETWORK SECURITY/ACCESS CONTROL

Attackers are constantly bombarding computers and computer components accessible from the internet with query functions looking for weaknesses. Unprotected devices can be compromised within minutes. As such, computer security requires access protection for each device on the network. Good access control is critical for wireless access as well, since use of this type of connectivity is less visible. Someone sitting outside could access an unsecured wireless network and jeopardize everything on the entire network, including point-of-sale (“POS”) devices and inventory devices that communicate to central servers via wireless.

Lockdown your network by:

- Limiting access to each device on the network with password management.
- Instructing employees to disconnect from the internet by turning off their computer when it is not in use.
- Eliminating any use of instant messaging, chat sessions, and music-sharing capabilities, since they establish other routes (peer-to-peer) into the network, bypassing many of the traditional network security mechanisms.
- Consider multi-factor authentication, especially for employees who log-in remotely. Multi-factor authentication is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting two or more pieces of evidence.

CASE STUDY:

In May 2017, over one million Google Docs users were sent a fake invitation (phished) to a document that looked like a legitimate invitation sent by the collaborative word processor. This led to access and control of email accounts, which are essential to almost all small businesses.

Source: WIRED

If you have a wireless network, it should be password protected and you should encrypt the information you send over your wireless network, so that nearby attackers are unable to eavesdrop on these communications. You should always use the most secure encryption, which at the time of this publication is called “WPA2.”

STEP 8: ESTABLISH PHYSICAL ACCESS CONTROLS FOR ALL COMPUTER EQUIPMENT

Think of all the people who have access to your computer and network throughout a given day: you, your employees, their friends and family, cleaning services, plumbers, repair people, mail carriers, and more. To limit who can access a computer:

- Make sure employees always log out when leaving the computer for any period of time.
- Limit use of personal devices on your network.
- Set computers to lock or “sleep” after a minute of inactivity.
- Make sure to lock down equipment and keep out of sight any manuals, accessories, or technology your business uses.

CASE STUDY:

The WannaCry ransomware attack was a worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied the patch, or were using older Windows systems that were past their end-of-life. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.

STEP 9: UPDATE YOUR SOFTWARE

Software updates, including mobile application updates, are more than extra frills or new features. They can provide critical security safeguards developed in response to various threats. It's easy to click “remind me later” when your computer wants you to update, but you risk leaving your computer vulnerable to security threats. Sometimes, it takes multiple patches to actually fix an issue, so it is important to consistently download them as the software provider releases new patches. Don't forget! These updates only work if you download and install them across all network computers and devices.

STEP 10: GET TECH HELP WHEN NEEDED

Turning to trusted security professionals can be a good option to ensure the utmost safety. Although hiring a professional may seem intimidating or expensive, there are many options that are reliable, affordable, and effective. Be careful, however, to make sure you're getting top-quality assistance from a safe and trusted source. Check websites for reviews and ask to speak with past clients. Some professionals can provide all necessary services from a remote location, which may be quick, convenient, and more affordable. Others can

implement a more thorough fix or preventative scheme in person, and may provide added comfort by guiding you through it all in your office space.

So What if I am Breached?

Here are some of the steps you should take if your business experiences a data breach:

1. **Investigate the Breach:** Investigate the breach and consider hiring information technology professionals to help you. Experts can capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps. You'll need to identify all the computer systems and applications affected; how the attackers gained access; and the identity of all victims including customers, employees, and vendors. You'll also need to address the vulnerability that led to the attack as soon as possible.

You should also consult with legal counsel who have privacy and data security expertise. They can advise you on federal and state laws that may be relevant to the breach.

2. **Contain the Breach:** Take all affected computer equipment offline immediately. Closely monitor all digital entry and exit points, especially those involved in the breach. If possible, put new computers online in place of affected ones. In addition, update credentials (i.e., usernames) and passwords of authorized users. If a hacker stole credentials, your system will remain vulnerable until you change those credentials, even if you've removed the hacker's tools.

Remember not to destroy evidence in the course of your investigation. It may be useful to you or law enforcement.

3. **Fix Vulnerabilities:** Work with your forensics experts and find out what happened. Analyze backup or preserved data. Review logs to determine who had access to the data at the time of the breach. Also, analyze who currently has access, determine whether that access is needed, and restrict access if it is not. If you receive a report for your forensic expert, implement any recommended remedial measures as soon as possible.

4. **Notify Relevant Parties**

- a. *Notify Consumers:* The faster consumers know that their personal information has been breached, the faster they can take action to prevent harm. Not only is consumer notification the right thing to do, most states, including New York, legally require notification if certain information is disclosed including a customer's name in combination with a social security number or credit card

number. Notification must also be sent to the Office of the Attorney General as well as the New York State Division of State Police and New York State Division of Consumer Protection. You should consult an attorney to review your notification requirements. **Attached as Exhibit A is a model consumer data breach notification letter.**

- b. *Notify Law Enforcement:* Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police aren't familiar with investigating information data breaches, contact the local office of the FBI or the U.S. Secret Service.
- c. *Notify Consumer Reporting Agencies:* If names and Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice. If the compromise involves thousands of people, advise the credit bureaus and consider recommending that the victims request fraud alerts and credit freezes for their files.

Equifax: equifax.com or 1-800-525-6285

Experian: experian.com or 1-888-397-3742

TransUnion: transunion.com or 1-800-680-7289

5. Manage Customer and Public Relations: How you break the news of the breach to your customers and vendors can be a strong determining factor of whether you will be able to maintain those business relationships. If you are providing credit monitoring or any other service or special offer, include information about the service in your notifications.

“An Ounce of Prevention Is Worth a Pound of Cure”

The best data breach response plan is one you never need. It's imperative that you protect your business – and customers – from falling victim to a data breach. A data breach can happen at any time and small businesses are common targets. Don't let another day go by unprepared.

ⁱ *Internet Privacy in the Digital Age*, CHAMPLAIN COLLEGE GRADUATE STUDIES, <http://mastersinlaw.champlain.edu/internet-privacy-in-the-digital-age/> (last visited Jan. 19, 2018).

ⁱⁱ *Hacked: Just Because It's In The Cloud, Doesn't Mean Bad Guys Can't Reach It.*, UPS CAPITAL, https://upscapital.com/wp-content/themes/upscapital/assets/media/CyberSecurity_Infographic.pdf (last visited Jan. 19, 2018).