nase

SelfInformed

Published by the National Association for the Self-Employed

September 2019

Member Spotlight

Laura Mauck

Juggernaut Cargo Bikes

Straightforward Data Security for Small Businesses

The technological landscape has changed enormously over the past decades for small businesses with the explosion of smartphones, online shopping, and cloud-based data storage. Small businesses and the self-employed have the ability to more efficiently manage operations, communicate with employees and clients no matter their location, and reach vastly greater numbers of potential customers.

But the same digital innovations that open up new horizons for business can bring catastrophic security risks if basic data and IT systems protocols are not in place. The technical nature of data security can feel overwhelming for small businesses, especially if money and time constraints are tight.

But small business owners cannot afford ignorance when it comes to securing their data and operations. According to the Better Business Bureau, more than **one in five businesses have been the target** of a cyberattack, with a median loss of $2,000. Perhaps even more worrisome, "smaller businesses may be unaware that they have been attacked." Security firm Fire Eye reports that, on average, it takes **146 days for a "cyber intrusion" to be detected**.

So where do you begin? In this article, the National Association for the Self-Employed (NASE) provides practical guidance on the following topics:

- Security and privacy policies
- Simple ways to guard against cyberattack
- Cloud-based data storage
- Local backup and security tips
- Free resources for cybersecurity planning

Secure The Perimeter

First, identify the **what**, **where**, **who**, and **how** of your sensitive information.

What: What is sensitive data?

Critical business data obviously includes your financial records, credit card transaction details, and any personal information of your employees.

Sensitive data can also include any documents, emails, spreadsheets, databases that contain any financial or personal information – in both electronic and paper form.

Where: Where is this information stored?

Whether it is on computers, smartphones, servers, ledgers, filing cabinets, or a desk drawer, you need to know every location of this data and secure it.

If you are using a wireless network for internet in your office or home business, there are a few highly effective precautions to take immediately:

- Protect your network with a password
- Hide your network name and password protect your router
- Use WPA2 encryption rather than WEP
- Review and change passwords every few months
- Ensure all passwords in your system are strong and updated regularly.

The US Small Business Administration recommends that you **use a firewall and encrypt information**. Although these precautions may sound technically daunting, they are all relatively simple – and entirely free.

Encryption expert and IT consultant Stephen Cooper, who offers a plain-language, **step-by-step guide to securing a wireless network**, notes that "You don't have to be a technical expert in order to improve the security of your home wifi network, you just need to be a little smarter in your habits."

Who: Do you know exactly who has access to your sensitive data?

No employee needs access to everything, not even an IT technician. Limit access to records on a need-to-know basis, and separately store different types of information. Maintain a record of who accesses

what, and when, in the event that sensitive data is compromised or disappears.

How: How do you access data?

Smartphones and personal laptops are increasingly used for work, which means work files and personal data can get mixed. It also means inadequate security precautions against an attack or accidental loss.

These devices are taken outside of the office, where they may be used on public wi-fi. Sensitive work data may also be exposed through apps that sniff through all the content on a user's phone.

Besides inadvertent online exposures, phones and laptops are prime targets for loss or theft because of their portability. The Small Business Administration advises having a "**mobile device action plan**" in case physical devices like smartphones are lost.

Workplace culture

The best precaution against a data breach is establishing a culture of security in the workplace.

If you have employees, they should be trained in privacy and security practices. They should know what data they are permitted to access, and how devices containing work information should be used.

All employees should use passwords on their computers and phones, and encrypt their data. Antivirus and security apps can help prevent their devices from being compromised while they are on non-work networks that may not be secure. And *everyone* should understand the dangers of downloading random files that could contain spyware.

Even if you have no employees at all, a culture of security means consciously cultivating your own habits of proper data management and technological maintenance.

Keep your systems up to date, change your passwords regularly, and educate yourself about ransomware, phishing scams, and other common cyberattacks.

Call For Backup

The loss of essential data could render a small business inoperable. Recovering from this kind of problem is difficult without a backup plan. Indeed, a **2017 survey of small business owners** by the Better Business Bureau found that only 35 percent of businesses "could remain profitable for more than three months if they permanently lost access to essential data" because of a cyberattack, and "more than half would be unprofitable in under a month."

Although the discussion on data backup is often presented as a question of local storage *versus* "the cloud," in reality small businesses can benefit from utilizing *both* methods. The purpose of storage solutions is to ensure your data is safely backed up in case of a disaster – including break-ins, fires, or just your garden-variety computer crash.

By having an out-of-office copy of your data, you can get back up to speed after an unfortunate event. "Out-of-office" is the key.

"We recommend backing up data through a cloud-service provider or a removable hard drive and keeping the backup away from your office, so if there is a fire, your data will be safe," says Pat Toth, who oversees **cybersecurity education for small businesses** at the National Institute of Standards and Technology (NIST).

Whichever option you choose, it's best to back your data up automatically if you can, or at least on a weekly basis.

Is your head in the cloud?

When we talk about sending data to "the cloud," we're actually talking about services that provide remote data storage space on secure servers, which you can access via high-speed internet from anywhere.

Chances are, you already use cloud-based filesharing systems like Dropbox or Google Drive. The difference between cloud backup and those free file services is security and comprehensive data backup.

The beauty of a service like Dropbox is that you can share a folder with someone else and it is synced when one of you uploads a file. A full-service cloud storage option allows this syncing for *all* of your data and system files in a secure manner.

Some affordable cloud options include:

- **Carbonite –** Probably the most well-known of cloud storage systems, Carbonite offers unlimited storage and encryption during data transfer at a reasonable price.
- **SpiderOak –** Similar to Carbonite in its encryption and backup syncing, SpiderOak offers up to 5 TB of cloud storage.
- **OpenDrive –** A smaller company that offers a *free* option for personal use, OpenDrive places a 500GB limit on cloud storage space – which may be all you need.

Think local

Locally, backing up your storage can be as simple as plugging in an **external hard drive** and copying

"We recommend backing up data through a cloud-service provider or a removable hard drive and keeping the backup away from your office, so if there is a fire, your data will be safe,"

Pat Toth

National Institute of Standards and Technology (NIST)

over your computer's files. While you'll need a separate external drive for each computer, with enough space for all your data, this is still a very affordable option for a micro-business or self-employed person.

A major upshot of this basic approach is that your data is secure as long as your hard drive is in a safe physical location. Again, away from your computer and place of work is best.

One obvious downside is that you can only access your backup data by physically plugging into it. Another is that external hard drives can crash just like your computer hard drive, resulting in data loss.

Unlike cloud services, with local backup no third-parties are involved, meaning only authorized personnel have access to the data. For this reason, local backup is preferred by companies dealing with personally identifiable information, medical records, or other sensitive data where state and federal laws may regulate how records can be stored.

Back to basics

Not all security measures are sophisticated. There are simple ways to prevent the loss of your data. For example, you should install surge protectors and power supplies that won't go down the instant you lose power.

To lower the risk of cyberattacks, turn off computers and routers at night or when you are not using them. Configure your software to automatically install updates.

Finally, don't forget about your paper trail. Regardless of company type, most small business owners generate their share of paper bills, receipts, or notes with the personal information of employees and customers.

It seems elementary, but two of the best security investments you can make are still a substantial, locking metal filing cabinet and a quality paper shredder.

Free Resources For Cybersecurity

The Computer Security Resource Center (CSRC) offers education in the **fundamentals of information cybersecurity** for small businesses.

The US Small Business Administration offers free courses for **cybercrime prevention** and tips to **protect your business against ransomware.**

The Financial Industry Regulatory Authority (FINRA) provides a free **Small Firm Cybersecurity Checklist** to help you identify vulnerabilities in your data security.

New!

Member Benefits

Visit **NASE.org** to learn more about the following benefits!

Careington
SOLUTIONS SIMPLIFIED®

Click Here to Get Started

CAREINGTON SAVINGS PLANS

Discounts on dental, vision and more!

Careington offers a variety of savings plans to help you and your family get high-quality health and wellness services at an affordable price.

500 Dental Savings Plan

Starting at: $8.95/month*

Save on most dental procedures, including routine and preventive dental care, major dental work and more. This is our most popular dental discount plan and it offers our deepest discounts.

Dental Only

Starting at: $8.95/month* Careington Savings

Save on the cost of most dental procedures, including cleanings, checkups and major work like crowns, root canals and more. Members can also email a dentist at any time to ask questions.

Dental & Vision

Starting at: $9.95/month*

Get discounts on dental care, including cleanings, checkups, fillings and more, vision care, including eye exams, frames, and lenses and medical information.

Telehealth with Healthcare Assistance

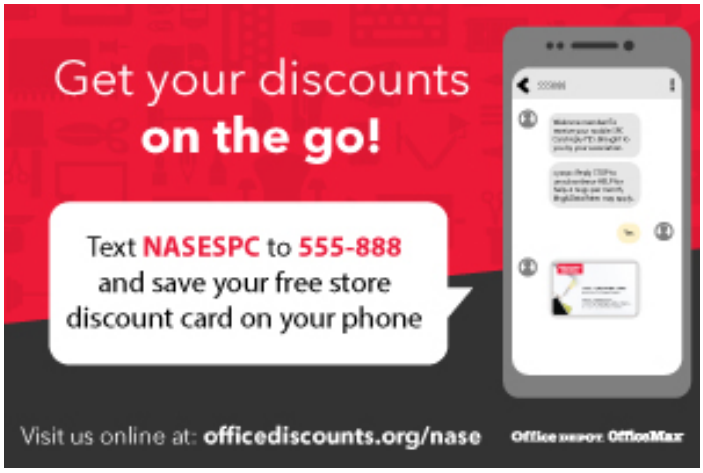
Starting at: $19.95/month*

Get 24-hour phone access to physician consultation and 24-hour access to a nurse phone line for symptom assessments, advice and recommendations, prescription discounts and travel and medical assistance.

Total Health

Starting at: $29.95/month*

Get the complete package and save on dental care, vision care, telemedicine services, diabetes care supplies, chiropractic and alternative medicine, prescriptions and more.



You can now text NASESPC to 555-888 to receive your free discount card!

Because you're a member of the NASE, you have access to these great benefits with Office Depot and OfficeMax.

- ✓ Substantial discounts on thousands of products
- ✓ Free next-day delivery
- ✓ Low cost on both printing and photocopying
- ✓ Choose online or in store, discounts apply either way

Start Saving Today!

Ask the Expert

Question:

I extended my tax return that is now due on October 15th. I just discovered that I left off some expenses from the previous year that I should have included. Can I include those amounts on this tax return or on next year's tax return, or have I lost the benefit of those expenses?

Answer:

The easy answer is 'No' to both questions. It would not be appropriate to include payments made in a prior year on the current year's income tax return or on the next year's tax return, but the good news is that does not mean you have lost the benefit. As you probably already know, the IRS keeps our tax returns 'open' for three years, meaning that they can go back and examine those returns for potential errors or omissions at any time during that three year period. That may not sound fair, but it also means that we can make adjustments to those returns as well if indeed we find that something was omitted or we discovered an error. The correct approach for the omitted deductions that you have discovered is to file an amended tax return for the tax year to which the items actually apply. The process is much easier than it sounds and in most cases you can complete the process yourself. If you use a tax professional, it would be a good idea to visit with them first to see how much in additional fees you will incur compared to the tax that you will recoup to determine whether or not the amended return is worth the effort.

The amended return is completed using IRS Form 1040X. You can download a copy of the form along with detailed instructions directly from the IRS website at www.IRS.gov. The form is basically just a comparison of the information that was originally filed and the new information that includes the missing items. Any specific forms from the original return that have changed based on the new data are also attached to the Form 1040X and that's it. Pretty simple and in most cases certainly worth the effort. The bottom line is that you should not include old items on the current tax return, but also don't assume that there is no benefit from those items.

As always, don't forget that you are not alone. Bookmark our website at **NASE.org** as well as the IRS website at **IRS.gov** you will always be able to find the help you need.

Riding Self-Employment

Laura Mauck is the Co-Owner & Communications Director of Juggernaut Cargo Bikes in Denver, Colorado. Juggernaut Cargo Bikes was born from Laura's experiences in urban planning, architecture and design. These influences came together to create a handcrafted and precision-engineered product that is practical, effective, and beautiful.

When and why did you join the NASE?

We joined NASE a year ago when we applied for and received the small business Growth Grant.

What inspired you to enter your current field?

We were inspired to start our business because of our backgrounds and our love of biking. My partner Jeff is a designer and urban planner and my other partner, Dan, is a real estate agent with a unique perspective on the changing urban environment in Denver, and I am a historic preservationist. We are all avid bikers and we wanted to offer an alternative form of transportation in our ever growing and congested city of Denver, with the dream of selling our product throughout the United States.

When and why did you start your business?

We started our business in 2017 after being inspired by European cargo bikes. We saw that they were very popular in places like Copenhagen, Amsterdam, and Barcelona and thought that the United States would embrace the concept as well.

How do you market your business?

We market our business through social media, newsletters, attendance at events/shows/conferences and by word of mouth.

What challenges have you faced in your business?

Our biggest challenge has been being "first to market" in America. While cargo bikes are very popular in Europe, Americans have not quite caught on to the movement. We are overcoming this obstacle by building awareness of our product and taking advantage of every opportunity that is offered to us to help share our love and passion for this product.

Do you have any employees?

We do not currently have employees, but work with independent contractors such as our bike builder and engineer. We hope to have employees after we have finished our production run.

Can you tell us about your schedule and what a typical day is like for you?

Since we are currently in the production phase of our business, a typical day finds us spending a lot of time with our bike builder and engineer. It takes a lot of effort to make sure all the parts are ordered and coming in at the right times from all over the world. We also spend a lot of time doing outreach and marketing both through social media and by attending events. We are also passionate about changing biking infrastructure for the better, so we spend a lot of time advocating on the local, state and federal level for improved bike lanes.

What's the best thing about being self-employed?

The best thing about being self-employed is being able to express our creativity and to take advantage of constant opportunities to learn new things. There is so much satisfaction in mastering new challenges and accomplishing something new and unknown.

What's the best compliment you've ever received from a client?

The best compliments for us are always the look on people's faces when they first drive, or ride in our cargo bike. They express sheer happiness and amazement at how easy it is to use and how comfortable it is. We love reminding people of the freedom that can come from letting go of your car and getting on a bike.

What's the most important piece of advice you would give to someone starting their own business?

The most important piece of advice I would give to someone starting a new business is to make sure that the thing you are starting is something you are passionate about. When the going gets rough, the pressure is on, or doubt starts to creep in, it is important to believe in your product and to be passionate about your purpose.

Which NASE member benefit is most important to you?

Applying for and receiving the grant was a great help to us, but we also enjoy receiving the informative emails and taking advantage of the discounts at Office Max.

NASE Supports New Legislation
Harmonizing Employee Definitions

In August, after careful evaluation, the National Association for the Self-Employed endorsed H.R. 4069, the *Modern Worker Empowerment Act,* introduced by Congresswoman Elise Stefanik (R-NY) and co-sponsored by Reps. Bradley Byrne (R-Al), Phil Roe (R-TN) and Ron Wright (R-TX).

The *Modern Worker Empowerment Act* would liberate independent entrepreneurs by updating the definition of the term "employee" for purposes of the Fair Labor Standards Act ("FLSA") and conforming it to the other New Deal statutes enacted during the 1930s that also applied an "economic realities" test many years ago but now apply a common-law definition for the term.

The common-law definitions include:

- **Behavioral:** Does the company control or have the right to control what the worker does and how the worker does his or her job?
- **Financial:** Are the business aspects of the worker's job controlled by the payer? (these include things like how worker is paid, whether expenses are reimbursed, who provides tools/ supplies, etc.)
- **Type of Relationship:** Are there written contracts or employee type benefits (i.e. pension plan, insurance, vacation pay, etc.)? Will the relationship continue and is the work performed a key aspect of the business?

Per the Coalition to Promote Independent Entrepreneurs (of which NASE is a supporter), "a harmonized definition of "employee" would be beneficial to all stakeholders. It would provide much needed certainty to independent entrepreneurs and their clients, while also enabling government agencies to more efficiently ensure proper worker classification."

Read the text, **H.R. 4069**.

Katie Vlietstra is NASE's Vice President for Government Relations and Public Affairs; You can contact her at **kvlietstra@nase.org**.