**The Bensman Group**
Joel Feiger, CPA/PFS
President & COO
2333 Waukegan Rd
Suite 275
847-572-0808
jfeiger@bensman.com
www.bensman.com

The BENSMAN group
*Your Strategic Alliance for Life™*

# How to Protect Your Small Business from Cyber Threats

***In addition to visiting the SBA cybersecurity website, business owners might want to review "Protecting Personal Information: A Guide for Business" and "Start with Security: A Guide for Business," both available on the FTC website.***

Risk management is a key component in any successful business plan. In today's world — where data breaches are common occurrences — it's especially important for business owners to understand the digital risks they face. Are you doing all you can to mitigate the risk of a cyberattack?

## The importance of cybersecurity

Many small-business owners may think their organizations hold little appeal to hackers due to their small size and limited scope. However, according to the Small Business Administration (SBA), this naiveté may actually make them ideal targets. Small businesses are keepers of employee and customer data, financial account information, and intellectual property. Their systems, if not adequately protected, may also inadvertently provide access to larger supplier networks. "Given their role in the nation's supply chain and economy, combined with fewer resources than their larger counterparts to secure their information, systems, and networks, small employers are an attractive target for cybercriminals," reports the SBA on its cybersecurity website. Consider the following tips compiled from information supplied by the SBA, the Federal Trade Commission (FTC), and the Federal Communications Commission (FCC).

## What are your vulnerabilities?

To protect your organization, you must first understand your vulnerabilities. How are your systems protected? Do you collect and store personal information of customers and employees, such as credit-card information, Social Security numbers, and birth dates? If so, how is this information stored and who may access it? Do you store it in multiple locations and formats? Are these files password protected and, if so, are you using multiple complex passwords? Do you have a Wi-Fi accessible to employees and customers? How do your vendors and other third-party service providers protect their information? You may want to engage a professional to help identify your risks.

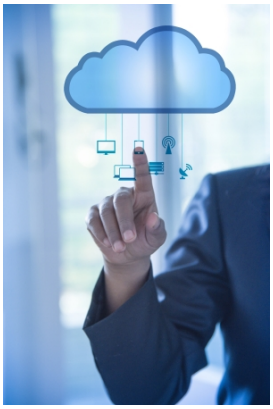
## Tips for security

When monitoring your security, ensure you have firewall and encryption technology that protects your Internet connections and Wi-Fi networks. Make sure your business's computers have antivirus and anti-spyware software installed and updated automatically. Require employees and others who access your systems to use complex passwords that are changed regularly. Keep only personal data that you actually need and dispose of it securely as soon as it no longer serves a business purpose. Back up critical information and data on a regular basis, and store the backups securely offsite. Assign individual user accounts to employees and permit access to software and systems only as needed. Be especially cautious with laptops and company-assigned smartphones. Question third-party vendors to ensure that their security practices comply with your standards.

## Redundancy is key

In writing or speaking, redundancy is typically not recommended unless you're really trying to drive a point home. When it comes to your digital life, however, redundancy is not only recommended, it's critical. That's because redundancy means having multiple data backups stored in different locations. Here are some ideas for redundancy when backing up your data:

- If you have digital assets that you don't want to risk losing forever — including photos, videos, original recordings, financial documents, and other materials — you'll want to back them up regularly. And it's not just materials on your personal computer, but your mobile devices as well. Depending on how much you use your devices, you may want to back them up as frequently as every few days.
- A good rule to follow is the 3-2-1 rule. This rule helps reduce the risk that any one event — such as a fire, theft, or hack — will destroy or compromise both your primary data and all your backups.



***A complex password is one that contains both upper- and lower-case letters, numbers, and symbols, and should not contain words or revealing combinations such as your birth date, phone number, or Social Security number.***

- Have at least three copies of your data. This means a minimum of the original plus two backups. In the world of computer redundancy, more is definitely better.
- Use at least two different formats. For example, you might have one copy on an external hard drive and another on a flash drive, or one copy on a flash drive and another using a cloud-based service.
- Ensure that at least one backup copy is stored offsite. You could store your external hard drive in a safe-deposit box or at a trusted friend or family member's house. Cloud storage is also considered offsite.

## More about cloud storage

Cloud storage — using Internet-based service providers to store digital assets such as books, music, videos, photos, and even important documents including financial statements and contracts — has become increasingly popular in recent years. But is it right for you? If a cloud service is one of your backup tactics, be sure to review carefully the company's policies and procedures for security and backup of its servers. Another good idea is to encrypt (that is, convert to code) to protect sensitive documents and your external drives. Other considerations include:

- Evaluate the provider's reputation. Is the service well known, well tested, and well reviewed by information security specialists?
- Consider the provider's own security and redundancy procedures. Look for such features as two-factor authentication and complex password requirements. Does it have copies of your data on servers at multiple geographic locations, so that a disaster in one area won't result in an irretrievable loss of data?
- Review the provider's service agreement and terms and conditions. Make sure you understand how your data will be protected and what recourse you have in the event of a breach or loss. Also understand what happens when you delete a file — will it be completely removed from all servers? In the event a government subpoena is issued, must the service provider hand over the data?
- Consider encryption processes, which prevent access to your data without your personal password (including access by people who work for the service provider). Will you be using a browser or app that provides for data encryption during transfer? And once your data is stored on the cloud servers, will it continue to be encrypted?
- Make sure you have a complex system for creating passwords and never share your passwords with anyone.

## Educate your employees

To help ensure that your employees are also maintaining sound cybersecurity practices, establish clear security policies and procedures and put them in writing. Cover such topics as handling sensitive or personal information, appropriate use of Internet and social media, and reporting vulnerabilities. Clearly spell out consequences for failing to follow the policies. Develop a mandatory employee training program on the importance of cybersecurity. Explain the basics of personal information, as well as what is and isn't acceptable to post on social media. Employees could unknowingly release information that could be used by competitors or, worse, by criminals. Ensure that employees understand the risks associated with phishing emails, as well as "social engineering" — manipulative tactics criminals use to trick employees into divulging confidential information.

For more information, visit the SBA cybersecurity website.

Securities may be offered through Kestra Investment Services, LLC, (Kestra IS), member FINRA/SIPC. Investment Advisory Services may be offered through Kestra Advisory Services, LLC, (Kestra AS) an affiliate of Kestra IS. Kestra IS and Kestra AS may or may not be affiliated with the firm branded on this material.


Prepared by Broadridge Investor Communication Solutions, Inc. Copyright 2016