CYBERSECURITY

Addressing The Growing Threat To Small Businesses

AMERICA'S SBDC VIRGINIA
BLUE RIDGE CROSSROADS

Twin County™
CHAMBER OF COMMERCE
Together to Prosper

Cybersecurity

Addressing the Growing Threat to Small Businesses

In the year 2019 43% of all data breaches were attacks on small businesses. While large corporations and public entities make headlines when they are victims, increasingly hackers are targeting small- to medium-sized businesses. They recognize that too often these companies fail to give the appropriate attention to the protection of their information, making them easy targets. The number of attacks is continuing to grow, making the likelihood of your business being a victim very high.

What are the hackers after? For one thing they are collecting information that can be used or sold – personal information such as dates of birth, social security numbers, and so forth. If you have employees, members, or customers who have supplied this information to you, it is likely stored in a place that is vulnerable to cyber-theft.

Rising at an alarming rate is the intrusion for ransom. Hackers often ask for as little as $1,500 as payment for unlocking your data, or for not distributing the information. Of course, they often ask for much larger amounts. Few small businesses, often operating on tight margins, can afford the payments these criminals demand.

Securing all the data you store to run your business is no longer something that can be put off. It must be a priority. There are experts you can turn to for risk assessment and solutions. If the cost of hiring a company feels beyond your reach, you can take a number of proactive steps yourself to improve data security. This guide will help walk you through the process.

Assessing the Threat to Your Business

The first step to protecting your business against a cyber-attack is to assess what actual threats your business is exposed to. Hackers can access information from many different entry points, so taking inventory of all the assets your company utilizes is important.

- ☑ Create a spreadsheet to keep a record of all hardware – laptops, desktops, tablets, cell phones, iOT devices, POS, routers, and modems. It's a good idea to record the serial numbers, date of purchase, last date it was updated, and who has access to it.
- ☑ A spreadsheet to track all of the software programs your business uses is also vital. You will no doubt be surprised just how many software and internet programs your company utilizes. Who has access to these systems? Limiting the number of people who have access to each program is strongly suggested.

➜ *Download a free spreadsheet for tracking at the CIS website:*
https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/

It is vitally important to track all online accounts - including email accounts - and who has access to them. Limit data access to only personnel who truly need it. (Making passwords difficult to guess helps prevent disgruntled employees and third-party associates from guessing them if the relationships are terminated. See tips for creating strong passwords later in this paper.)

60% of data breaches at small- to medium-sized companies were a result of a negligent employee or contractor, according to a study by Ponemon Institute (2018)

Do you have old devices laying around you no longer use that is still storing data? Are there old online accounts and software applications that you have forgotten about? Make a record of these and then delete all data. Re-set unused devices to factory settings or have them professionally wiped clean of all data.

Addressing the Threat to Your Business

Once you have taken inventory of all possible entry points that could threaten your data security, it's time to take action to strengthen the security measures you have in place.

- ☑ Ensure all of your systems are updated with the latest versions, including cell phones, browsers, and all applications (Microsoft Office, etc.) These updates include enhanced protection against malware and ransomware. ⇨ Set these systems to automatically update.
- ☑ Encrypt your data utilizing online freeware for emails and operating systems (Windows, Mac).

➔ *Find links to this freeware at the CIS website:*
https://gcatoolkit.org/smallbusiness/update-your-defenses/?_tk=encrypt-your-data

Email Security Tips

- ☑ Implement 2-Factor or Multi-Factor authentication where possible. This adds a layer of protection by requiring verification through a biometric (fingerprint or facial recognition) or via a verification sent to your phone or an application token (Google Authenticator, for example).
- ☑ Avoid signing into accounts when using public Wi-Fi. If you travel often and need to utilize public Wi-Fi consider investing in a VPN (Virtual Private Network) app.
- ☑ Never click on a link in an email that tells you to reset your password. Go directly to the site via a browser and reset your password if necessary. (Be suspicious of *all* links in emails. Make it a practice to access sites by navigating there manually on your secure browser.)

Hackers use software programs that run through possible combination of letters, numbers, and symbols. The longer the password the longer it takes the program to get it. Hackers are looking for quick and easy access. You can deter them by using the suggestions in the box when creating your passwords.

- Avoid using names of family and pets – this is the first thing hackers will try.
- Use long, nonsense phrases that include upper- and lower-case letters, numbers and symbols.
- Don't use the same password for multiple accounts.
- Use an online password manager – a virtual lock box for storing all your passwords.

Website Security Tips

☑ If your website collects any customer data it is especially prone to getting attention from hackers. Strong security and encryption measures should be in place. This is definitely not an area where you want to cut corners. The trust of your clientele is paramount.

⇨ Check with your webmaster or designer, or with your host, to determine if your site is encrypted with HTTPS (SSL/ TLS) certificates.

☑ Go to ImmuniWeb (immuniweb.com/websec) to check for security weaknesses. This site also scans your site for encryption strength, HIPAA compliance, and other security checks.

Phishing and Malware Prevention

Phishing: the practice of sending fraudulent emails that falsely claim to be from reputable companies and institutions with the intent to induce people to reveal confidential information such as passwords or credit card information.

Malware: ('malicious software') intrusive software designed to damage or destroy computer systems. Examples include worms, viruses, spyware, Trojan viruses, ransomware.

- If you run Microsoft systems, go the Microsoft support website and search for Microsoft Defender. This program is a security tool designed to prevent malware from infecting your computer systems. There are also other paid anti-virus protection tools you can install.
- If you use a Mac or other Apple systems, there are various anti-virus options available such as Norton, McAfee and Bitdefender. Research which option is best for your needs and budget. (While Apple products are less prone to viruses, they are not invincible and hackers are gaining ground on invading these products.)

System Backup and Recovery

Ransomware is designed to infiltrate your systems and 'lock' all your data. The hacker then demands an exorbitant ransom be paid to 'release' your data. Having a backup protocol in place will provide you access to recent data that you can recover thus making the need to pay the ransom unnecessary.

Both Apple and Microsoft offer tools that allow you to back up your data at regular intervals. (Navigate to the Apple website and search for Time Machine Backup, or to Microsoft's website and search for Windows Auto-Backup.)

Security Checks and Protocols

- ☑ Delegate one individual to be responsible for the oversight of data security. (This creates efficiency as they become familiar with the process, and more importantly, they will be attuned to any irregularities.)
- ☑ Maintain a strict regimen for updating hardware and systems, recording the dates in the spreadsheets.
- ☑ Regularly run diagnostics on your website, checking for phishing activity. (ImmuniWeb has an excellent Phishing Detection tool.)
- ☑ Educate your entire staff on safety protocols, particularly in relation to emails, as this is the most common entry point for breaches.
- ☑ Have an incident response plan in place for the action steps needed in the event of a data breach. Be prepared for the different scenarios (ransom attack, malware, etc.).

Talk to your insurance agent about cybercrime insurance.

In the Event of a Cybercrime / Data Breach

- ☑ If one of your hardware devices such as a laptop or cell phone is lost it would be prudent to change all of your online account passwords as a safety precaution.
- ☑ If an employee or third-party contractor who had access to any devices or data leaves or is dismissed, change all passwords immediately.
- ☑ If you are the victim of a data breach, immediate action is important.
    - You must notify your employees and customers as soon as possible if personal data has been accessed by an unauthorized person(s), in accordance with your state's statutes.
    - Your state may also require that you notify the state Attorney General, or other government agency.
    - To report the crime to the FBI go to ic3.gov
- ☑ Notify your insurance agent immediately.

If you have not already done so, consider contracting with a cybersecurity expert to assess your security measures and offer solutions to strengthen your data security.

Summary

Technology changes rapidly, and hackers work tirelessly to break through security protocols. Diligence is required to ensure that your data – and data your are entrusted with, such as employee's and customer's personal information - is protected. It is important to schedule regular, frequent security checks on all your equipment and programs. This should be delegated to one trustworthy person who will become familiar with the data and the steps necessary to maintain a strong security protocol. Thus, this person will more readily recognize when something is 'off.' Having an incident response plan in place will help address any issues quickly and, hopefully, limit the damage.

As the owner of a small business you wear many hats, and no doubt work long hours to keep your business running smoothly. Cybersecurity must be a top priority and not an 'out of site, out of mind' issue. The trust of your employees and customers and your reputation are at stake.

REFERENCE MATERIALS

- For more information reference the following websites:
  - cisecurity.org
  - usa.gov/online-safety
  - fbi.gov/investigate/cyber

- For information regarding Virginia law and the code regarding the 'breach of personal information' –
  - https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

The Virginia SBDC Network is funded in part through a cooperative agreement with the U.S. Small Business Administration, George Mason University, and local host institutions. The Virginia SBDC is nationally accredited by America's SBDC. All opinions, conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of the SBA.

CYBERSECURITY – THE GROWING THREAT TO SMALL BUISNESSES

Prepared by Chappell Business Strategies for
Blue Ridge Crossroads SBDC and Twin County Chamber of Commerce