EAG-060 8/20

# SIMPLE STEPS FOR SMALL BUSINESS CYBERSECURITY

Blane Counsil[1] and Rebekka Dudensing[2]

Small businesses employ almost one-half of the US workforce and anchor many local economies, especially in small towns and rural areas. Most small businesses have traditionally served local markets, but today's consumers can easily purchase a product online from halfway around the world and have it delivered to their doorstep. In the 21st century's online economy, an online presence is essential to build your brand, enhance sales, and promote your products and services.

This online presence brings a new series of threats to small businesses, proprietors, and customers. Customers place their trust in businesses when paying online or in person. A Nationwide Insurance survey found that 45 percent of small business owners had been victims of cyberattacks. However, small adjustments in business practices and information management can have a significant impact on a business's cybersecurity.

By incorporating physical and cybersecurity controls, small businesses can protect their assets as well as the clients they serve from breaches in confidentiality, losses of informational integrity, and issues with access to critical data. Every one of your customers relies on you to protect them and mitigate their risk of having their information stolen, so here are a few tips to help.

## PHYSICAL AND ENVIRONMENTAL PROTECTION

When most people think of cybersecurity, they think about computers and technology. In reality, cybersecurity includes many components. The physical security of information is often overlooked, but barriers to accessing information may deter potential criminals. Criminals are typically opportunistic individuals, meaning that they are often looking for the easiest target to yield the highest reward. The reward they gain from committing their crime has to exceed the risk of getting caught. Therefore, criminals often choose soft targets or targets of opportunity.

Simple deterrents can prevent your business from becoming a target of opportunity. For starters, putting exterior deterrents, such as fences, around your business and adding quality locks on your external and private doors can go a long way in preventing criminals from gaining access to your business and, ultimately, access to your files and technological systems. Physical protection also involves ensuring that every door is locked at the close of business before the property is vacated. As mentioned earlier, preventing your business from becoming a soft target can go a long way in deterring criminals. Another way to protect your business is to ensure that access panels to main computer servers are locked and cannot be easily opened. Each of these simple steps significantly increases your resistance to physical attacks.

A gate outside of a business protects technology and other assets inside. *(Image courtesy of Blane Counsil)*

Another high-risk situation small businesses often overlook is taking secure payments over the phone. This method of payment may require you to repeat credit card information back to the customer. When doing so, it is best to be in a secure location, such as an office with the door closed. If this is not possible, be aware of the individuals around you and take steps to prevent other employees or customers from overhearing and stealing private information. If you cannot

[1] Graduate Student in the Department of Agricultural Economics
[2] Associate Professor/Extension Economist

safely repeat the payment information, ask the customer to repeat the information a second time to verify it is typed or written correctly. When possible, direct customers to a secure online payment system.

## ACCESS CONTROLS

A simple step to protect yourself and your small business is to limit who has access to critical information within your small business. There are many ways that small businesses can accomplish this task. For starters, if your business has a computer with customer information, be sure that there is adequate security on the device. This security can most commonly be achieved in the form of login credentials for the computer itself and the online system. Only certain employees within the organization should have access to these login credentials, based on the information they need to complete their job duties. By limiting the number of individuals within your organization that can access your sensitive information, you greatly reduce your risk of theft and data integrity becoming compromised. Only trusted information technology (IT) staff and key managers within your business should be granted administrative privileges.

Login

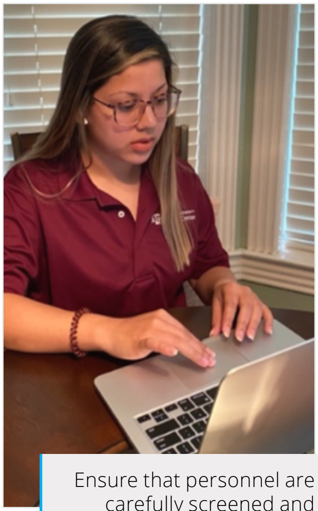
Each employee should have his or her own unique username and password. Employees should be trained in and follow good cyber practices. Never, under any circumstances, should anyone in the business openly display usernames or passwords. Shared or open credentials may seem like the easiest way for multiple employees to access your system, and it may assist you if you struggle to remember passwords. However, displaying or sharing your password undermines the security that you have set up to protect that system and the information that exists on it. If there is a security breach, unique credentials will help you track the source and remediate the damage.

## PERSONNEL SECURITY

One of the greatest challenges facing a small business is staffing. Many small businesses rely on minimum- or low-wage labor to conduct day-to-day operations. Precautions must be taken to properly screen employees prior to hiring in order to mitigate your risks. Ensuring that staff are carefully selected and adequately screened can prevent undue risk for your business in the future. Background checks and personal credit score reports are the most common forms of personnel screening and help inform employers of the risk that they are subjecting themselves and their business to by hiring each employee.

**People are the weakest link in any security plan.**

The screening of employees is not just limited to employees with access to customers or data. For example, individuals who conduct cleaning services and maintenance should be screened as well. You can also request that your service contractors screen their employees. Individuals who are brought in to work on your networks or devices should not be left unattended while working within your business. In addition, individuals who do not work in your organization should not be allowed to freely enter your business workspace without being questioned or stopped.



Ensure that personnel are carefully screened and follow security practices. *(Image courtesy of Blane Counsil)*

Personnel screening should also establish clearly defined roles and responsibilities for each member of your organization. Employees' roles indicate the devices and technology they should be using. Defining employee roles can prevent misunderstandings and foster accountability between peers as well as between employees and managers.

## PROTECTING ADDITIONAL INFORMATION AND ORGANIZATIONAL IMAGE

We often see social media as a valuable resource for our businesses and organizations. However, most individuals forget that the platforms we share our information on can be exploited and possibly even portray the wrong image for ourselves and business. Additional personnel security issues that are becoming more frequent are social engineering attacks. People are the weakest link in any security plan; therefore, they are the easiest part of an organization to exploit. These direct attacks are often primarily done through phishing attacks, which are a form of social engineering where emails and websites maliciously solicit information from users by building relationships or posing as a trusted organization. Not only are email and pop-up website attacks becoming more frequent, but phishing attacks are also occurring on varying platforms and media, such as phone calls and social media. Employees must remain vigilant of suspicious links, websites, and information requests in order to prevent these forms of attacks.

Social media allows us to post images, share information about sales, and follow trendy hashtags. It can also be a treasure trove of information for criminals looking to exploit your personal data. Often, we inadvertently share information such as birthdays, trips, family pet names, and nicknames, all of which can be leveraged by criminals to gain access to your home, business, or sensitive information. Shared photos are often the greatest culprit. Our backgrounds may have information such as addresses on packages, serial numbers on devices, family photos, or even sensitive documents that we do not realize are visible. This information can then be used by criminals to build trust and launch more successful phishing attacks. Businesses may inadvertently make themselves targets for thieves by posting when they receive large shipments of valuable goods or revealing that there is a safe located in your business if it is shown in the background of a photo.

Not only can social media photos expose your business to threats from criminals, but they also can offend potential customers. You may not care what type of clothing an employee is wearing or what logos are present on their attire, but if they are present in an image displayed by your organization, their clothing and conduct may be perceived as a reflection of your values. Not only must photos of employees be monitored, but photos taken with customers should also be reviewed to ensure they reflect your organization's values and brand image. Images posted with your product or organization's branding can reflect positively or negatively on your organization.

Overall, social media can serve as a valuable tool to spread information about your business or organization. However, if measures are not taken to limit your exposure when posting images and content, it can leave your business vulnerable to attacks and exploitation.

## CONTINGENCY PLANNING

Disasters and unexpected events can leave small business computer systems corrupted, destroyed, or missing. It is essential to conduct a full backup of all data used within your small business at least once a month. However, it is highly encouraged to do so more frequently. No one knows when a storm, flood, fire, electrical short, or theft will destroy their system. A full backup of your information will allow you to quickly return to providing service to your customers with minimal information loss.

Plan to back up your data in case of an emergency.
*(Image courtesy of Blane Counsil)*

Backups can be stored on the cloud, an off-site server, external hard drives, etc. Carefully research backup options to ensure the method you select is safe, reliable, and the best option for you and your organization. This backup should then be stored in a safe, off-site location to ensure its availability if an unfortunate event does occur.

## NETWORK SECURITY

Firewalls are often the first image that comes to mind when someone mentions network security. Firewalls deter individuals from freely moving in and out of your devices and network and accessing your information. Many devices possess factory default firewalls, but they may require the operator of the device to activate them. If devices do not have a factory firewall, there are several free firewall software options that can be downloaded online. Properly researched antivirus software complements a firewall by detecting and removing malware and other suspicious files in your system that may destroy stored data.

Another way to prevent unwanted traffic is to ensure that your wireless router is properly secured, encrypted, and hidden. Businesses often provide patrons with Wi-Fi passwords to their networks as a customer convenience or in order to conduct business. Patrons should be provided an alternative network that does not house the primary information for the business. The primary network should be password-protected, and only employees should have access. Access to the primary network should never be granted to patrons. Also, the Wi-Fi router itself should be stored in a secure location where it cannot be tampered with. Hiding the device in a locked cabinet or on a shelf out of reach can prevent individuals tempted to manipulate the device.

Protect your wireless network and router.
*(Image courtesy of Blane Counsil)*

Home wireless networks usually are less secure than business networks, which poses an indirect threat to small businesses. Small business employees and managers may be issued work devices that may then be taken home. Inadvertently or intentionally, these devices are then able to connect to unsecured home networks, leaving sensitive data vulnerable. Home networks may have insufficient passwords, or the password may be openly given to all guests within the house. Individual's devices may create unwanted traffic on the network and expose the company device to a host of threats while on the network. To avoid this situation, individuals who take work devices home should ensure that they are disconnected from home networks, or that home networks are properly secured prior to the use of work equipment.

Only accessing secure websites can also significantly enhance network security. Website addresses containing a padlock or lock icon within the web browser let the user know that they are operating on a secure website that uses encryption to prevent outside sources from modifying data exchanged between the web browser and web server. This is the safest way to access the web and maintain a secure network.

## CONCLUSION

No matter what form of cybersecurity you choose to implement to protect your business and the clients that you serve, there is one thing that you should remember:

**Your security is only as reliable as the individuals that you entrust to operate within your security features.**

No matter how many firewalls, gates, or passwords you put in place to protect your systems and information, if you or your employees choose to ignore established security protocols, implemented security features are useless. Using common sense and maintaining awareness of privacy goes a long way toward ensuring cybersecurity. Remember that you are constantly working to maintain your customers' trust.

## FOR MORE INFORMATION

For more information and specific details regarding steps that can be taken to further protect yourself and your business, please feel free to consult the National Institute of Standards and Technology document provided in the link *here*. You may also consult the Texas A&M Cybersecurity Center webpage for additional resources and publications regarding cybersecurity by clicking *here*. The Federal Communications Commission published a document further detailing many of the topics discussed *here*. Finally, the Texas Department of Information Resources has great information that can be accessed *here*.

Texas A&M AgriLife Extension Service
Community Economic Development, August 2020