

# DATA ASSURED

Presented By:



# Cyber Workbook

In Partnership with:



Small Business  
Development  
Center



# Executive Summary

Technology is a double-edged sword. On the one hand, it creates productivity and business opportunities never seen before. On the other it can allow remote users access to an entire business, enabling them to take it down with a few keystrokes. With fewer employees than ever, technology can allow small businesses to directly compete with medium and large firms. Federal, State, and Industry regulators have decided that the threats posed by malicious actors in cyberspace must be addressed. For the small business owner, responding to new regulatory demands to protect business and client data is essential. This is not just a matter of following the rules, nor illustrating to your clients and customers that their safety and security matters, but it is a matter of outright survival of your company should it experience a breach. Many businesses cannot afford the legal, regulatory, and forensic hassles that accompany a breach of systems exposing client or internal information, let alone the loss of trust from a client or customer base.

**For the small businesses of the world, security is vital to survival.**

The threat beyond regulatory concerns is significant. The Criminals, Competitors, Hacktivists, and State-Sponsored Terrorists are targeting you for several reasons:

- Do you have a relationship or dependency with a larger company who may be a target? You could be an easy access point along their path.
- Are you a retailer, health care provider, or financial firm who utilizes credit card payment and or aggregates client information? The type of business you are in may increase your risk profile and attack surface.

**Bad actors believe smaller companies with less resources for both physical and digital security are a ripe target for attack. Let's prove them wrong together.**

Security does not have to mean reduced productivity and increased operational costs. In fact, it can mean quite the opposite. With strong security, Bring-Your-Own-Device and other relaxed work policies can allow employees to be far more productive, increasing efficiency and saving on IT costs.

**The increased productivity from effective security can far outweigh its cost.**

Given this landscape of both business and regulatory threats, what can, and should a small business owner do? It is paramount for the small business owner, in the absence of vast personnel and funding, to have precise controls and solid policies in place.

**The Data Assured program can help you keep it simple and effective.**

## Purpose

The Data Assured Cybersecurity Workbook is designed to provide the small business with a guide for creating a Written Information Security Program (WISP). Seemingly complicated at first, the essence of a WISP defines a reasonable program for handling cybersecurity within your organization. You'll need to review written items on a regular basis, but beyond that, maintenance of a WISP is a simple process that grows with your business.

This document will guide you through each of the sections of your company's WISP and leave you with a working program. This program will require adjustments going forward, and you may also wish to expand it based upon your business's unique circumstances. It is key to note that this workbook is just a starting point to develop your cybersecurity measures.

It is meant to guide your thinking and help you develop a security mindset. You must make security your own and live it day in and day out at your business.





## Intended Audience

The Data Assured workbook is primarily designed for the small business that typically does not have a Chief Information Security Officer (CISO) or enough headcount to form cybersecurity committees.

Some of the advice and pointers offered in this workbook will have applicability to solopreneurs who have little to no actual infrastructure and very little in the way of retained data.

For the small company that has some headcount but maybe isn't sure where to start, we offer that all of the pointers contained herein will benefit you if applied to your daily business. As your business will undoubtedly grow, you will be in a good place to help your employees understand and embrace their role with respect to cybersecurity.

For the medium company, you may find many topics here that have not been thoroughly explored and acted upon in your day to day business. This can serve as material to train employees on the importance of cybersecurity, and ensure the security of your operations.

On the opposite end of the spectrum, large companies may find some of the information contained herein to be of an introductory nature. This workbook can be used as a communications tool within your organization. It is designed to be simple enough that you don't have to be an "IT Person" to understand it. You can simply define all of the points we list herein for your firm. Then take the opportunity to explain the work that you're doing to your senior managers. Let them know what's going on in the company. If you find that there are some items here that you can't answer easily – you have just discovered items that will help you further secure your business!



One caveat here for all businesses – as we have said, this workbook is a starting point that you can use to help define your cybersecurity practices. It cannot prevent breach on its own nor will it be able to answer specific questions about your network or your legal liability. We recommend, if you have questions that are highly specialized and unique, you consult a security/IT vendor who may be able to help you, or in the question of liability, a qualified lawyer.

# What is the Basis of This Workbook?

In 2013, the Federal Government formally addressed the issue of cybersecurity in the wake of several high-profile, front-page news breaches. The outcome of this was the Framework for Improving Critical Infrastructure Cybersecurity (or Cybersecurity Framework, the "CSF"), published by the National Institute of Standards and Technology, a division of the Commerce Department.

The complex naming conventions belie the actual simplicity of what it attempted to do. A framework is really just a list of suggested activities that your company can think about as a form of guidance for how to address cybersecurity.

## Pretty simple, right?

Since the CSF was published in February of 2014, almost every significant regulatory agency has referenced it, typically in light of being an effective starting point for addressing cybersecurity. The CSF itself has gone on to enjoy success in businesses of all sizes and across all industries, because of its flexibility. When it first published the Framework, NIST stated clearly that it was to be adapted, expanded, contracted, and used as a form of guidance.

The Data Assured workbook and, by extension, your cybersecurity practices are based upon the 5 central concepts of the NIST Cybersecurity Framework:

### STEP 1 IDENTIFY



Can you identify the assets and systems that are susceptible to cyber threats?

### STEP 2 PROTECT



What basic practices do you have in place to protect your systems and assets?

### STEP 3 DETECT



What do you use to detect someone or something malicious?

### STEP 4 RESPOND



How will you deal with a breach if and when it occurs?

### STEP 5 RECOVER



How will you restore your business back to normal after a breach?

# Using this Workbook

In order to make this process as user-friendly as possible, we have included blank spaces for you to fill in your information and create a customized Written Information Security Program. In addition, we have provided a template policy on the Montana SBDC website where you can go to download and type in the information as you work through this plan.

Keep in mind that the information that you fill out in this workbook is sensitive information. It's designed to highlight your strengths but also weaknesses. We urge you to keep the answers to these questions within your organization so that they do not fall into the wrong hands and ultimately leave you vulnerable to attack.

## NOTE:

This workbook is general in nature and attempts to provide best practices for all businesses. Your business may have specific requirements if it retains certain types of information, such as Payment Card Information (PCI) and/or Personal Health Information (PHI). Make sure to address these information specific requirements as well as the items contained herein.

If you hit a stumbling block somewhere along the way, reach out to us at:

### Montana SBDC Lead Center

301 S Park Ave  
Helena, MT 59620  
(406)-841-2747

### Montana SBDC Locations

Billings SBDC .....	(406)-254-6014
Bozeman SBDC .....	(406)-587-3113
Butte SBDC .....	(406)-533-6780
Great Falls SBDC .....	(406)-750-0314
Havre SBDC .....	(406)-399-1557
Helena SBDC .....	(406)-447-6376
Kalispell SBDC .....	(406)-756-3836
Miles City SBDC .....	(406)-874-6168
Missoula SBDC .....	(406)-243-4770
Wolf Point SBDC .....	(406)-653-2590



**Email**  
[MTSBDC@mt.gov](mailto:MTSBDC@mt.gov)



**Website**  
[www.SBDC.MT.gov](http://www.SBDC.MT.gov)

STEP 1  
**IDENTIFY**

# Who, What, Where, and When?



### Why Do This?

Identifying the threat is the most fundamental part in protecting against it. Specifically, identifying all the pieces that make up your network that are susceptible to attacks gives you the advantage you need to protect and/or recover.

### Identify Who is Responsible for Cybersecurity

Here is the simplest starting point. Who makes the calls when it comes to the security of the company? If you are filling out this workbook for a small company, chances are it is you, but there may be someone else who takes the security lead.

Name of Person Responsible for Cybersecurity:

### Identify Outside Consultants

Is there anyone outside of your company that you might turn to in order to help with your cybersecurity or enacting protection?

Name of Outside Consultant (If Any):

### Prioritization

As you work through the next few items, try to prioritize them in terms of criticality. What do you really need for your business to function, and what is a convenience? This thinking will help you consider what you should restore first in the event of a disaster, and what you may want to remove to decrease complexity.

## Identify What Data You Collect & Where You Keep it

This is the root of a cybersecurity policy. What data do you maintain that could be useful or valuable to a bad actor?

Data can be stored on your devices (like a laptop or external storage devices), in cloud storage (like Google Drive), or in a service (like Quickbooks). Make note of what security requirements are used to access this data (passwords, multi-factor authentication, IP whitelisting, etc.)

Examples include:

- Personal Identifiable Information or PII (SSNs, DOBs, etc.)
- Payment Card Information (Credit Card Numbers)
- Personal Health Information
- HR Records that could contain Bank Account Information
- Business Plan Documents (Bank Statements, Taxes, etc.)
- Proprietary Schematics, Patent Applications, etc.

Our Sensitive Data and Where It's Stored		Date:
	Data Type	Location
Ex:	Credit Card Numbers	Stored in Quickbooks Desktop version on work computer in office.
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		



## Identify What Devices Need Protecting

What devices are you using that could be used to compromise your sensitive data? Fill in the below table to create an inventory of devices that interact with sensitive data by any means. List every single device you can think of. Chances are the more specific the purpose of the device, the harder it is to protect and update (eg: printers).

Hardware Inventory			Date:
Desktops	Laptops	Phones and Tablets	Other (printers, routers, NAS, etc.)
-----	-----	-----	-----
-----	-----	-----	-----
-----	-----	-----	-----
-----	-----	-----	-----
-----	-----	-----	-----

## Identify What Operating Systems You Are Using

Windows tends to be the most targeted, yet Linux tends to be the most exposed to the open internet. Make sure that all of your operating systems are patched, updated, and supported. For instance, support for Microsoft Windows XP ended in 2014, Windows 7 support ended Jan. 14, 2020. Similarly, Apple typically only creates security updates for the three most recent operating systems, with that being said macOS 10.13 or earlier are no longer supported. Your business should not be running unsupported versions of operating systems. Check to make sure all devices are updated to the current version. This includes mobile devices as well. If your device does not support the most updated version, it is time for an upgrade. Use of an unsupported or unpatched device is asking for a breach.

*Please take some time to write down what types of operating systems you currently use and for which devices it might be time for an update. Be careful to make note of the Operating System on each individual device*

OS Check	Date:
All Systems Supported	
-----	
-----	
-----	
All systems supported but the following need to be updated/losing support soon	
-----	
-----	
-----	
Non-Supported System(s)/Device(s) In Use	
-----	
-----	
-----	

## Identify What Software You Are Using

Just like operating systems, software has supported versions and security updates. Backup and storage software that is out of date could allow bad actors access to your data. Old versions of password managers could leave your passwords exposed. It is vital that you keep the software used for business updated just like you would with operating systems. An operating system could be fully patched, but old software could allow remote access.

*Please take some time to write down what software you currently use and check if it might be time for an update. Be careful to make note of the software on each individual device*

Software Check	Date:
Up to date software	
Can be updated or losing support soon	
Out of date and unsupported by software publisher	

## Asset Management

Earlier you created a list of all the physical devices that your business owns. What you need to do now is expand that and record where that physical device/asset is and who it is assigned to. This way in the event of a breach all devices are accounted for. This will also help investigators track down the cause of the breach. The last thing you need is an old laptop that hasn't been updated in years sitting on your WiFi. That can give attackers the opportunity they need to gain access to your more secure devices.

## Technology Usage Policy

As your company grows and you begin to add employees you will need to make sure you have a technology usage policy. This policy spells out what employees can and can not do on company owned technology (ex: internet usage, checking emails, etc). It also explains what actions you as a business can take against an employee in the event they break the rules.

Does your company have a technology usage policy?

Yes                      Date Last Updated: .....

No

## Where Is Your Business In The Supply Chain?

As a small business owner, you need to know where your business falls in the overall supply chain to understand the importance to being cyber secure. You are only as strong as your weakest link and if you are doing business with larger corporations you very well could be their weakest link. This is why it is very important to make sure you are doing what you can to keep your information safe.

STEP 2  
**PROTECT**

# What Are You Protecting?



You have now identified the data that you keep. Now, we are going to go through the specific ways you can protect that data. Along the way, we'll offer tips and some industry best practices for securing your information and how employees access it. These best practices should extend into private life as well.

## How Do You Manage Identities?

User Identities are a means of determining who is accessing what data when. Role-based access also provides you protection by preventing access to unauthorized data. Do users use the same account for all services and systems? Or is each login unique?

*Please take some time to write down how you currently keep track of user identities. Be careful to make note of who has access to the User Identity information and who has the ability to alter them.*

### Account Check

Date:

User Identities accessible to only one individual  
(Computer passwords, emails, etc.)

.....

.....

.....

User Identities accessible to multiple people. (Ex: shared accounts)

.....

.....

.....

List areas where anyone could gain access to accounts, or places where User Identities currently do not exist

.....

.....

.....

## NOTE:

Remember, if you use a personal system for logging in or accessing your company data that you should also have separate usernames for that system as well. Private computers with multiple users can be more susceptible to malware or viruses than dedicated business machines. If you use a personal computer that is shared with other members of your family, create a different username and password for business purposes and keep it distinct and separate.

## How Secure Are Your Passwords?

The term 'Password' is not the best. It should really be 'Passphrase'. That alone should tell you a lot about password strength. Using passwords that have association with yourself, like a maiden name, birthday, favorite food, etc. are recipes for disaster.

The key to a strong password depends on two things: character space and length. Passwords with only letters take a fraction of the time to crack compared to passwords of the same length with numbers and symbols.

If your systems and software can support the use of passphrases, essentially very long passwords that are easily memorized but would be impossible for a machine to guess, go ahead and use them. They make your system more secure than a shorter password and can be easier to remember than a jumble of characters and symbols.

The evolution of creating a good passphrase is as easy as 1-2-3:

1. Create Original Passphrase "Pizza is my favorite food"
2. Ensure Passphrase Usability: "pizzaismyfavoritefood"  
(Removed spaces)
3. Strengthen Passphrase: "P1zz4l5Myfav\*r1teF\*d"  
(Capitalized first letter of each word, replaced non-caps letters with numbers where possible, replaced o with \*)

This process will allow you to create a strong passphrase for every system, device, or service you use, thus protecting your business. As you can see, creating even a short passphrase like this can serve under many password requirements where a longer passphrase is not allowed.

When forced to use a password, the following guidelines should ensure that you keep yourself as secure as possible:

- **Complexity:** A minimum of 3 of the following 4: Upper-Case Letters, Lower-Case Letters, Numbers, Symbols
- **Length:** At least 12 characters
- **Change Frequency:** Passwords are changed every 180 days at least, more if required by specific mandate (PCI-DSS, etc.)
- **Reuse:** No reuse of the last 6 passwords
- **Lockout:** 10-minute lockout after 8 unsuccessful login attempts (if possible to customize)

Biometrics (ie. Fingerprints, Face ID) provide a great opportunity for using a very complex passphrase, while also keeping it easy to login every time. Mobile devices now use 6-Digit passcodes and biometrics by default, and most support passphrases as well. Using a passphrase with a mobile device, and then using biometrics to log in between reboots allows for immense security with ease.

#### Password Check

Date:

- Complex Passwords Required
  - Upper-Case Letters
  - Lower-Case Letters
  - Numbers
  - Symbols
- Length Standards Met (12 Characters Minimum)
- Change Frequency Every 180 Days or More Regularly
- No Reuse of Last 6 Passwords
- 10 Minute Lockout After 8 Unsuccessful Attempts
- Use of very long passphrases possible
- Mobile Devices Secured by a 6-Digit PIN at Minimum
- Mobile Devices Secured by a passphrase
- Additional Controls: .....

### Inactive Device Locking

By default, devices will fall asleep and lock themselves after a certain period of inactivity. While you should always lock/logout of a system or device when no longer in use, humans aren't perfect, and mistakes happen. Reducing the time it takes for a device to fall asleep and lock can save your business from unauthorized physical access.

### Going Further - Passwords

Entire books have been written on password construction and management. While the notions that we recommended are currently industry-standard, you have to make sure that your policy for changing passwords isn't creating vulnerabilities. If you or your employees are having a hard time remembering passwords that you have to write them down, email them, or store them on your phone, you'll need to reassess and consider using a password manager or other form of authentication.

#### NOTE:

Your capabilities for enforcing these controls will vary depending on your systems and services. For advanced businesses with an IT staff you may be able to use ActiveDirectory in a Windows environment, or some cloud-based systems will let you control these details. For small businesses that don't have access to such tools, you may need to rely on training your employees and manual reminders to change passwords.



## Data Encryption

Encryption is something that is commonly overlooked, yet vital to secure data handling and storage. Some basic examples of encrypting data are as follows:



### Databases

Databases that contain sensitive information, including PCI, PHI, or PII should have some form of encryption in place. This doesn't have to be the entire database, as it could cause performance issues, but the columns of data that are deemed to be sensitive (such as Social Security numbers) should be encrypted at the very least.



### Storage on Servers

Server storage should be encrypted. This will ensure that the drive is inaccessible should it be physically removed or stolen.



### Storage of Laptops

Laptops are susceptible to theft or loss. All modern operating systems will allow for full disk encryption, which should be used. With Apple laptops, FileVault is free and easy to use. With Windows enterprise, BitLocker can be used for full disk encryption.



### Storage on Mobile Devices

Mobile devices from Apple are automatically encrypted when a pin number or password is put in place. Android devices require an additional setting to be switched on to fully encrypt those devices. Make sure your employees turn encryption on if they are accessing company data from their Android devices.



### Cloud Storage

Many services store your files encrypted on disk. For the most part this can be enough. However, if a bad actor is able to gain access to your cloud storage, they could get at everything. An advanced step to increase your data security is having a separate system for encrypting your files before they get to the cloud like boxcryptor or rclone/rsync.



### Email in Transit

Email can be encrypted in transit through the use of SSL/TLS, which is enabled by default on most mail servers. It will only work if both the sender and the recipient have SSL/TLS encryption enabled, so it is a "best efforts" process. This encryption will only protect email from being intercepted when in transit. Services like Gmail, iCloud, and Microsoft Outlook are encrypted by default.

### Encryption Checklist

Date:

#### Our Company Encrypts The Following:

- |   |  |
|---|--|
| <input type="checkbox"/> Database           | <input type="checkbox"/> N/A                                 |
| <input type="checkbox"/> Server Storage     | <input type="checkbox"/> N/A                                 |
| <input type="checkbox"/> Laptop Hard Drives |  |
| <input type="checkbox"/> Mobile Devices     | <input type="checkbox"/> N/A (devices not used for business) |
| <input type="checkbox"/> Email in Transit   |  |
| <input type="checkbox"/> Other .....        |  |

## Role Based Access Control (RBAC) of Data

If you are a solopreneur, you probably don't need to implement a data segregation plan. However for even the smallest companies, putting your data into various places that are restricted to only those who need the information is a great idea.

In order to properly segregate data, you need to first determine what data you collect. The "identify" step you already completed on page 8 gives you that data. Now you should determine who needs access to that data.

Take your time and think through this process, because it can be very tempting to just say "everyone needs everything". This is seldom the case – especially with HR information including payroll. Below is a numbered list that correlates with the identify section of this workbook, write down who within your company needs access to that data. Set up folders or other permission methods and restrict access to those folders.

Data Segregation List:		Date:	
	Who has access:		Who has access:
EX:	Accountant, Dan from billing, Mary in HR		
1		11	
2		12	
3		13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

## Multi-Factor Authentication

2FA, or Two-Factor Authentication is one of many forms of MFA (Multi-Factor Authentication). 2FA greatly increases account security and should be used wherever possible. 2FA can be done many ways, most online services currently support text message verification and/or token verification. Text message verification is simply getting a text from the online service with a code to verify your identity once you have entered in your password.

Token verification can come from multiple third party apps (ex: Google Authenticator). The apps link to your online account and when you login with your password, it will ask for the code generated by the linked app. This method is much safer than text messages because the codes change every 30 seconds or less.

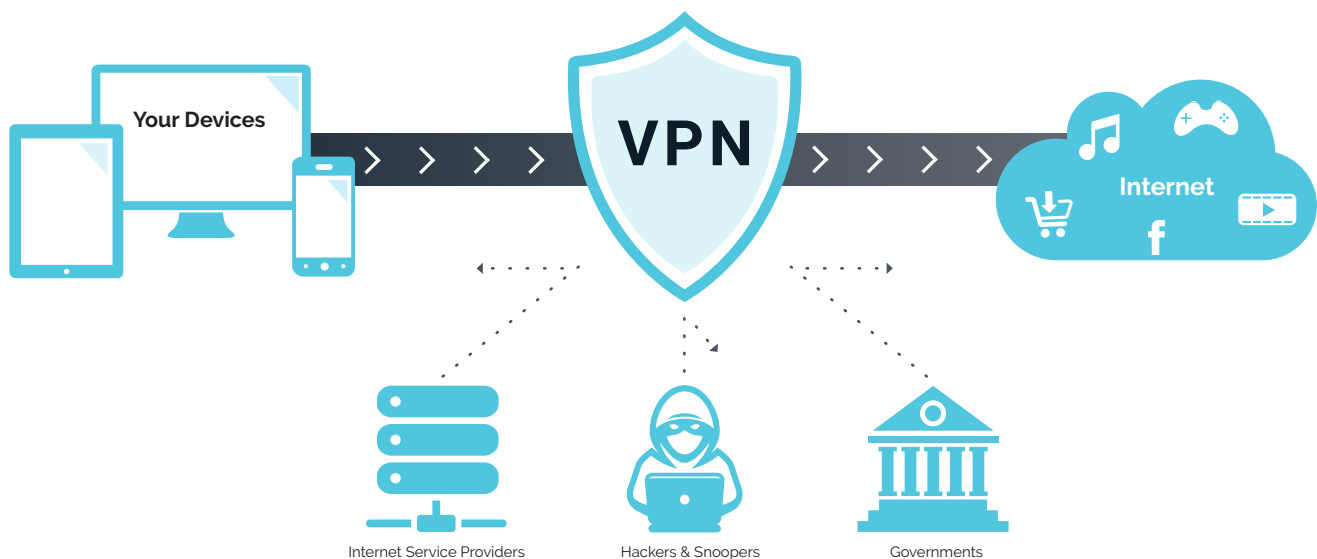
In some online services, administrators can mandate 2FA or MFA for all users and we highly recommend you do so. If backup codes are given, make sure they are stored in a safe place whether they are stored digitally, physically, or both. Your account can become unrecoverable if you lose access to your app and you do not have the backup keys.

## Virtual Private Networks (VPNs)

Using public WiFi to run your business should be avoided at all costs. However we understand that at times you need to check your bank information or need to send some emails while away from your business network. This is where Virtual Private Networks (VPNs) come in handy.

Public networks are not very secure and allow others to intercept your data. A VPN, whether it be an app on your mobile device or software on your computer, routes your data through servers located elsewhere in the world. In other words it masks your identity, making it look as if you are using a device from somewhere else in the world. This is similar to how a company might use a VPN to allow employees to use their work computer as if they were on the company's network, even while they're on the road.

An important advantage with some VPN applications is that it can create a dedicated encrypted tunnel allowing your data being sent to be secure no matter the WiFi network. Before you download a VPN application, you should know that there are benefits and risks. Not all VPNs encrypt your data, so make sure to do your research to pick the best one that works for your business.



## Employee Training

If your business has employees, you should train them regularly on cybersecurity best practices. They should be provided training upon hire and annually, and also on an as-needed basis. If you have an incident at your firm that highlights poor cybersecurity choices, you may want to spend some time training your employees on how to better react to cyber threats. There are many free resources available for cybersecurity training. A couple good places to start are:

SANS Information Training – [www.sans.org](http://www.sans.org)

OPEN DNS Phishing Training – [www.opendns.com/phishing-quiz/](http://www.opendns.com/phishing-quiz/)

*If you are writing down a policy to go with your plan, try the following language:*

"Personnel are provided training regarding information security practices upon hire, annually going forward, and as necessary based upon events at our company."

## Phishing

In cybersecurity, the human element is the weakest link. From a one-person business to a large organization, they are vulnerable all the same. The most common and dangerous attack methods that exploits human vulnerabilities is phishing. It is a simple and effective method that affects most businesses. It just requires the attacker to get one person to click on something they should not have.

Phishing is the art of getting people to share sensitive information. Victims receive a malicious email or text message that looks legitimate, from a person or organization they trust (e.g. coworker, bank, government, etc.). It typically conveys a sense of urgency and requires the person to act fast by clicking on a link or opening an attachment.

If victims click the link, they are sent to a fake website that looks legitimate. There they are required to enter their username and password. If they comply the attacker will collect their credentials and can use it to steal identities, pilfer bank accounts, and sell personal information. The same goes for email attachments. By opening the attachment, it downloads malicious code to the victim's computer granting the attacker remote access to the machine.

## Types of Phishing

As with real fishing, there's more than one way to reel in a victim:



### Email Phishing

This attack method is the most common of all phishing methods because it is the easiest and requires the least amount of work for the attacker. The emails are designed to get you to click a link or open an attachment. The emails are typically riddled with spelling mistakes, have very little content, and are generic in nature.



### Spear Phishing

Takes regular email phishing and customizes it slightly. Typically it is targeted to one individual versus mass amounts of people. Attackers have your name and some basic information about you. These attacks are harder to spot because it is customized to the individual.



### Whaling

Yet another advanced layer of phishing. The attacker is more invested in a particular company and has typically already gained access to some low level employees and is now trying to target a more high profile target such as a CEO or CFO.



### Smishing

SMS phishing utilizes your mobile device rather than your email to phish you. This is when you receive text messages from random numbers with a link and typically the prompt is asking you to verify your account.



### Vishing

Voice phishing are the phone calls you get that try to convince you there is something wrong and that you need to pay them money to fix it. This can be calls from attackers claiming to be IRS agents, computer repair people, or car warranty agents.

## NOTE:

As a small business you are more of a target than a larger corporation and the reason being is because you are the ticket into a larger corporation. Maybe you are a restaurant using a POS that stores information on a high level CEO. Maybe you are an HVAC repair company that does repairs for major businesses. No matter the industry, no matter your size your small business is a target.

## Mobile Devices

In today's society almost everyone has a smart phone and it has become a crucial business tool. If you do any type of business transactions through a smart phone you need to consider protecting that device and having a policy in place for any employee that uses their own device on your business network.

Any device that connects to your business network or has access to your businesses data needs to be protected. It does not matter if it is your own device or your employees personal device. At a very minimum you as the employer should mandate all mobile devices have some type of password protection, encryption turned on, and a security app installed.

## Mobile Device Management Software (MDM)

With small businesses trying to manage their costs they have decided to go down the route of BYOD (Bring Your Own Device). This unfortunately leads to a lack of control of the devices.

This is where MDM software comes into play. The software is installed on a employees phone. The software allows you as a business owner to mandate certain security features be turned on to protect your business network. Some added benefits are that it also allows you to remote wipe the device in the event it is lost or stolen. Not to mention it allows you to track OS and App configuration making inventorying your hardware that much easier.

## Business WiFi Security

You pretty much can not transact business today without the use of the internet. Like we already explained in the VPN section, you never want to transact business over a public WiFi network. This section details what you as a small business should do to create a secure business network.

For starters you will want to consider getting a business level internet package from your Internet Service Provider (ISP). Typically the speeds are faster and come with a better level of customer service. Not to mention that some ISPs provide stricter security measures around their rental modems and routers then typical residential modems and routers.

Secondly you will want to decide on if you are going to provide free WiFi to customers. If you are a business that does not need customers to have WiFi then make sure access to guest WiFi is turned off on your router. If you are a coffee shop or something of that nature and want to offer free WiFi you want to make sure it is setup in a way that it is on its own secure channel and does not allow attackers to tunnel their way into your business network. Newer routers come with features to control guest WiFi. You also might want to consider a policy notice for anyone connecting to your free public WiFi.

In addition to securing guest WiFi you will want to change the admin password of your modem and router. This password is usually different from your actual WiFi password and grants you access to the settings of your modem and router. In the past router manufactures left the username and password the same. With most rented equipment from your ISP today come pretty secure but you will want to verify if you own your own router or modem.

Lastly, a more advanced layer of protection would be to create users on the WiFi so that every person connecting to the network has a different username and password.

### WiFi Check

We have the following:

- Business WiFi
- Offer Public WiFi
  - It is protected
- Changed the default system password
- Separate WiFi logins for all



## STEP 3 DETECT

# Recognize if Something is Going Wrong, and Stop it



### Antivirus / Antimalware

Every business needs antivirus/antimalware software. You need these to help protect your computers and mobile devices from malicious programs that may be present on your systems. All PCs running Windows 10 have a native antivirus software installed called Windows Defender, which if turned on, does a decent job of protecting your computer however it is not to replace actual software designed to protect you. Apple devices do not have such software, instead they trust the user knows what he/she is doing with yes/no prompts when opening or running files.

Antivirus works by storing known signatures (fingerprints for files) of malicious code and files, it then scans your system to check if any files on your system match those malicious signatures. If it finds those bad files it either quarantined the file or deletes it from your system completely. The antivirus/antimalware is only as good as its signature base and since new viruses and malware is found daily that is why we urge you to keep the software up to date.

Most modern antivirus/antimalware software offer total protection. Meaning they bundle the softwares together in one convenient program. This is important to know because in some circumstances if you have two separate softwares such as one for antivirus and one for antimalware they may end up detecting each other as malicious and can cause issues.

One myth circulating out there is that Apple products are more secure than Windows PCs meaning you do not need software to protect them. That is not the case anymore. The reason being, Apple products used to be more secure than Windows. However, Windows machines dominated the workplace. As an attacker it was more lucrative to spend time developing malicious codes that would affect the majority of computers. With the development of Windows 10 however, security has come a long way and brought Windows to the level of Apple. This means now attackers have the same level of difficulty to exploit a Windows PC versus an Apple device making apple devices just as likely to be attacked.

### **Going Further - Endpoint Protection**

If your business is more advanced and has a more sophisticated network or you store a high level of personal identification information, antivirus/antimalware might not be enough for you. You may need an endpoint protection software. A common misconception about endpoint protection is associated with the term 'Antivirus'. For the smaller mom and pop shops, this is most likely enough protection. However, more developed business networks need to be prepared for threats they can't predict.

This is where the term 'Endpoint Protection' comes into play. Advanced solutions like Watchdog by Anchor Security offer what is known as a Host-based Intrusion Detection System (HIDS). The HIDS software sends all computer activity to a backend server cluster that does anomaly detection, vulnerability analysis, intrusion detection, active response, reporting, historical analysis and statistics, and more to make sure that new threats are detected (and hopefully stopped) and the correct personnel are notified. These are the same methods that large businesses use internally on their infrastructure and devices to ensure their operational and data security.

### **Vulnerability Scanning**

Similar to antivirus, vulnerability scanning looks for known threats, but before the threat is present. If your endpoint protection software does not offer scheduled or persistent vulnerability analysis, scheduled vulnerability scanning is something that should be introduced into your security arsenal.

Vulnerability scanning is one of the many actions performed by security consultants and penetration testers to detect weak spots in your network.

### **Network Intrusion Detection System (IDS) and Firewalls**

By scanning all network traffic, bad actors can be discovered. However, an IDS requires a very powerful server and great knowledge to maintain. Firewalls offer a sort of 'dumb protection'. While some have active response features, firewalls generally just block and allow whatever the user configures them to block or allow. Firewalls don't look for threats or notify personnel about anomalies. Reporting is an essential feature for network security analysis and to determine if network usage has changed, which could indicate compromise.

Please take some time to write down any endpoint protection products you are currently using. These include software that scans devices for vulnerabilities, WiFi monitors, etc.

Protection Check

Date:

We use the following products:

-----

-----

-----

-----

-----

Our products cover the following categories:

- Antivirus
- Antimalware
- Vulnerability Analysis/Scanning
- Anomaly Detection
- Intrusion Detection
- Active Response
- Alerting/Notification
- Historical Analysis and Statistics
- Reporting

## Determining the Impact of an Intrusion

When you do discover an intrusion (ex: a piece of malware has infected your system), you will need to make a determination of the impact of that event. Generally, your endpoint protection will block most attempts to install viruses or malware. In this instance the impact is pretty low – the software blocked it, and you should determine how and why it was attempted to be installed in the first place in order to decide further actions.

In the event that a malicious piece of code does make it on to your systems, you will need to determine what that code's purpose is - is it ransomware looking for a payment or a keystroke logger designed to steal usernames and passwords?

With that understanding you can make a determination of the impact the piece of malware or virus has on your business and begin to take steps to respond. For the small business, this is usually the time to bring in third party consulting and disaster recovery, as the enemy is now in the building.

STEP 4  
**RESPOND**

## What is Your Plan for an Incident?

A security breach requires a plan. Incident response and recovery is usually a struggle for smaller companies, so having a strong plan in place will control the chaos. Smaller companies generally don't have the time to create elaborate plans and test those plans, which is where this section comes in.

### How Often Do You Backup Data?

One of the most prevalent forms of attack is the ransomware. Ransomware encrypts all files on the system and demands a ransom to unlock the files (which it frequently never does). The severity of this attack depends on a few key factors:

- How many devices were impacted?
- How frequently do you backup your data?
- Are your backups version controlled?

The more frequently you backup your data, the less of an impact ransomware has due to less lost data. If you work entirely online using Google Workspace or similar business web-apps, you are less likely to be affected because you are already on a cloud storage however you are not entirely immune. Businesses should create a series of backups, also known as version-controlled backups. These are backups that have all happened at different points in time. This will ensure that you always have a clean backup to restore your system in the event your system becomes infected. If you do not have version-controlled backups and you continuously overwrite a single backup file, you could possibly be backing up the infected files leaving you with no usable, clean backup file to restore your system.

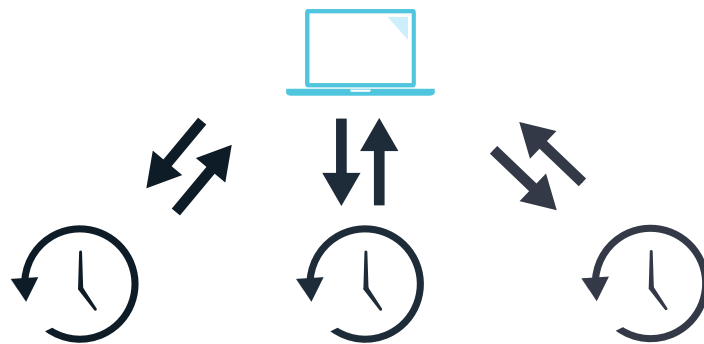
These attacks can be quite harmless if you have good backups in place, however it can be quite tedious to restore data if you use raw file backup instead of full system backups like Time Machine for macOS.

One Continuously Overwritten Backup File



Monday, Wednesday, Friday

Several Version-Controlled Backup Files



Monday

Wednesday

Friday



## What Types of Backups Do You Run?

There are different types of backups that a small business can run in their environment. The level of sensitivity of the data and the importance of it, will dictate what type of backup up should be run.

- **Full System Backup:** This backup will create an exact copy of the computer, including all operating system files. This can also be considered a mirror of your computer's hard drive.
- **File Level Backup:** This is a backup of only user created files on a system. This backup uses less space since it is not copying system files but it will have all of the user's data such as pictures, documents, etc.
- **Incremental Backup:** This backup scans the system for any file changes since the last Full System or File Level backup and only backs up the files that have changed, saving time and space during routine backups.

Each backup comes with different sets of advantages and disadvantages. A small business should consider running a Full System or File Level Backup once a week and run an incremental back up daily. This is to ensure that their files are always up to date.

For small businesses running Windows 7 there is a native free backup program called Backup and Restore. For Windows 8 or higher there is a file level backup called File History. For all businesses running macOS there is Time Machine.

*Please take some time to write down any types of data protection that you use. These can come in many forms such as: Storing data in the cloud, keeping an on-site backup of all data, creating regular backups, and using version control software*

**Backup Schema:**

**Date:**

We backup the following information:

-----  
-----  
-----  
-----

We Back Up Data on the Following Timeline:

Daily     Weekly     Monthly     Other -----

Backups are version controlled

Full system backups are created (ex — Time Machine)



## Who Is In Your Corner?

In the event of a data breach your business needs to move quickly and strategically. In order to do so you should put together an incident response team. An incident response team should be formed with all relevant business personnel. This team includes technical workers to investigate the breach such as a digital forensic investigator that we cover later in this section, along with your IT staff whether they are internal or an external company. You will also want to include your human resource personnel, intellectual property experts, a legal representative when customer data is involved, and your marketing team.

If you are a small business, chances are, you or one of your employees wears all the hats mentioned above. That is okay as long as you acknowledge that you know where to go for help in all the specified areas. A number of legal issues can arise around a data breach, so it is imperative that you seek legal advice as soon as a breach is discovered.

Incident Response Team		Date:
Name:	Department:	Contact Info:
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....

## Containing an Event

To the extent possible when you do discover an event, you will want to contain it. Systems that have been infected with malware or a virus should be taken off the network as quickly as possible. Do not power off an infected system as you may lose valuable forensic evidence, instead quarantine the system by disconnecting from the network. Your endpoint protection may actively respond and quarantine the infected files automatically.

## Do You Require Digital Forensics?

Conducting a thorough investigation in the event of a breach in order to determine what information was actually exfiltrated is crucial. This type of skill set is specialized, and most businesses do not possess the required capabilities in house, so you may require the expertise of a digital forensics investigator. We recommend that you find a company, firm, or individual who can handle these services. You don't necessarily need to have them on retainer but knowing who you will call and perhaps having an initial conversation about how to preserve files for forensics work will help you.

Digital Forensics Contact: .....
Telephone: .....
Contact Email: .....
<input type="checkbox"/> On Retainer

## Cyber Insurance

Data breaches and other cyber crimes are becoming a lot more common. They result in major fines and legal fees as well as unexpected expenses and down time. Cyber insurance has come into play in the last few years and can be a smart precaution for businesses.

Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information. Your general business liability policy does not cover data loss. This is why it is necessary to have cyber insurance.

Typical cyber insurance is designed to provide insurance coverage necessary to help protect your business from the high unexpected costs and effects of a cyber attack or other types of data breaches. This coverage also helps you comply with state and federal regulations.

**America's SBDC has partnered with insurance providers to offer a comprehensive cyber insurance policy for all SBDC clients.**

**Check it out at [www.360coveragepros.com/sbdc](http://www.360coveragepros.com/sbdc)**

When shopping for cyber insurance you want to make sure it has a comprehensive liability coverage for both first-party (internal) and third-party (external) losses.

## First-Party Liability Coverage

This coverage type covers any general cost incurred as a result of a cyber or data breach. Make sure the following items are covered when looking for this type of liability coverage:

- Legal fees
- Cost of notifying affected customers
- Forensics investigation costs
- Business interruption costs
- Public relations expenses
- Expenses to recover or restore lost data

## Third-Party Liability Coverage

This coverage type covers defense costs if the affected parties seek legal action against your business. It also is designed to cover regulatory fines and other costs. Make sure the following items are covered when looking for this type of liability coverage:

- Payments to affected parties
- Cyber extortion costs/payments
- Regulatory fines and penalties
- Settlements, damages and judgments
- Cost to responding to regulatory inquiries
- Bookkeeping costs

## Get Your Business Back on Track Fast and Smoothly



### **Putting The Pieces Back Together**

Response and recovery notions go hand-in-hand, but you want to make sure you are considering the viability of your company and protecting your customers in the event of a significant incident. Once again, time, resources, and expense are all considerations, but some firms find it beneficial to think about “the day after”. Who are you going to call first? How do you ensure your actions will help your company prevent harm to its reputation?

### **Managing Your Brand**

Most small businesses go out of business after a breach. This is due in part to having a tarnished reputation. That is why it is imperative you get in front of the story as soon as possible. The sooner the incident response team knows about the breach, the sooner they can work to fix the issue requiring less down time and loss of revenue. If your business is consumer-facing and you are breached, keeping the public up-to-date within reason helps save face with your customers. Not all security breaches will become public, but if your customers find out and they were not informed you are likely to lose customer loyalty which is hard to get back. Being timely, open, honest and accurate is crucial when making public announcements.

### **Legal Responsibilities**

The size of the data breach and the type of data taken determines what your legal responsibilities are. In the event of breach your first call should likely be to legal support, an attorney with knowledge of breach response and remediation. Few states have specific detailed cybersecurity laws, but that is rapidly changing. Some laws will apply across all business industries, while industry-specific legislation is continuing to develop and target more at-risk sectors. Being aware of what your state and federal laws are will help protect you in the event of a breach.

Legal Contact: .....

Telephone: .....

Contact Email: .....

On Retainer

## Lessons Learned

As you respond to an event, you will always want to incorporate the lessons you learned into your security program going forward. You want to prevent the same type of attack from happening again. If you were subject to a ransomware attack, take the time to train your employees and yourself on identifying malicious links. If you lost data that was unrecoverable because your backup schema didn't adequately address it, take the time to go back and tighten up that area again.

You can never be one hundred percent impervious to cyberattacks, but a real weakness would be to have the exact same type of attack affect your company multiple times without taking steps to identify the root causes. Use the table below to help identify lessons from a breach.

Date of Incident: .....

Explanation of Incident: .....

How was it Discovered?: .....

How was it Remediated?: .....

Data Affected: .....

Steps Taken to Close Vulnerability: .....

*State & Local  
Montana SBDC  
Resources*

<https://sitsd.mt.gov/Cybersecurity/Reporting>

<https://dojmt.gov/consumer/data-breaches-businesses/>

# Montana SBDC Resources

While no technology or program can stop every attack, taking basic precautions can reduce your technical risk and make your company a less attractive target. To help small businesses in this area that is uncertain to most, the Montana SBDC has created resources in partnership with the Delaware SBDC. These resources range from simple cybersecurity check-lists to more detailed industry specific workforce development. Below you will notice just a few of our resources.

The Data Assured program is always looking to grow and expand its resources. Please reach out to us with any suggestions you might have on possible topics you would like to see covered.

## Resources



Cybersecurity Solutions



Cybersecurity Tips



In-person Training



Phishing Training Tool

Additional resources can be found at:

[www.SBDC.MT.gov](http://www.SBDC.MT.gov)

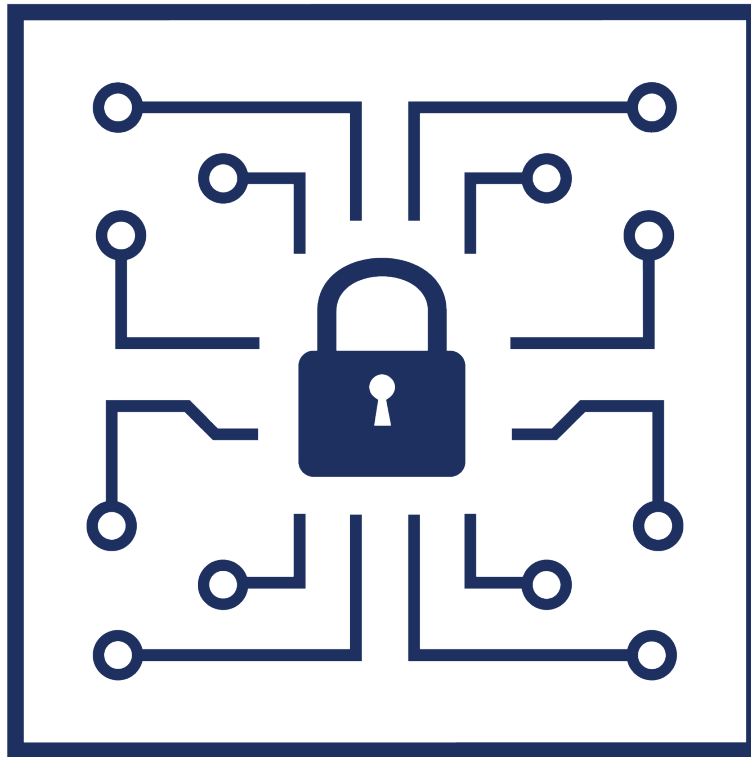
[www.DelawareSBDC.org](http://www.DelawareSBDC.org)





D A T A

A S S U R E D



**Montana SBDC Lead Center**

301 S Park Ave  
Helena, MT 59620  
(406)-841-2747



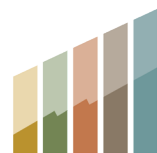
**Email**  
[MTSBDC@mt.gov](mailto:MTSBDC@mt.gov)



**Website**  
[www.SBDC.MT.gov](http://www.SBDC.MT.gov)



U.S. Small Business  
Administration



**MONTANA**  
DEPARTMENT OF COMMERCE

The Montana SBDC is funded in-part through a Cooperative Agreement with the Montana Department of Commerce and the U.S. Small Business Administration.

Services are provided on a non-discriminatory basis. Reasonable accommodations will be made for persons with disabilities and/or limited English proficiency. Please contact the Montana SBDC office nearest you two weeks in advance.