ANCHOR SECURITY

Cyber Workbook

A NOTE FROM THE DELAWARE SBDC

Dear Small Business Owner,

The largest threat currently facing small businesses is cybersecurity. Small to medium sized businesses are particularly at risk because they are viewed by hackers as easier to penetrate due to their general lack of awareness and resources. Small businesses can no longer afford to remain unaware of the threats or remain complacent with inadequate technology. They have to take action to enhance their systems, processes, and staffing in order to remain viable in today's online economy. You are not alone, however. The Delaware Small Business Development Center (DSBDC) is here to help.

For over 35 years, DSBDC has been helping small businesses start, grow, and succeed. By keeping our finger on the pulse of today's rapid economic and technological changes, we have adapted our advising approaches and educational offerings to meet the unique needs of Delaware's small business community.

Supported by a cooperative agreement from the Small Business Administration, in 2016 DSBDC responded to the need to equip small businesses with cybersecurity knowledge and resources by introducing new materials and tools to speed up and ease the process. Developed in partnership with the University of Delaware, Anchor Security, and stakeholders, this material is designed to provide ongoing face to face and webbased training targeted to the small business in need of cyber guidance. We also provide print resources, such as this workbook, and 1:1 advising with our experienced business advisors who understand the needs of small businesses.

The information within this workbook is a starting point for your planning and should be updated regularly. As the cybersecurity landscape continues to change rapidly, so must your business strategy and operations. As mentioned earlier, DSBDC is here to help. If you would like to continue your learning beyond this workbook, we encourage you to visit our website where you will find upcoming events, local resource partners, brief videos, and much more. The website is: http://delawaresbdc.org/specialprograms/datassured/.

Don't wait for a cyber-attack on your business. Work with DSBDC today to plan ahead. Call (302) 831-1555 to make an appointment for one on one, confidential and free counseling with one of our business advisors or visit our website for more information: www.delawaresbdc.org

Sincerely,

J. Michael Bowman
State Director

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 less employees than ever, technology can allow small businesses to directly compete with those of medium and large size. 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 to the 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 just a step along their path.
- The type of business you are in may increase your risk profile and attack surface. Are you a retailer, health care provider, or financial firm who utilized credit card payment and or aggregates client information?

Bad actors believe smaller companies with less resources for both physical and digital security are a ripe target, 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 for 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? We believe 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. Keep it simple and effective.

Purpose

This 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 the unique circumstances that your business exists under. It is key to note that his workbook is just a starting point in your cybersecurity measures.

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

Intended Audience

In creating this cybersecurity workbook, we have attempted to offer something that works for companies of all sizes, but we are limited to how much information we can put in one place and make it easily digestible. To that end, this workbook is 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 ways of retained data. On the opposite end of the spectrum, large companies may find some of the information contained herein to be of an elementary nature.

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 new employees understand and embrace their role with respect to cybersecurity.

For the medium company you many find many topics here that have not been thoroughly discussed 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.

For the larger company, 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. If you can clearly define all of the points we list herein for your firm, 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!

Difficulty

Easy Medium *(You can do this!)* Hard

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 that, if you have questions that are highly specialized and unique, that 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 Framework was then updated to Version 1.1 on April 16, 2018. Among other refinements and enhancements, the document provides a more comprehensive treatment of identity management and additional description of how to manage supply chain cybersecurity. The CSF itself has gone on to enjoy success in businesses of all sizes, version 1.1 has been used by over half a million companies in just nine months post release. Since the first publication of the Framework, NIST stated clearly that it was to be adapted, expanded, contracted, and used as a form of guidance. This workbook and, by extension, your cybersecurity practices are based upon the 5 central concepts of the NIST CSF:

STEP 1
IDENTIFY

What structures and practices do you have in place to identify cyber threats?

STEP 2
PROTECT

What are the basic practices you have in place to protect your systems?

STEP 3
DETECT

What do you use to identify 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 get 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 here (LINK TBD) where you can go to download and type in the information as you work through this plan.

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:

Northern Delaware SBDC

(State-wide Headquarters)
Delaware Technology Park
1 Innovation Way
Suite 301
Newark, DE 19711
(302) 831-1555

Southern Delaware SBDC

(Serving Kent & Sussex Counties)
103 W. Pine St.
Georgetown, DE 19947
(302) 856-1555

Email
Delaware-SBDC@udel.edu

Website
www.delawaresbdc.org

STEP 1
IDENTIFY

Who, What, Where, and When?

Why Do This?

Identifying the threat is the most fundamental part in protecting against it. Knowing what is coming, or has attacked, gives you the advantage you need to protect and/or recover.

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:

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 Consulting (If Any):

Prioritization

As you work though 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 decraese complexity.

What Data Do You Keep? Where Do 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 NAS), 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 auth, IP whitelisting, etc.)

Examples include:

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

Our Sensitive Data, and Where It's Stored

	Data Type	Location
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		

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 and 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.)

What Operating Systems Are You 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 on April 8, 2014. Windows 7 support will end Jan. 14, 2020. Similarly, Apple ended support for OS X 10.6 (Snow Leopard), on February 26, 2014. Your business should not be running unsupported versions of operating systems. Check to make sure all devices are updated to the current version. 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 ___ can be updated or is losing support soon	
NON-SUPPORTED SYSTEM(S)/DEVICE(S) IN USE	

What Software Are You 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	

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 in which you protect that data. Along the way, we'll offer tips and industry best practices for securing your information and how employees access it. The 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 do have use a personal computer that is shared with other members of your family, create a separate 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. Using only letters takes a small fraction of the time to crack all possible passwords of the same length including 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 can be as follows:

1. Original Passphrase "Pizza is my favorite food"
2. Passphrase usability: "pizzaismyfavoritefood" (removed spaces)
3. Passphrase strengthening: "P1zz415Myfav*r1teF**d" (Capitalized first letter of each word, replaced non-caps letters with numbers where possible, replaces 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 8 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 provide a great opportunity for setting a very complex passphrase, while also keeping it easy to login every time. Mobile devices now use 6-Digit passcodes and biometrics by default, while most support passphrases as well. Using a passphrase with a mobile device, and then using biometrics to log in between reboots allow for immense security with ease.

PASSWORD CHECK **Date:.....**

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

Device Inactivity 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 locking sleep to occur on a device 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. You may be able to use ActiveDirectory in a Windows environment, or some cloud-based systems will let you control these details. If you 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 of 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 and should be used. With Apple laptops, FileVault is easy to use and free. 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 that on if they are accessing company data from their Android devices, and encourage them for personal security If not.

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 is having a separate system for encrypting your files before they get to the cloud like boxcryptor or rclone/rsync increases your data security.

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 "bestefforts" process. This encryption will only protect email from being intercepted when in transit. Services the Gmail, iCloud, and Microsoft Outlook are encrypted by default

ENCRYPTION CHECKLIST **Date:**

Our Company Encrypts The Following:

- ☐ Database ☐ N/A
- ☐ Server Storage ☐ N/A
- ☐ Laptop Disk
- ☐ Mobile Devices ☐ N/A (devices not used for business)
- ☐ Email in Transit
- ☐ Other .....

Role Based Access Control (RBAC) of Data

If you are a solopreneur, you probably don't need to implement a data segregation plan, but for even the smallest companies, putting your data into various places that are restricted to those who need the information is a great idea. In order to properly segregate data, you need to first determine what data you collect and then who needs access to your 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. Write down below the types of data that you might collect and who within your company needs access to them. Set up folders or other permission methods and restrict access to those folders.

Please take some time to write down which types of date your business currently uses. This could include emails, accounting information, sensitive customer information, CRM data, and employee information.

DATA SEGREGATION LIST:	Date:
Types of Data:	Who has access:

Employee Training

If your business has employees, you should be training them regularly on cybersecurity best practices. They should be provided training on hire and annually, and also on an as-needed basis. If you have an event 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

OPEN DNS Phishing Training – 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."

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 where ever possible. If more than 2FA is possible, it should be used as appropriate. Most online services lie Gsuite, Microsoft Office, etc. offer 2FA or MFA. Additionally, administrators can choose for accounts to require 2FA or MFA. If backup codes are given, make sure they are stored in a safe place whether they are stored digitally, physically, or both.

STEP 3
DETECT

Recognize if Something is Going Wrong, and Stop it

Endpoint Protection

A common misconception about endpoint protection is associated with the term 'Antivirus'. Simply put, an antivirus is not enough. Antivirus works by storing known signatures of malicious code and files and checking against the signature of any new files on the device. Windows comes installed with Windows Defender, Microsoft's in-house antivirus. Apple devices trust that the user knows what they are doing with yes/no prompts when opening or running files downloaded from the internet. For the individual user, this is most likely enough protection. However, any sized business needs to be prepared for threats they can't predict. It is in this scenario that regular antivirus does not provide enough protection.

This is where the term 'Endpoint Protection' steps in. Advanced solutions like Sonar by Anchor Security offer far more than antivirus. Known as an Host-based Intrusion Detection System (HIDS), the 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, the correct personnel are notified, and hopefully stopped. These are the same methods that large business use internally on their infrastructure and devices to make ensure their operational and data security.

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.

Endpoint Protection Check **Date:**

We Use the Following Endpoint protection Products:

Our products cover the following categories:

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

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.

NOTE:

Some antivirus/antimalware, endpoint protection, and vulnerability analysis software are not compatible and may recognize each other as threats. An endpoint protection package that offers all features is the ideal scenario.

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, generally firewalls just block and allow whatever they are configured to do without looking for threats or notifying personnel about changes. Reporting is an essential feature for network security for analysis and to determine if network usage has changed, which could indicate compromise.

Determining the Impact of an Event

When you do discover an event (eg – a piece of malware on 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 correct 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 in life 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 disasterrecovery, 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, 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 (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 Gsuite or similar business web-apps, this should not be an issue. If your backups are not version controlled, they may not even be useful in the event of ransomware as you could just backup the ransomware, overwriting the important data.

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.

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 Back up the following Information:

.....

.....

.....

.....

We Back Up Data on the Following Timeline:

☐ Daily ☐ Weekly ☐ Monthly ☐ Other .....

☐ Backups are version controlled

☐ Full system backups are taken (eg — Time Machine)

Do you Require Digital Forensics?

Digital forensics may be needed in the event of a breach in order to determine what information was actually exfiltrated. This type of skill set is specialized, and most businesses do not possess the required capabilities in house to perform them. 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: .....

☐ On Retainer

Containing an Event

To the extent possible when you do discover an event, you will want to contain it. If your endpoint protection does not actively respond or does not already do so, systems that have been infected with malware or a virus should be removed from the network as quickly as possible. Do not power off a system as you may lose valuable forensic evidence.

Lessons Learned

As you respond to an event, you will always want to incorporate the lessons you learned into your 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: .....

STEP 5
RECOVER

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 of benefit 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?

Who are your resources?

Before a breach, identify what resources you will need to help you in the event of a serious security event or one which involved client/sensitive information.

In the event of breach your first call should likely be to legal support, an attorney with knowledge of breach response and remediation. Again, you need not put an attorney on retainer, but knowing who you are going to call before you need them will save valuable time in the event of a breach. Identify your legal resources below:

Anchor Security as a resource. info@anchorsecurityteam.com

Legal Contact: .....

Telephone: .....

Contact Email: .....

☐ On Retainer

You may also wish to consider identifying your local police resources who may be of assistance. The Delaware State Police Intelligence Unit will be able to assist you in finding proper law enforcement reporting and support points. They can be reached at:

Delaware State Police Intelligence Unit | 800-FORCE-1-2 www.dediac.org

Beyond Delaware, the FBI's field offices can provide assistance in the event of breach. They can be found online at: **www.fbi.gov/contact-us**