DATASSURED™

Small Business Cybersecurity Workbook

Prepared By:

Tim Villano & Lyman Terni

ARTEMIS
GLOBAL SECURITY, LLC

Presented By:

AMERICA'S SBDC DELAWARE
Small Business Development Center

UNIVERSITY OF DELAWARE | oei
Office of Economic Innovation & Partnerships

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 DatAssured™. Developed in partnership with the University of Delaware and stakeholders all across the state, DatAssured™ is designed to provide ongoing face to face and web-based trainings targeted to Delaware's industry segments. We also provide print resources, such as this workbook developed by Artemis Global Security, and 1:1 advising with our experienced business advisors who understand the needs of Delaware's small businesses.

The information within this workbook is a starting point for your planning and should be updated regularly. As the cyber 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/special-programs/datassured/.

Don't wait for a cyber-attack on your small business to occur. Work with DSBDC today to plan ahead. Call (302) 831-1555 to make an appointment for 1:1, 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

For many small business owners, technology is both a great equalizer and a significant threat. With a relatively small number of employees and the right combination of systems and services, your business can now communicate with and service customers and clients and compete directly with medium and large-sized businesses. 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 client information is essential. This is not just a matter demonstrating the "reasonable" practices your company has put in place should your firm be subject to breach, but important to outright survival for small companies. Many businesses cannot afford the legal, regulatory, and forensic hassles and expenses that typically accompany a breach of systems which involves the exposure of client or partners' information.

At the same time, the threat beyond regulatory concerns is very real. The bad actors out there, Criminals, Competitors, Hacktivists, and State-Sponsored Terrorists, are targeting you for several reasons:

- Do you have relationships and dependencies with larger companies who may be a target? Bad actors may be targeting you to get at other firms;
- The type of business you are in may increase your risk profile. Are you a retailer, health care provider, financial company who utilizes credit card payment and or aggregates client information?
- Bad actors believe smaller companies, with less resources for both physical and IT security, are a ripe target.

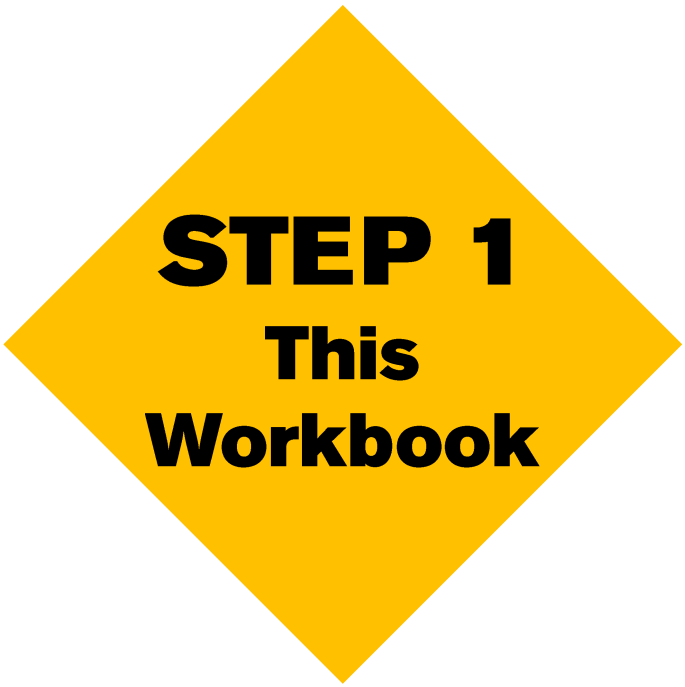
Given this landscape of both business and regulatory threats, what can and should a small business owner do? In many ways, we believe it is essential for the small business owner, in the absence of unlimited personnel and funding, to have precise controls and solid policy in place. Keep it simple and effective.

Purpose

The Cybersecurity Workbook is designed to provide your small business with a starting concept for creating a Written Information Security Program or (WISP). It may sound complicated at first, but the essence of a WISP really comes down to defining a reasonable program for handling cybersecurity within your organization. It may mean some extra work for you, as you'll need to write some items down and review them on a regular basis. But beyond that, maintenance of a WISP should be a relatively simple process that grows with your business.

This document is designed to map you through the sections of your company's WISP and leave you with a working (and workable) program. Yes, you will have to change and adjust this Program going forward and you may also wish to expand it based upon the unique circumstances at your business.

It is essential to note that this workbook is just a ***starting point*** *in your cybersecurity measures. It is meant to get you thinking in a security mindset. This workbook on its own cannot serve as your "hat tip" to cybersecurity. You must make security your own and live it day in and day out at your business.*



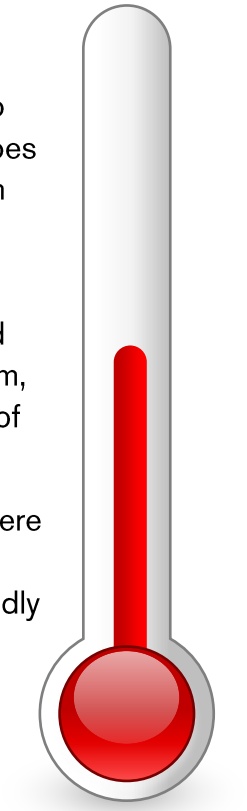
Intended Audience

In creating this cybersecurity workbook, we have attempted to offer something that works for companies of all sizes, but we are limited in 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 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 you can apply them 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 **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

Medium. You can do this!

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 an 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 or 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**.

This workbook and, by extension, your cybersecurity practices are based upon the 5 central concepts of the NIST CSF:

IDENTIFY (Pg 8)	What structures and practices do you have in place to identify cyber threats?
PROTECT (Pg 12)	What are the basic practices you have in place to protect your systems?
DETECT (Pg 19)	What do you use to identify someone or something malicious?
RESPOND (Pg 21)	How will you deal with a breach if and when it occurs?
RECOVER (Pg 23)	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 (http://delawaresbdc.org/special-programs/datassured/) 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

Q: What are we identifying here?

A: Simply Put – Who, What, and Where?

Why Do This?

Without knowing who is responsible for cybersecurity you cannot begin to address it. Beyond that, without knowing what systems you have or what software you are using, you do not have any means of understanding the controls and security items you can put in place, or that may already exist. There may also be no way to identify the potential source of a security event of breach.

Who is Responsible for Cybersecurity?

Here is the simple starting point. Who at your company is responsible for cybersecurity? If you're filling out this workbook, chances are it's you, but there may be someone else at your company who will take the lead. Write down their name or role here:

NAME OF PERSON RESPONSIBLE FOR CYBERSECURITY:

Outside Consultants

Is there anyone outside of your firm that you might turn to in order to help you with cybersecurity or with helping to enact protections or changes? It's ok if you don't have one.

NAME OF OUTSIDE CONSULTANT (IF ANY):

Extra Credit – Prioritization

As you work through the next few items and determine what data, systems, and software you keep or use, try to prioritize them in terms of criticality. What do you really need for your business to function, and what's just a nice add-on? This thinking will help you consider which systems and applications you should restore first in the event of a disaster.

What Data Do You Keep?

This is the root of a cybersecurity policy so take your time here. What data do you maintain that could be useful (or profitable) to a hacker? Some 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 Information

What Devices Need Protecting?

Let's think about what you're protecting from a physical standpoint first. We will create an inventory for your systems and devices. Think about everything that might be used to access your company's information: desktops and laptops, obviously, but include smartphones and tablets here too. It's ok to just name them something simple (like Mary's laptop).

Hardware Inventory		**Today's Date:**	
Desktops	Laptops	Smartphones	Tablets

What Operating Systems Are you Using?

Make sure that all your operating systems are patched and updated. For instance, support for Microsoft Windows XP ended on April 8, 2014. Similarly, Apple ended support for OS X 10.6, aka Snow Leopard, on February 26, 2014. These systems could be vulnerable to attack and their manufacturers will no longer secure them. Your business should NOT be running any of these operating systems. Check as well to make sure your mobile devices are running currently supported versions. If not, it is time to upgrade. Use of an unsupported device is asking for a breach.

OS CHECK	**Date:**
☐All Systems Supported	
☐All Systems Supported But The Following Are Expiring Soon _____	
☐NON-SUPPORTED SYSTEM(S)/DEVICE(S) IN USE	

What Software & Cloud Storage Keeps My Information?

Information is typically stored via different types of software, such as in Quickbooks for payroll and customer data, or perhaps in a Customer Relationship Management Software (CRM), like Salesforce. Identify the places where you store electronic data here and enter in next to it any security features that you need to use to access the data (such a complex password, or two-factor authentication (where you enter a PIN number after your password). Also, include cloud storage facilities here as well, such as Dropbox, Box.com, iCloud, or OneDrive. We're just interested in your business files here, not where you keep personal photos, etc.

TIP: If you know the version of a particular piece of software, write it down here. If not, take a look when you get back to your office.

MAKE SURE THE VERSION IS STILL SUPPORTED.

Software and Cloud Inventory		**Today's Date:**
Local Software (You installed the software on your computer)	Hosted Software (You go to a website to access the software)	Cloud Storage (You go to a website or have an installed program to save files to – like Dropbox)

Step 2: Protect

Question: What are you protecting?

Answer: The items you identified above. And your business's reputation.

We identified the data that you keep in the first step, and now we're 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 making sure that your employees access that information securely as well. The best practices can and should extend into your private life as well. If you're not using complex passwords for your personal information, take the time to do so now. It's just good **cyber hygiene!**

How do you Manage Identities?

User Identities are a means of determining who is accessing what data at what time. It also provides you a level of protection because you can disable a single user on your systems if you need to, versus having to re-authenticate everyone logging into your network or systems.

USERNAME CHECK	**Date:**
☐All Users have their own logins	
☐Some Systems Use a Common Login_____	
☐NO Logins in Place/One Shared Login	

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?

Password complexity is one of the easiest pieces of the cybersecurity puzzle to solve. General best practices call for the following:

- 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; And
- Lockout: 10 minute lockout after 8 unsuccessful login attempts.

Extra Credit: Passphrases

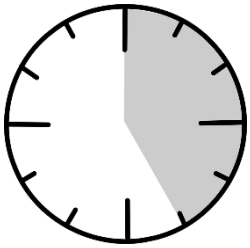
If your systems can support the use of passphrases, essentially very long passwords that are easily memorized but would be impossible for a machine to guess, go ahead and use them. They make your system more secure than a shorter password and can be easier to remember than a jumble of characters and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

What About Mobile Device Passwords?

Mobile Devices that access company information should be protected with at least a four-digit PIN number. If you are using a biometric reader, like your fingerprint, we recommend using a more complex and secure password as you won't have to type it in very often.

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: _____ ☐ Mobile Devices Secured by a 4-Digit PIN at Minimum	

Do you Lock Your Systems After Inactivity?



System timeouts are a good way to protect your systems in the event that you or an employee walk away from a computer for a period of time. All computers should be set to lock and require a password again after 25 minutes of inactivity.

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 is its own right. If you or your employees are having such 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.

Do You Encrypt Your Data?

Encryption is something that can be undertaken by most companies regardless of size. However, there are different things that can be encrypted, it's important to understand what they are:

- **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.
- **Hard Drives of Servers** – Server hard drives can be encrypted if necessary. This will ensure that the drive is inaccessible should it be physically removed or stolen.
- **Hard Drives of Laptops** – Laptops are susceptible to theft or loss. If you have the ability to encrypt the hard drives on those systems and you store sensitive information on them, you should do so. This can be easily done with a number of different products economically. BitLocker is a built in Microsoft Technology that can be used, and Apple offers built in encryption as well.
- **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.

- **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.

ENCRYPTION CHECKLIST	**Date:**
Our Company Encrypts The Following: ☐ Database ☐ Server Hard Drives ☐ Laptops ☐ Mobile Devices ☐ Email in Transit ☐ Other _____	

How Do You Segregate 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 folders 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. When you get back to your office, set up folders or other permission methods and restrict access to those folders.

DATA SEGREGATION LIST:	**Today's Date:**
Type Of Data	Who Should Have Access

If you are writing down a policy to go along with your plan, try the following language as a starting point:

[Company Name] permits access to drives, folders, and files on an as-needed basis. For example, only our accounting group/individual has access to Payroll Information.

[Company Name] manages data with the following considerations

- Customer information and other data deemed to be sensitive is segregated;
- Data in Transit, specifically that data contained within our email system is encrypted with SSL/TLS technology if supported; and
- Enhanced controls are in place on systems accessing customer data to prevent data leakage.

Do you Access Files Remotely?

Remote, personal system use is a source of potential vulnerabilities. Basically you need to ensure that, if your workforce is using a home office, that those systems are reasonably controlled. Do home workers have complex passwords in place? When was the last time that the OS was patched? Is there current Antivirus in place?

Training on this point is also essential. If your company has set up a Virtual Private network (VPN) to access files at your office, employees should know to use the VPN whenever they are in a public place or may have concerns about the security of the connection. Employees should not access any sensitive information over public networks, such as those found in coffee shops or in airports

HOME ACCESS CHECK	**Date:**
☐ We Do **NOT** allow remote access of any files	
☐ We Allow Access of Remote Files	
☐Employees Trained on Patching & Password Controls for their Systems	
☐Employees Use a VPN to connect securely	
☐Employees do not access sensitive information over public WiFi connections.	

How Do You Use Firewalls?

Firewalls are effective devices for blocking potentially malicious activities on your network and systems. Your business should have a firewall of some kind in place. Different sized business will have different firewall needs, however. Check the box that applies to you.

☐**Large Businesses:** Large businesses that can afford separate firewalls to protect their entire network structure at the edge of the network (IE – where your internet connection from the outside world joins your internal network) should have firewalls. Any firewalls that are in place should still be supported and patched with the most recent firmware.

☐**Small Businesses:** Small businesses that may not have an internal network can take advantage of the internal firewalls that are present on Windows and Apple computers. All workstations and laptops should have these firewalls enabled at all times.

How Do You Handle System Patching?

Operating system patching is an essential security measure. Known weaknesses are constantly exploited by hackers so make sure that your system is set to automatically download and apply system patches on a regular basis. It's generally best to leave a system on overnight to apply patches when it won't interfere with your work. Just make sure that you don't power down your system on patch night!

Beyond operating systems, applications such as your internet browser, Adobe products like Reader and Flash, and Java are updated very regularly. Make sure that you are including these patches in your regular update cycle as they are just as important as Operating System patches!

PATCH CHECK	**Date:**
☐ We automatically download and install all updates for Operating Systems and Applications.	
☐ We automatically download and install all updates for Operating Systems and manually patch applications.	
☐ We manually patch or do not patch Operating Systems and Applications.	

How Do You Train Your Employees?

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."

Extra Credit: 2 Factor Authentication

If you use any additional access and authorization controls like two-factor authentication, make sure that this is listed in any written policy under your Protections section. 2 factor is available through common cloud-based applications like Dropbox, Facebook, LinkedIn, Twitter, and platforms like Microsoft365 and Google Apps.

2 Factor adds a layer of security to any login process by requiring a passcode that is randomly generated and sent to the user by text message, email or code-generating application and is used in addition to a normal password. If you use two-factor, even if someone gets your password, they generally won't be able to login because they won't be able to receive the secondary PIN number.

Step 3: Detect

Q: What are we detecting?

A: Detection is the process to recognize if something is going wrong on your network and, if possible, stopping it.

Antivirus Applications

All systems need some form of antivirus application that is installed, updated, and run regularly. Larger companies may want to look at a unified program such as Symantec Endpoint Protection, which lets an administrator push updates and require scanning at regular intervals.

For smaller companies, Windows does offer built-in antivirus software, and there are many good free options out there as well. The most important thing to remember when you are installing an antivirus application is that it won't do anything on its own. An Antivirus program needs to be scheduled to first update and then secondarily actually run to scan for viruses which can lay dormant or not be immediately apparent.

Antivirus Information:				**Date:**
We Use the Following Antivirus Product: _____				
We update Antivirus Definitions	☐ Automatically		☐ Manually Before Each Scan	
We Run Scans	☐ Hourly	☐ Daily	☐ Weekly	☐ As Necessary
Scans are Initiated	☐ Automatically		☐ Manually	

Antimalware Applications

Antimalware applications are similar to antivirus applications, but most systems do typically require some combination of the two as they are designed to address different areas. Similar to Antivirus applications, there are many free antimalware programs out there. The same caveats apply to Antimalware applications as to Antivirus Applications: They must be scheduled to update as well as to run scans in order to be effective!

Antimalware Information:				**Date:**
We Use the Following Antimalware Product: _____				
We update Antimalware Definitions	☐ Automatically		☐ Manually Before Each Scan	
We Run Scans	☐ Hourly	☐ Daily	☐ Weekly	☐ As Necessary
Scans are Initiated	☐ Automatically		☐ Manually	

TIP: In addition, be aware that at times antimalware and antivirus applications can conflict, so be on the lookout for one system identifying the other as potential virus or piece of malware.

More Complex Methods of Detection

There are more complex methods of detection out there that a larger business, or a business with particularly sensitive information may wish to use to further lock down their networks. They include next generation firewalls that offer unified threat management. Unified threat management firewalls incorporate the functions of a traditional firewall (blocking ports, etc.) and also incorporate web filtering and email filtering into their roles. These devices can provide reporting and other outputs that may let a business know when it is under some form of attack. These solutions are typically customized for each business and require some knowledge to properly configure. When in doubt, we'd recommend seeking out an IT professional to help you.

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 antivirus program or antimalware program will block most attempts to install viruses or malware. In this instance the impact is pretty low – the program blocked it, move on with your day.

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.

Step 4: Respond

Q: How do we respond to an Incident?

A: You need to have a plan in place beforehand

IT Security incident response and recovery is an area with which firms may struggle. Smaller companies generally do not have the time to create elaborate plans and to test, so you need to plan in a fashion that works for your firm.

If you maintain client information and have represented a certain degree of diligence in this process via a Privacy Statement, then you need to take these sections seriously. If your company is small and you have avoided aggregating sensitive information, you still should take a bit of time here to understand these concepts and come up with a basic idea of approaching breach in order to protect your business.

How Often Do You Take Backups?

One of the most prevalent forms of attack today is the Cryptolocker variant of malware. When this type of malware is installed on a system, all the files are locked and a ransom is demanded in order to obtain the key to unlock them. Your only recourse in this event is to go back to your backups. If you have them! When you define a backup schema (that is, how often you back up systems and what you backup) you need to make a determination of how much information (from a time standpoint) you are willing to lose. Is it an hour? A day? A week? Make this decision now and set up a backup structure for your systems that meets these requirements.

Backup Schema:	**Date:**
We Back up the following Information: _____	
We Back Up Data on the Following Timeline: ☐ Daily ☐ Weekly ☐ Monthly ☐Other _____	

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 or an 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:**

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 removed from the network as quickly as possible. Do not power off a system as you may lose valuable forensic evidence.

Incorporating Lessons Learned

As you respond to an event, you will always want to incorporate the lessons you learned into your program going forward. The idea is that you want to prevent the same type of attack from happening again. If you were subject to a cryptolocker 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.

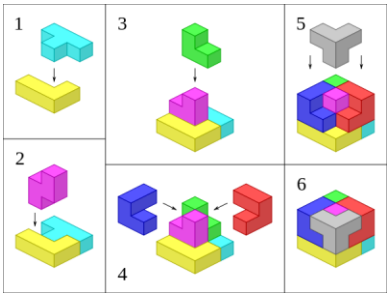
You can never be one hundred percent impervious to cyberattacks, but a real weakness would be to have the exact same type of attack affect your company multiple times without taking steps to identify the root causes. Use the table below to help idenfity lessons from a breach

Date of Incident:
Explanation of Incident:
How Discovered?:
How Remediated?:
Data Affected:
Steps Taken To Close Vulnerability:

Step 5: Recover

Q: What is Recovery?

A: Recovery is getting your business back to a pre-incident state as quickly and smoothly as possible



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 IT 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:

Legal Contact:	**Telephone:**

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

AMERICA'S SBDC DELAWARE

Small Business Development Center

Northern Delaware SBDC
Delaware Technology Park
1 Innovation Way, Suite 301
Newark, DE 19711
(302) 831-1555

Southern Delaware SBDC
(Serving Kent & Sussex Counties)
103 W. Pine Street
Georgetown, DE 19947
(302) 856-1555

www.delawaresbdc.org/

U.S. Small Business Administration

SBA

Your Small Business Resource

The Delaware SBDC Network is funded in part by the U.S. Small Business Administration (SBA), Defense Logistics Agency, State of Delaware, and other private and public partners. Nationally accredited by the Association of SBDCs.