

DATA
ASSURED



Cyber Workbook



UNIVERSITY OF DELAWARE
ECONOMIC INNOVATION
& PARTNERSHIPS

In Partnership with:
ANCHOR SECURITY



Small Business
Development
Center

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 this 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 may 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



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 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:

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:

Delaware SBDC - New Castle County Office

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

Delaware SBDC - Kent County Office

Delaware State University
Bank of America Building, Rm 108
1200 North DuPont Highway
Dover, DE 19901
(302) 831-1555

Delaware SBDC - Sussex County Office

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 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.

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 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.)
.....
.....
.....
.....
.....

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	
.....	
.....	
.....	