Chapter 14 – Cybersecurity Resilience

What this section is about – what you should learn

In this chapter you will learn about Cybersecurity Resilience, which is ensuring that a business can survive even when disaster strikes. This chapter is mainly about business continuity, and contains lessons that are typically found in business and management classes. So, it's less about the technical side of cyber security and more about Information Assurance and the business side of cyber security. Learning about a subject that's more about business than it is about computers might seem a little strange in a computer security class. But learning about business continuity actually makes sense as business continuity is *the* reason that almost every business needs someone who knows about cyber security. And it's the reason there are so many career opportunities in cyber security.

Think about it this way. Businesses have lots of essential items and jobs that need to be done. The essential work includes things that directly help the company create and deliver its products or services. But companies may also have lots of non-essential items, like a bag of potato chips or an umbrella. The non-essential things are nice to have around but the business could still run without them. Today most businesses of any size rely heavily on their computers and their data, and in many cases could not function without them. Many businesses face disaster when their computers or networks fail or when they fall victim to a cyber-attack. And it's not just the immediate financial disaster, it's also a loss of customer confidence and damage to their public image that can occur when a company falls victim to a cyber attack. That is, any company that doesn't protect its sensitive customer information and loses it during a cyber attack will receive negative news coverage and lose the trust of its customers, both of which will have an impact on the company's long-term prospects. This perspective on the value of a company's data moves the company's computing devices and services from the "nice to have but not essential" category into the essential category. And since their technology is essential, companies are willing to pay to ensure that their computers and networks are available.

As you learn about business continuity you'll see that this is another subject that requires a change in mindset and a different outlook than you have when the only thing you need to protect is your home computer. Understanding business continuity and planning for possible disasters requires taking a look at the bigger picture of the business and how it's run, instead of just focusing on taking care of hardware and software. You'll have to evolve from just being in the tech bubble where you deal with hardware and software, to seeing how the systems you support are actually used in a real world business.

The book discusses several aspects of business continuity, but in general it's accomplished in two or three ways, depending on how you count. The first is redundancy, and the second or second and third are having well established policies and procedures in place and ensuring those policies and procedures are followed and enforced.

Business Continuity

Redundancy

A harsh fact of life is that every piece of hardware will fail sooner or later. You may have already had the bad luck to experience this personally. Maybe you had a hard drive fail, which caused you to lose all your data. Or maybe you've had a router stop working which prevented you from connecting to the Internet. In any case, nothing lasts forever, and all your hardware is guaranteed to stop working someday. While this can be super frustrating if it happens to one of your personal devices, it can be catastrophic to a business.

For a business organization, the solution to the problem of hardware failure is to have replacements for every critical piece of hardware the company uses. In some cases, at larger organizations, there will be entire duplicate computers or even entire networks, ready to go online at a moment's notice. In other cases, the replacement hardware may be purchased and available, but will take some time to install and configure. The decision on whether to have a hot backup system, ready to go in a matter of seconds, versus just having replacement computers or replacement parts requires some cost analysis. The business needs to determine how much they would lose in the minutes or hours a system may be down, and balance that against the cost and type of the redundancy. For example, if a business would lose $100,000 a minute if a system were down, and a hot backup costs $50,000; the hot backup would probably be worth the cost. But if a business only faced a loss of $5 per day on a system, then having the $50,000 hot backup is probably not worth the cost. I have a friend who is ex-military special ops, and he has a saying regarding essential systems that sums this up pretty well. "One is none, and two is one …"

You can probably think of some good examples of doing this type of cost analysis in your own life. For example, consider your vehicle. This is probably an essential piece of equipment in your life, as you need transportation to get to school, your job, shopping etc. And all cars are pretty much guaranteed to stop working at some point. Hopefully you'll get years of use from your car, but sooner or later it's going to stop working. One of the ways you could avoid any down time if your car stops is to purchase a second vehicle. But is the cost of owning a second car worth it, when you look at the chance of your car not working? I'd guess the answer is probably no. But is it worth buying an extra $10 thumb drive, in case the one you're using stops working, or you lose it? I'd say sure … just remember where you put the spare drive. LOL. The point of this is that you're already doing risk analysis and cost/benefit analysis in your life, even if you don't realize it.

Performing this type of analysis, deciding what redundancies are needed, and deciding if they're worth the cost requires some specific knowledge of the business or organization you're supporting. It typically takes several year of experience as well, so don't be concerned that this is something that you'll be asked to do the first day on your new job. This work is usually done by a senior person with a title like Chief Information Security Officer (CISO) or Chief Security Officer (CSO).

It might seem like providing redundancy to ensure business continuity is non-issue, and that any sensible business person will be willing to pay the costs. In a sense it's just like buying insurance against some catastrophic failure. If this were the case then all that needs to be done is to figure out what redundant systems need to be purchased and setup. But you need to remember that most businesses exist to make a profit, and purchasing redundant systems will be reducing the immediate profits. Once again, it's just like insurance, in that it only pays off if there's a disaster, otherwise it's just an ongoing cost, and possibly an expensive cost.

Plus, with the constant advances in technology, any redundant systems you buy today may be obsolete in a couple of years. For example, say that 4 years ago you bought an extra cell phone that you could use, just in case your primary phone gets lost or damaged. A year ago, you upgraded your primary phone, but decided that you would keep the same backup phone. If you actually lost your primary phone and needed to use the backup phone you will certainly find that it's "old" compared to modern phones, with a smaller screen, less storage, etc. You also may find that you can't even use the backup phone, as the cell phone networks are evolving to 5G and may be dropping support for older technology. The solution to this, is to update your backup systems any time you upgrade your primary systems, which essentially doubles the costs.

The reason I'm bringing this up is that most companies have some type of Chief Financial Officer (CFO) whose main job is to ensure that the company earns a profit. The CFO is typically towards the top of the org chart in any company, and has major influence over any major decisions. And most CFOs won't want to pay for redundant systems that will only be needed "if" something bad occurs. They'll always be willing to pay for the insurance or protection after the fact, but if they've never lived through a disaster or personally experienced a technology failure they probably won't see the need to pay for redundancy. The only way to have a fighting chance of getting the funds for the redundant systems is if the CISO/CSO is at the same level on the company org chart as the CFO. If you get a job as the cyber security specialist for a company, and you're not at the same level as the CFO then you're going to have a fight on your hands when it comes to funding the redundant systems.

Policies and Procedures

Another subject covered in this chapter is the need for policies and procedures. And, not just to have the policies and procedures, but to ensure that are enforced or are being used as well.

For example, one of the big security issues you've learned about is users selecting weak passwords. You might tell users you want them to only use strong passwords, and even create a policy that says passwords must be at least 10 characters and contain a mix of alphanumeric and special characters. But just having the policy won't help at all unless you have some way to enforce the password selection rules.

You may have noticed that most of the policies discussed in the book may be related to Information Technology, but they're a little outside of what we normally consider Information Technology issues. That is, setting up and enforcing password rules are something a network

administrator will do, but ensuring that employees take their mandatory vacation is typically more of an HR issue.

Cybersecurity Frameworks

When you're first exposed to the lists of policies and procedures it might seem like they might seem a little mysterious. That is, how would anyone know that you need a policy for mandatory vacation? Luckily there are some guidelines, referred to as frameworks, that have well thought out lists of policies and procedures that should be used[1]. Some of the most widely used frameworks are:

- https://www.nist.gov/cyberframework - US National Institute of Standards and Technology (NIST) Framework
- https://www.cisecurity.org/ - The Center for Internet Security Critical Security Controls (CIS)
- https://www.itgovernanceusa.com/iso27002 - The International Standards Organization (ISO) framework

Even though are several frameworks, they all do the same general things. The reason there are multiple frameworks documents is that as the need for cybersecurity became apparent different organizations and industries developed their own sets of standards. Some frameworks are industry specific and were developed to meet the needs of a specific industry, like PCI-DSS which is required in the financial industry, and HIPPA which is required for medical providers. Other frameworks like the NIST and ISO 27002 frameworks are more general and can be applied to almost any company or organization.

Before we look at the policies specified in the frameworks, let me say this about the framework documents. These documents aren't really built for casual reading as they pack a lot of information into a small, concise document. But if you become a cyber security specialist you'll be able to use one of these framework documents as a checklist to ensure that you've covered all your bases. If you want to see this for yourself you can check out the NIST framework at https://www.nist.gov/cyberframework.

Ok, let's get back to the list(s) of policies. As an example, here's the checklist for the policies specified in the NIST framework. Note that this is just part of the framework, the part that deals with policies. Don't worry about understanding all of the policies or trying to memorize the list. At this point in your career you just need to be aware that there lists that have been put together for you to use, and that these lists are pretty comprehensive.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-2: Physical access to assets is managed and protected

[1] https://preyproject.com/blog/en/cybersecurity-frameworks-101/

PR.AC-3: Remote access is managed
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
PR.AT-1: All users are informed and trained
PR.AT-2: Privileged users understand their roles and responsibilities
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.AT-4: Senior executives understand their roles and responsibilities
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
PR.DS-1: Data-at-rest is protected
PR.DS-2: Data-in-transit is protected
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
PR.DS-4: Adequate capacity to ensure availability is maintained
PR.DS-5: Protections against data leaks are implemented
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.DS-7: The development and testing environment(s) are separate from the production environment
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
PR.IP-2: A System Development Life Cycle to manage systems is implemented
PR.IP-3: Configuration change control processes are in place
PR.IP-4: Backups of information are conducted, maintained, and tested
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-6: Data is destroyed according to policy
PR.IP-7: Protection processes are improved
PR.IP-8: Effectiveness of protection technologies is shared
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.IP-10: Response and recovery plans are tested
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
PR.IP-12: A vulnerability management plan is developed and implemented

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2: Removable media is protected and its use restricted according to policy
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4: Communications and control networks are protected
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

If you look at any single policy in the complete framework document, you'll find a crosswalk that includes references to other documents that have more informative text which will explain exactly what needs to be done for this specific policy. For example, here's a list of other documents that will provide a more complete explanation for the first policy in the NIST framework. Each of these documents will contain lengthy explanations. For example, the NIST SP 800-53 document is nearly 500 pages, although not all of it applies to this single policy. In any case, the documents will all provide explanations that won't be exactly the same, but will be very similar to one another. The point to take away is that there are documents that will provide comprehensive explanations for each policy in a framework.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**IS CSC** 1, 5, 15, 16
	COBIT 5 DSS05.04, DSS06.03
	ISA 62443-2-1:2009 4.3.3.5.1
	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
	NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

When you look at the explanations in the detailed documents, a lot of the explanation may seem obvious. For example, NIST SP 800-53 contains the following explanation about passwords. A lot of the language in this policy should seem obvious, but including even the obvious items makes it possible to use this as a checklist to make sure that all of the important items are covered, and nothing is forgotten.

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION For password-based authentication:
(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
(c) Transmit passwords only over cryptographically-protected channels;
(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
(e) Require immediate selection of a new password upon account recovery;
(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
(g) Employ automated tools to assist the user in selecting strong password authenticators; and
(h) Enforce the following composition and complexity rules: [Assignment: organization defined composition and complexity rules]. Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)
(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

I'm going to repeat myself and say that you don't need to worry about any of the details on policies and procedures for this class. At this point you just need to know that the frameworks exist and will provide you with guidance on with policies and procedures. You'll learn the details of the frameworks and specific policies in later classes.

Applying What You've Learned to Your Home System(s)

When we're looking at how this material may be applicable to your personal systems there is one thing you can do. This is creating a personal Disaster Recovery Plan (DRP), which is one the Case Projects you can choose to do for this chapter. When most people think of a DRP they think about creating backups, and then if disaster strikes restoring their data from the backup.

But if you've ever lost a computer or bought a replacement you know it takes a lot more than restoring a backup to get the computer back to the same state as the computer it's replacing. And some of the things you'll need to do will be extremely difficult if you haven't planned ahead and documented passwords, install codes, or other information you need configure the computer.

To ensure you can get a replacement computer running my suggestion isn't that you create a formal DRP document, but that you at least think about the steps you would need to take to recover if your computer or phone were lost, damaged, or destroyed, and collecting all the information you need in one place. I personally gather everything I need in a zipper binder. This mainly includes things like DVDs or thumb drives with the OS ISO and application install files, and a sheet of paper that documents any install codes, passwords, and settings I'll need to restore the system

Here are the things that I document or think about for my DRP:

1. Any changes to the BIOS/UEFI. Before you start this, you'll need to know which key(s) to hit to get into the BIOS/UEFI settings during boot and the BIOS/UEFI password if you set one. You'll also need to know what settings you need to change. For example, enable virtualization, change CPU speed/multiplier, etc.
2. Reinstalling the OS. You will need the install code for the OS, as well as the install media.
3. Creating user accounts. You'll need to know the name(s) used for the accounts.
4. Configuring the network. You will need the network name, password, etc.
5. Reinstalling any hardware devices. For example, printers, cameras, microphones, etc. You may need the device drivers, and driver updates.
6. Reinstalling and configuring any applications. You may need the install media, install codes, and changes to configuration settings.
7. Connect to cloud accounts such as Google, Apple or Microsoft. You will need user names and passwords.
8. Reinstalling data backups. This includes the obvious files, such as those in Documents, My Pictures, Music, etc. But, you should also ensure you're backing up non-obvious files. Because these files are non-obvious files it's hard to know what they are and where they're located, until you need them on the new computer and find they're missing. The ones I've had trouble with are things like virtual machine folders, music editing projects, 3D printing projects, etc.
9. Connect to social media accounts. You will need user names and passwords.

As you can see creating a DRP and collecting the information and items you'll need to restore a computer is much more involved than simply creating a backup of your data and pictures.

And, some of this information, such as install codes, can be hard to locate if you're not meticulous about saving or documenting them. One of the tools I've found that helps me document a computer's hardware and software settings, including install codes, is Belarc Advisor. Belarc is a free tool that I use on all my computers as it quickly creates a succinct

inventory of a computer's hardware and software. If you're interested in using Belarc I've made a video for my PC Hardware class that shows how to download and use it.

https://tonysako.com/home/pc-hardware/pc-hardware-system-inventory-with-belarc-advisor/

Ways to Check Your Comprehension

The test over this chapter, Test 3, won't happen until after you finish all the remaining Modules. If you want check your comprehension you can use the review questions at the end of the chapter or the Practice Test. I don't have the review questions loaded in Canvas, so you'll have to just read them and figure out your answers on your own. Or you could try and connect with some other students in the class and drill each other using these questions.

If you want to use the Practice Test, look in the Test 3 Module in Canvas for the link to a Practice Test 3. You can take the Practice Test as few or as many times as you want. You're not required to take the practice test, but it's also a good way to check your comprehension and prepare for the "real" test.

The Activities for This Section

There are four activities for this section, Hands-On Projects 14-1, 14-2 and 14-3, and a Case Project (writing assignment). Hands-On Projects 14-1 and 14-2 have been designed to provide you with experience with Windows features for creating backups, which are an essential part of resilience. Hands-On Project 14-3 provides you with experience with implementing policies. Some of the key policies for any organization are the password policies, such as minimum length, maximum age, etc. In this project you'll be using Microsoft's Group Policy Editor to see how the password policies are set on a Windows computer.

1. Hands-On Project 14-1: Using Windows File History to Perform Data Backups

The purpose of this assignment is to provide you with experience with using the built-in File History in Windows for creating backups. You don't have to create an actual backup for this exercise, you can just walk through the steps to inspect the various settings. If you decide you want to use this feature, you'll need a drive large enough to hold your backups.

What to submit for Project 14-1:

- Take a screen shot after steps 8, 12, and 16.
- Answer the questions in steps 9, 10, 11, 16 and 17.

2. Hands-On Project 14-2: Viewing and Changing the Backup Archive Bit

The purpose of this assignment is to demonstrate what happens "behind the scenes" in Microsoft's backup system, and how the system knows whether a file has already been backed up or not. Manually setting and clearing this attribute isn't something you'll ever do as these days it's all done by software. But, this might help take some of the mystery out of how

Windows knows whether a file needs to be backed up or not. It might be of interest to note that the archive bit has been around since the original version of DOS, way back in the early 1980s. This assignment requires using a CMD Window, and typing commands to change directories. I've made a video that demonstrates using the CD and DIR commands, which you can watch if you haven't done this before and need some help. The video can be found in Canvas or at:

https://tonysako.com/home/cs150-introduction-to-computer-security/intro-to-computer-security-business-continuity-cd-dir-commands-for-attrib/

What to submit for Project 14-2:

- Take a screen shot after steps 5, 6, and 8.

3. Hands-On Project 14-4: Using Windows Local Security Policy

The purpose of this assignment is to provide you with experience with implementing policies. You'll be using a Microsoft tool called the Local Group Policy Editor to set some password policies. I suggest doing this on your VM. If you decide to do this on your own machine, you might want to restore any setting you change back to its original state before closing the Group Policy Editor. The tool itself should be of interest, especially if you've never had to set password policies before. As you do this exercise, try to keep in mind that password policies are only one set of many security policies that need to be implemented to keep a system secure. You might want to take a few minutes and look at some of the other policies in the Group Policy Editor. But, don't change any other settings, don't change anything unless you know what you're doing as there are some combinations of settings that can make the system impossible to use.

What to submit for Project 14-4:

- Take a screen shot after step 5 before clicking OK.
- Take a screen shot after step 7 before clicking OK.
- Take a screen shot after step 10 before clicking OK.
- Take a screen shot after step 16 before clicking OK.

4. Case Project Homework (Writing Assignment)

Choose one of the following Case projects located at the end of chapter 14: 14-2, 14-4 or 14-7.

If you don't remember what's required you can refer to the Written Project Guidelines document for details on how your paper/report will be graded. You can find the document at:

https://tonysako.com/writingprojectguidelines2021/