`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2022

Technology Track – Session 4

The Small Firm’s 9 Step Data Protection and Disaster Recovery Checklist

James Pearson

About the Presenter...

James Pearson, with over 30 years of experience in the computer industry purchased The Computer Center from its founder Paul Braun after being an employee for ten years. His background has included computer sales, repair, and classroom instruction. He is a Microsoft Certified Professional. James holds a Bachelor of Arts degree in Communications from Beloit College. He remains a resident of Janesville, with his wife, two daughters, and three extra lazy cats. James has been a regular guest on WCLO covering cybersecurity and safety topics including working from home and protecting against phishing scams. He has written 3 IT-related books, and a couple of roleplaying game supplements. He is currently speaking on cybersecurity to small businesses, training their staff on identifying scams and identity thieves, protecting themselves

The Small Firm's 9-Step Data Protection and Disaster Recovery Checklist

By James D. Pearson, IT-Nerd, Author, Speaker, CEO
The Computer Center, Janesville, WI

The Small Firm's 9-Step Data Protection and Disaster Recovery Checklist

Are you concerned about the safety of your data? Are you sure your firm is prepared for a potential disaster, data breach, or ransomware attack? If so, then this seminar is for you! In this seminar, 30-year IT veteran James Pearson will guide you through a simple 9-step checklist you can use to evaluate your current cybersecurity posture and help you determine what security areas you must address. At the end of this seminar, you'll have a practical and cost-effective security checklist you can start implementing yourself or with the assistance of an IT company.

1 INTRODUCTION

Of course, all solo and small firms understand the importance of protecting their data and their clients' data. However, I find that, despite this requirement, most smaller firms have no idea how to start securing their network and protecting their data. Many firms not only lack the technical expertise but an idea of where to begin, but they also believe they don't have the resources (neither time nor money) to implement enough security.

Further, most smaller firms feel that they are not "big enough" or their data isn't "important enough" to become the target of an attack, so security is not high on their priority list. Unfortunately, this couldn't be further from the truth.

Before working through the 9-Step Data Protection and Disaster Recovery Checklist, we must discuss the current cyber threat landscape. Having at least a high-level overview of what's happening and what we are up against is essential.

1.1 ACKNOWLEDGING THE THREAT

Ransomware, identity theft, extortion, and data breaches affect even small firms and can have devastating business and reputational effects. As these threats and techniques adapt and change, so does the need to change your security strategy. So, let's begin by understanding the current state of the cybercrime landscape.

Here are some key factors you must know:

Regardless of size, we have a legal and ethical obligation to protect all PII data.

Personally Identifiable Information (PII) can include names, addresses, a date of birth, social security numbers, driver's licenses, and any other information that is not publicly accessible. PII data is often stored and shared across the Internet. As a result, you must take steps to protect this data from misuse.

> Breach of Security – Wisconsin Statute § 134.98(1)(b) "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable.
>
> SCR 20:1.6 Confidentiality. (d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

After completing this checklist, you can take reasonable and educated efforts to improve your security and protect your data.

1.1.1 Cybercriminals Cast a Wide, Automated Net

Computer criminals use software that scans the Internet for computers with security vulnerabilities. They send millions of emails trying to trick someone into clicking on links that will install ransomware or steal account credentials.

Studies have shown that a hacker locates and attacks a vulnerable computer via the Internet every 39 seconds![1] And, with our own monitoring experiences, we've also seen email and Microsoft account attacks increase, especially from countries like Russia.

1.1.2 The Dark Web is Real

The dark web is a shadowy place where your data is traded instead of in a dark alleyway or seedy bar. And while it may sound like something out of a movie, your credentials may already be available on the dark web. This is because data breaches have become commonplace, with even major corporations like Yahoo! and Equifax falling victim.

The dark web is a part of the Internet that can only be accessed using special software, making it hidden from search engines. Criminals use the dark web to buy and sell stolen data, including login credentials and credit card numbers. Credential theft is on the rise, and we are personally seeing more and more attacks against email, Microsoft, Google, and other vital accounts. Gaining access to these accounts gives cybercriminals incredible power over your identity and data.

1.1.3 Email is Still a Primary Target

Criminals use Phishing and Business Email Compromise (BEC) attacks to pretend to be legitimate emails or even someone else within your organization to fool even the most astute person (including cybercrime experts). Phishing and BEC are threats that target businesses of all sizes.

In a phishing attack, criminals use fraudulent emails or websites to trick victims into disclosing sensitive information, such as login credentials or financial data.

[1] "Hackers Attack Every 39 Seconds | 2017-02-10 | Security Magazine." 10 Feb. 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

BEC attacks involve fraudsters impersonating a high-level executive within an organization to convince employees to wire funds to a bank account controlled by the attacker, purchase gift cards and send the codes via email, or disclose other financial or sensitive data. BEC attacks prey upon people's desire to be helpful and good employees. These attacks are often difficult to detect, as criminals go to great lengths to spoof email addresses and create believable messages. As a result, even the most astute cybercrime experts are sometimes fooled by these attacks.

Cybercriminals take advantage of current events such as COVID-19 and holidays to entice users into interacting with their phishing emails. Russian-based phishing attacks increased by eight times over previous years in February 2022, with scammers taking advantage of the current events and Ukraine Conflict as topics to ensnare unwary users.[2]

1.1.4 Ransomware is Now Extortionware!

In the past, ransomware attackers would encrypt your data and demand a ransom to decrypt it. But now, they're also including extortion in their repertoire of techniques. The threat is that if you don't pay a ransom, they will post about your company's data breach on social media and release your information to others on the dark web. Naturally, this puts you and your clients at more risk.

Not only that, but this type of attack can damage your reputation as a business. People will lose trust in you if they think you can't keep their information safe. So, even if you don't believe that your data has value, your reputation certainly does, and that's what's at risk here now.

- According to Law360, law firm data breaches surged in 2020, and "Small and boutique firms experienced the most data security incidents."[3]
- Law firms are low-hanging fruit because they "obtain, store and use highly sensitive information." As a result, they aren't devoting the attention and resources needed to be secure. As a result, approximately one-third of law firms are breached.[4]
- The ABA's 2021 Cybersecurity report states that up to 50% of firms have experienced a data breach in their lifetime, and this number is growing.[5]
- While many people think of large firms when they hear the term "cybersecurity threat," small firms are just as vulnerable to these attacks. Firms of all sizes need to take steps to protect themselves from cyberattacks. Of course, not all firms, especially firms under ten computers, have the budget or resources to handle their own security. While some of the

[2] "Russian-based phishing attacks increased eight-fold since Feb. 27." 01 Mar. 2022, https://www.scmagazine.com/analysis/phishing/russian-based-phishing-attacks-increased-eight-fold-since-feb-27.

[3] "Law Firm Data Breaches Surged In 2020 - Law360." https://www.law360.com/pulse/articles/1343218/law-firm-data-breaches-surged-in-2020.

[4] "ABA TECHREPORT 2019 - American Bar Association." https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/.

[5] "2021 Cybersecurity - American Bar Association." https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/.

items I'm going to discuss may require you to consult with an outside IT firm, even if you do that, having this checklist to hand over to them will expedite the process.

2 The Small Firm's 9-Step Data Protection and Disaster Recovery Checklist

I've developed this checklist specifically for solo and small firms. I will go through what I believe are the nine most crucial steps you need to take, and can take on your own, to instantly improve your security and sleep better at night knowing you've done your due diligence.

By the end of the seminar, you'll know what security holes are the quickest and easiest to shore up now. You'll learn what you can do, no matter your technical level, and you'll also know when to reach out to an IT company.

My goal here is to help you close as many potential security holes as possible and give you a solid foundation from which to build your cybersecurity plan, either on your own or with the help of a third-party vendor or IT company.

Let's dive in!

2.1 Step 1: Take Inventory and Assess Your Environment.

It is crucial to understand your current situation before implementing a security solution. This inventory step will help you get an understanding of where your current weaknesses are. Without this knowledge, it would be impossible to make any kind of meaningful progress. Therefore, taking the time to assess your current environment and gather information is an essential first step in our planning process.

Many firms don't have good digital document management hygiene, meaning they don't know where all their data is. The goal of cybersecurity is to protect your company from cyberattacks. However, without knowing the status of all data and devices to make informed decisions about how best to maintain this protection, it becomes difficult - if not impossible- to achieve that objective.

Review the items on the checklist and mark them as complete once you have gathered the information. If there are items you are unsure about or need help with, you may need to reach out to an IT professional; skip those for now. It's essential to list the type of data here. A brief note or a mark about it being for client data will suffice. This will help you track what needs to be secured and what doesn't.

Here are some common locations you need to check on:

1. On firm computers
2. On employee's personal devices
3. In the cloud
4. On mobile devices
5. On home computers
6. In your Practice Management Software
7. In your emails
8. OneDrive
9. SharePoint
10. Flash drive
11. External Hard Drives
12. Backup software
13. Google Drive
14. Dropbox
15. Vendors
16. A server
17. Your Desktop (on your computer)
18. My Documents Folders

Any comprehensive approach to data security must begin with an inventory of where your organization's data is stored. The challenge of tracking all data is a daunting one. It often lives on various devices and platforms inside your network or in the cloud with third parties.

Take stock of all your organization's data before you can begin to protect it. Once you have compiled a list of all the places where your data is stored, you can start to put security measures in place to protect it. This may include access control measures such as password protection or encryption or physical security measures such as locked cabinets or restricted server access. By taking inventory of your data stores, you can ensure that all your organization's data is adequately protected.

2.1.1 Remediation

- Consolidate data into fewer, or more manageable locations.
- Set up data policies for retention, storage locations, etc.
- Delete old data.
- Correct inaccurate data with vendors and accounts. Look for old employees, email addresses, passwords, etc.
- Review physical access and secure if needed.

2.2 STEP 2. WHO HAS ACCESS TO THE DATA?

A key element of your plan is knowing who has access to your data and what level of access they have. So what we are trying to accomplish here is a self-audit and awareness of all the different people that come into contact with your data and how much they have access to it.

Especially with small firms, there is usually no formal employee termination process. At most I will find that a password has been changed or a single "master" account removed or disabled. However, any staff member who has spent time with your organization probably has more access to your digital data than you think.

This part of our checklist will help ensure that you begin working towards a process to properly onboard and offboard employees, and uncover what access risks currently exist so they can be remediated. Then, in the future you're going to adopt a Zero Trust model with your current and future staff members.

Under a Zero Trust model, we assume that everyone and everything is untrustworthy until proven otherwise. This approach starts with the most restrictive policies and gradually loosens them as needed. Taking a Zero Trust approach to data security can help ensure that your company's data remains safe and secure.

You wouldn't hand the whole checkbook and the signature stamp to your brand-new bookkeeper - at least not immediately. Security is the same way. Start by not trusting anyone (employees, ourselves, our vendors, our clients) or anything (software, websites, emails) and don't give them access to our data. Then, we give only the absolute minimum access necessary.

So, our next step in the process is to review all the data locations from above and determine who has access to that data and at what level.

This part requires that you have access to the security component of every location you may have listed in your data locations in the step above. Again, this may require the assistance of an IT company or a software vendor.

If you don't have that granular detail, that's ok for now. It's important to just get this done on our worksheet as a place to start.

2.2.1 Remediation

- Review the access levels in your software and restrict them if possible
- Set your shared document links from Microsoft 365 to expire! (Less worry about old links out there)
- Change permissions on folders (server or cloud-based)
- Remove old accounts
- Don't share passwords to vendors' sites, etc.
- Create separate accounts for each user, with minimal permissions needed.
- Use a password manager if needed.

2.3 Step 3. How is Your Data Accessed?

In this step, you will focus now on how the data is accessed. Each point of access can be a potential security risk. Therefore, you want to ensure that you understand how each type of data is accessed so that you can control and limit that access if needed.

How our data is accessed includes physical access to your computers and networks and remote access from devices such as laptops, smartphones, and tablets. Once you've identified all the ways your data is accessed, you need to take steps to secure each entry point. This may include installing physical security measures such as locks and alarms, setting up a password-protected user account, and enabling Multi-Factor Authentication (MFA). By taking these steps, you can help ensure that your data is safe from unauthorized access, even if it is accessed remotely.

Let's begin by listing all the ways that data may be accessed. I've broken these down into the two simple most common access categories you should evaluate. Although you may have additional ways of accessing the data, list those as well.

2.3.1 Local Access

Local access is when you access a computer while physically sitting in front of it. This type of access usually refers to someone who has physical access to the computer and is using it to interact directly with the operating system or software.

> "Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network)."[6]

You and your internal staff are usually sitting at your desks working on your computers. But, it could also include anyone who has access to your office - janitorial staff, IT staff from other companies, and clients who visit your office. It can also be software running on a computer acting as a person, such as using administrative credentials to run a process either legitimately or as part of a malicious attack.

Examples

- Computers at desk
- Server/server room
- Shared equipment such as a front desk, reception, or kiosk computer.
- Access to owner/superior's computer

2.3.1.1 Remediation

- Set computers to automatically lock after a few minutes
- All have passwords for individual accounts, no sharing
- Encrypt local hard drives
- Physically secure locations
- Who has physical keys?
- No password lists on desks/notes/under keyboards
- Do you have a shredding policy for all paper documents?

2.3.2 Remote Access

Remote access is when you access a computer from a remote location. This type of access usually refers to someone using a computer to connect to another computer or server remotely.

> "Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet)."[7]

[6] "local access - Glossary | CSRC - NIST." https://csrc.nist.gov/glossary/term/local_access.

[7] "remote access - Glossary | CSRC - NIST." https://csrc.nist.gov/glossary/term/remote_access.

Examples

- Remote into a server or workstation (using RDP)
- Software like GoToMyPC
- Websites, portals, shopping sites, etc.
- Employees remote into computers?
- Website accounts
- Online portals or software like your Practice Management software
- Dropbox, Onedrive, cloud storage

2.3.2.1 Remediation

- Disable old accounts.
- Password rotations and no sharing.
- Updates and patches.
- Monitoring accounts for unusual activity
- Enable MFA everywhere you can!
- Do you have a VPN for all remote access?
- Are your web pages SSL encrypted?

2.4 Step 4. What about Encryption?

Encrypting your data not only protects it from prying eyes but also has some ramifications regarding data breach reporting requirements. First, there's a safe harbor for data that is encrypted. This means that if someone gets through perimeter security, or you lose your phone, tablet, or laptop if the data is encrypted, then not only is it secure, but you may not have to report it as a data breach.

> Breach of Security – Wisconsin Statute § 134.98(1)
>
> (a)1. Entity means a person, other than an individual, that does any of the following:
>
> Conducts business in this state and maintains personal information in the ordinary course of business.
>
> (b) "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, ***if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable*** (emphasis mine).

There are two types of encryptions to consider: Encryption at rest and in transit.

At rest means that the data is encrypted on the device. This includes your computer's hard drives, tablets, phones, and external devices like flash drives and backup drives.

Even though encrypting mobile devices seems obvious, it's still important to consider encrypting workstation computers.

In transit encryption means that the data is encrypted as it travels from one location to another. This is what we do when we use a VPN to connect to our firm's network. The data traveling across the Internet is encrypted so that if it were intercepted, it could not be read. This is also why it's important to verify that the websites you visit, especially when entering information and credentials, is using encryption (indicated by the "s" it https:// and lock or other indicator in your web browser.

Some things to consider encrypting

- Mobile Devices (phones, tablets, etc)
- Laptops
- Backups - external drives (depends on your software)
- Backups - cloud-based (traditionally encrypted)
- Servers
- Workstations
- Email communications

2.4.1 Remediation

- Turn on encryption on all devices.
- Verify that you can encrypt emails.
- Verify that all backup and external drives are encrypted.

2.5 Step 5. Do you have a Backup Plan?

The next item on our checklist is to create a backup plan for all your firm's data. This is probably one of the most important items on the list! A good backup plan will protect your firm's data in the event of a natural disaster, power outage, system crash, or any other type of data loss. It's currently the only way to restore your data from a successful ransomware attack.

There are two main types of backups - local and cloud-based. Local backups are typically stored on an external hard drive or server, while cloud-based backups are stored off-site (usually with a third-party provider).

Keep in mind that you want to have at least two copies of your data, stored in two different places. That way, if one copy is lost or damaged, you always have a second copy.

Further, it's no longer good enough to simply backup your data once daily. While most small firms feel like they are too small to be considered a target, ransomware software can cripple a firm of any size.

Once ransomware has access to the network it works quietly in the background to scramble all your files and programs, rendering your data and computers useless. This process can take hours or even days before being completed, alerting you by the ransomware software.

Just as a fortress has many layers of defense, so too must your backup be multi-layered to protect against all sorts of attacks. It is your last line of defense against threats such as ransomware.

Here's what to look for in a backup solution:

- **Automated**: in my 35 years of IT work, I have found people don't swap backup disks, never check that they are working, and generally fail at making good backups. Automating your backups is essential, but with the caveats below.
- **Tested**: If you don't check that the backup worked it's worthless. Modern backup solutions can automatically test and verify backups. I can't tell you how many times someone has assured me was their backup was working only to find that nobody had ever verified it by testing the backup. Backups are worthless without tests, so you need some process sot test these backups daily. Newer backup solutions provide data tests and verification and many even scan the backup for suspicious file changes that may signify a ransomware or other malware infection.
- **Off Site:** This protects against natural disasters. separate from the network (isolated or air-gapped) it is sometimes called. It provides the benefit of not being accessible if a ransomware attack is successful on the network. Also, by automating moving your backups offsite, we reduce the chance of human error.
- **Frequent:** Multiple times throughout the day. Consider this; If you have a ransomware infection at 4:30pm, but your last and only backup was done at 11PM the previous day, you've lost nearly an entire day's worth of work and data that would have to be replicated. Backups are targeted by ransomware authors. They are attempting to turn off or disable backup solutions to make ransomware more effective. Consider backing up several times per day.[8] Multiple restore points decrease the potential amount of data lost. A backup every two hours provides more opportunities for a successful backup as well as only two hours of potential work to be recreated
- **Image based**: Frequent snapshots, or images, of an entire critical computer, is the best form of protection and the fastest way to recover from a disaster. By taking a snapshot of a key computer, it can be recovered to the state it was at that time, as opposed to having to reinstall windows and all software, reducing your downtime due to ransomware.
- **Cloud Backups:** Your cloud-based data needs some backup love too. Microsoft does not back up our data. Yes, there is some redundancy, but now that we have ransomware and other malware that can affect your online accounts and data, you need to take a similar approach to back up that data. I recommend a third-party solution that also has encryption and meets all the criteria above.

2.5.1 Remediation

- Automate your backups
- Test your backups frequently
- Store your backups offsite
- Back up multiple times per day

[8] "Backup “Removal” Solutions - From Conti Ransomware With Love - AdvIntel." 29 Sept. 2021, https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love.

- Use an image-based backup
- Back up your cloud data

2.6 Step 6. Protect Your Email.

Most ransomware and credential theft start with an email. Generally, this is a phishing email attempting to trick you into clicking a link or entering further sensitive data like account credentials.

Not only is email one of the biggest productivity killers it's one of the weakest points in security for most organizations. Without taking special precautions, your emails travel through the Internet in plain text. Imagine sending your client a private document about a case via postcard. Anyone that intercepts that postcard along its route to reach the destination can plainly and clearly read its contents.

Personally, I find that email is one of the most challenging things to protect since we interact with it so much more than something like a backup solution. This introduces a significantly higher possibility of human error releasing PII data into the wild (considered a data breach). Further, phishing emails have become more difficult to spot and more sophisticated in recent years.

There are two issues to consider when it comes to protecting email data. First, you must protect data from accidentally going out of your organization via email. This is usually accidental.

Next, you must block incoming threats such as phishing, malicious attachments, links, and even emails constructed to exploit security holes in programs such as Outlook.

For this part of the checklist, review all your email accounts from all sources and who has access to them. Next, review whether or not you need email encryption, spam filtering, or archival in place.

2.6.1 Remediation

- Use a reliable email provider that offers encryption at rest (stored on their servers) as well as in transit (traveling across the Internet.)
- Do NOT use a free email address like @gmail or @yahoo. Not only is it unprofessional, but there is no recourse if there is an issue.
- Enable Multi-Factor Authentication on all email accounts.
- Configure your email client to only display plain text emails by default
- Use strong passwords for each of your firm's email accounts
- Use a quality email filter that blocks things before they end up in your mailbox
- Install and use email encryption software to automatically encrypt accidental outgoing data as well as provide a secure means of communication with clients.
- Find a solution that protects you from malicious links. This is called URL filtering
- Email archiving saves copies of all emails and may even be used to meet legal retention requirements
- Back up your emails throughout the day.

2.7 STEP 7: EDUCATE YOUR EMPLOYEES

We are truly the weakest link in the security chain. While technology can assist in building many great and strong layers of around your data to protect it, at the end of the day if a person with malicious intent wants to get in, they'll find a way.

The best way to combat this is by having firm-wide policies and procedures in place and employee training on best practices for data security. Here are some things you can do:

2.7.1 Remediation

- Implement firm-wide training policies.
- Subscribe to a Phishing testing and training service
- Subscribe to a security training service
- Include this training in your onboarding

2.8 STEP 8: DON'T IGNORE ROUTINE MAINTENANCE.

While fires, flooding and other natural disasters are always a risk, it's ever more likely that you'll have downtime due to a software or hardware glitch or cyber-attack. That's why it's critical to keep your network maintained.

Gone are the days of "set it and forget it." Your network is like a living, breathing entity that needs constant checkups, monitoring, and attention.

For this part of your checklist make a list of everything that needs to be updated, such as every computer, each piece of specialty software and key piece of software you have, and each network device such as an antenna or router.

Enabling Automatic Updates will handle Microsoft Windows patches, and most software will install an updater. However, specialty software, especially if it's practice management software that still resides in your office, may not update automatically. That's why we want that on the list, so we can check it occasionally.

Once you have your inventory of devices and key pieces of software, you can move on to the remediation section. However, if you have 5-10 or more computers, managing updates, even when all this is turned on, can really be a part-time job. Further, updates occasionally break other software or are incompatible with your organization's line of business application. In this case, I recommend you begin working with an outside IT consultant. Our industry can completely manage these updates, control when they are installed, and even pre-vet them for potential conflicts.

2.8.1 Remediation

- Enable Windows automatic updates on all computers.
- Say "Yes" when you are prompted for an update.
- Keep your Practice Management and other specialty programs on the latest versions.
- Keep your computers on overnight to allow patches to install.

- Rebooting can trigger a pending installation, restart before you leave at night.
- Work with an IT company with Patch Management Services
- Check that any backups ran successfully (and test them)
- Is all antivirus software running still?

2.9 Step 9. Canaries in Coal Mines

Now that you've gone through the checklist, taken inventory, assessed your risk environment and begun strengthening your data security it's time to put a couple of important measures in place as early-warning systems to help you react quickly to external threats.

For the workbook, I want you to list anything you get a report from that details any security issues. You may not have these in place right now as a solo or small firm, and that's ok.

If you don't have any reports or warning systems in place, then we want to monitor two things (especially): your Microsoft accounts and the dark web.

Because data breaches can go unannounced for years (Yahoo! for example), monitoring for the release of your credentials and data on the dark web can let you know about breaches that may affect you but came from somewhere else.

You may need to reach out to an IT provider for these services. Do NOT try to access the dark web on your own.

2.9.1 Remediation

- Work with an IT provider for account monitoring.
- Find current data breach risks manually at https://haveibeenpwned.com
- Work with an IT provider to set up dark web monitoring.

Attendees of this seminar are eligible to receive a free dark web credential scan. See the workbook for more information.

The Small Firm's 9-Step Data Protection and Disaster Recovery Checklist

By James D. Pearson, IT-Nerd, Author, Speaker, CEO
The Computer Center, Janesville, WI

The Computer Center

www.computer-center.com

YOUR 9-STEP-SLEEP-EASIER-SECURITY CHECK LIST FOR THE SMALL FIRM

I’ve developed this checklist specifically for solo and small firms with what I believe are the 9 most crucial steps you need to take, and can take on your own, to instantly improve your security and sleep better at night knowing you've done your due diligence.

The Computer Center

www.computer-center.com

9-Step Data Protection and Disaster Recovery Checklist

□ **Step 1: Take inventory and assess your environment.**

Before any sort of plan can be put into place, it is crucial to have a clear understanding of your current situation.

□ **Step 2. Who has access to the data?**

And a key element of our plan is knowing who has access to your data and what level of access they have.

□ **Step 3. How is your data accessed?**

Each point of access can be a potential security risk.

□ **Step 4. What about encryption?**

Encrypting your data not only protects your data from prying eyes, but it also has some ramifications regarding data breach reporting requirements.

□ **Step 5. Do you have a backup plan?**

The next item on our checklist is to create a backup plan for all your firm's data.

□ **Step 6. Protect your email.**

Some statistics state that as much as 90% of ransomware or credential theft starts with an email.

□ **Step 7: Educate your employees.**

The best way to combat this is by having firm-wide policies and procedures in place as well as employee training on data security best practices.

□ **Step 8: Don’t ignore routine maintenance.**

Gone are the days of “set it and forget it.” Your network is like a living, breathing entity that needs constant checkups, monitoring, and attention.

□ **Step 9: Canaries in coal mines.**

Now it’s time to implement some early-warning systems.

STEP 1: TAKE INVENTORY AND ASSESS YOUR ENVIRONMENT.

Review the items on the checklist and mark them as complete once you have gathered the information. If there are items you are unsure about or need help with you may need to reach out to an IT professional, just skip those for now. List the type of data here, just a brief note or a mark about it being for client data. This will help you keep track of what needs to be secured and what doesn't.

1. Step 1: Take Inventory and Assess Your Environment.

Check	**Data Location**	**Describe the Data (Documents, PDFs, Client Facing)**
	On firm computers	
	On employee's personal devices	
	In the cloud	
	On mobile devices	
	On home computers	
	In your Practice Management Software	
	In your emails	
	OneDrive	
	SharePoint	
	Flash drive	
	External Hard Drives	
	Backup software	
	Google Drive	
	Drop box	
	Vendors	
	A server	
	Your Desktop (on your computer)	
	My Documents Folders	

REMEDIATION

- Consolidate data into fewer, or more manageable locations.
- Set up data policies for retention, storage locations, etc.
- Delete old data.
- Correct inaccurate data with vendors and accounts. Look for old employees, email addresses, passwords, etc.
- Review physical access and secure if needed.

NOTES

STEP 2. WHO HAS ACCESS TO THE DATA?

This part requires that you have access to the security component of every location you may have listed in your data locations in the step above. This may require the assistance of an IT company, or the software vendor.

For example, to view the Microsoft access on your accounts you'll need administrative privileges. Here's what that looks like

Check	**Person**	**Data Access**	**Access level (Admin, User, Other)**

REMEDIATION

- Review the access levels in your software and restrict them if possible
- Set your shared document links from Microsoft 365 to expire! (Less worry about old links out there)
- Change permissions on folders (server or cloud based)
- Remove old accounts
- Don’t share passwords to vendors sites, etc.
- Create separate accounts for each user, with the minimal permissions needed.
- Use a password manager if needed.

NOTES

STEP 3. HOW IS THE DATA ACCESSED?

Let's begin by listing all the ways that data can be accessed. I've broken these down into XX simple most common categories of access that you should evaluate. Of course, you may have additional ways of accessing the data.

Check	Person	Accesses	Description
	Computers at desk		
	Server/server room		
	Shared equipment?		
	Access to owner/superiors computer?		

REMEDIATION

Physical

- Set computers to automatically lock after a few minutes
- All have passwords for individual accounts, no sharing
- Encrypt local hard drives
- Physically secure locations
- Who has physical keys?
- No password lists on desks/notes/under keyboards
- Do you have a shredding policy for all paper documents

REMEDIATION

Remote

- Disable old accounts.
- Password rotations and no sharing.
- Updates and patches.
- Monitoring accounts for unusual activity
- Enable MFA everywhere you can!
- Do you have a VPN for all remote access?
- Are your web pages SSL encrypted?

NOTES

STEP 4. AND WHAT ABOUT ENCRYPTION?

Encrypting your data not only protects it from prying eyes, but it also has some ramifications regarding data breach reporting requirements.

At rest means that the data is encrypted on the device

In transit encryption means that the data is encrypted as it travels from one location to another.

check	Encrypted	Device (list them below and a blank line or two)

REMEDIATION

- Turn on encryption on all devices.
- Verify that you can encrypt emails.
- Verify that all backup and external drives are encrypted.

NOTES

STEP 5. DO YOU HAVE A BACKUP PLAN?

Once ransomware has access to the network it works quietly in the background to encrypt all your files and programs, rendering your data and computers useless. This process can take hours or even days before being completed an you are alerted by the ransomware software that the process is completed. Simply having one backup a night is no longer enough.

Check	What is being backed up	How	Schedule	verification	where to	encryption

REMEDIATION

- Automate your backups
- Test your backups frequently
- Store your backups offsite
- Back up multiple times per day
- Use an image-based backup
- Back up your cloud data

NOTES

STEP 6. PROTECT YOUR EMAIL.

Most ransomware and credential theft start with an email. Generally, this is a phishing email attempting to trick you into clicking a link or entering further sensitive data like account credentials. Not only is email one of the biggest productivity killers it’s one of the weakest points in security for most organizations

Check	[email provider] - [backup provider] - [frequency] - [archival frequency] -[MFA]

REMEDIATION

- Use a reliable email provider that offers encryption at rest (stored on their servers) as well as in transit (traveling across the internet.)
- Do NOT use a free email address like @gmail or @yahoo. Not only is it unprofessional, but there is no recourse if there is an issue.
- Enable Multi-Factor Authentication on all email accounts.
- Configure your email client to only display plain text emails by default
- Use strong passwords for each of your firm's email accounts
- Use a quality email filter that blocks things before they end up in your mailbox
- Install and use email encryption software to automatically encrypt accidental outgoing data as well as provide a secure means of communication with clients.
- Find a solution that protects you from malicious links. This is called URL filtering
- Email archiving saves copies of all emails and may even be used to meet legal retention requirements
- Back up your emails throughout the day.

NOTES

STEP 7: EDUCATE YOUR EMPLOYEES

We are truly the weakest link in the security chain. While technology can assist in building many great and strong layers of around your data to protect it, at the end of the day if a person with malicious intent wants to get in, they'll find a way.

The best way to combat this is by having firm-wide policies and procedures in place as well as employee training on data security best practices.

Check	Employee	phishing	security	data breach response	Application/ Software

REMEDIATION

- Implement firm-wide training policies.
- Subscribe to a Phishing testing and training service
- Subscribe to a security training service
- Include this training in your onboarding

NOTES

STEP 8: DON’T IGNORE ROUTINE MAINTENANCE.

Gone are the days of “set it and forget it.” Your network is like a living, breathing entity that needs constant checkups, monitoring, and attention. For this part of your checklist make a list of everything that needs to be updated, such as every computer, each piece of specialty software and key piece of software you have, and each network device such as an antenna or router.

Check	**Maintenance Checklist**
	Patches on all computers
	Is AV Up to date ?
	Did the backup run ?
	Did you test the backup ?
	Update routers.

REMEDIATION

- Enable Windows automatic updates on all computers.
- Say “Yes” when you are prompted for an update.
- Keep your Practice Management and other specialty programs on the latest versions.
- Keep your computers on overnight to allow patches to install.
- Rebooting can trigger a pending installation, restart before you leave at night.
- Work with an IT company with Patch Management Services
- Check that any backups ran successfully (and test them)
- Is all antivirus software running still?

NOTES

STEP 9. CANARIES IN COAL MINES

If you don’t have any reports or warning systems in place, then what we want to do is monitor two things (especially), and those are your Microsoft accounts and the dark web.

Check	**Reporting in place**
	Network access
	Microsoft accounts
	Dark web credential exposures
	Antivirus health
	Computer health (drive space, issues, etc.)

REMEDIATION

- Work with an IT provider for account monitoring.
- Find current data breach risks manually at https://haveibeenpwned.com
- Work with an IT provider to set up dark web monitoring.

Attendees of this seminar are eligible to receive a free dark web credential scan.

Visit:

https://www.computer-center.com/wssfc2022

NOTES

THE SMALL FIRM'S 9-STEP DATA PROTECTION AND DISASTER RECOVERY CHECKLIST-OUTLINE

TODAY'S GOAL

At the end of this seminar, you'll have:

- A better understanding of the threats
- A better understanding of your IT environment
- A checklist of security-related issues
- Practical and cost-effective action steps to instantly improve your network security

ABOUT THE CHECKLIST

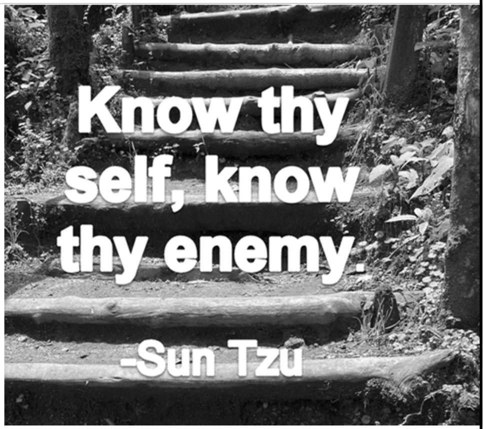
Designed to answer these questions:

- Are the cybercriminals *really* out to get *me?*
- Is all this security really necessary?
- Is it really that expensive?
- Can't I just do it myself?

SEE THE WORKBOOK!

See the accompanying workbook for:

- The Checklist
- Worksheets
- Remediation steps



Regardless of size, we have a legal and ethical obligation to protect all PII data

OBLIGATION

Breach of Security – Wisconsin Statute § 134.98(1)(b) "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable.

SCR 20:1.6 **Confidentiality.** (d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

THE CYBERCRIME LANDSCAPE

- Cybercriminals cast a wide, automated net
- The dark web is real
- Email is still a primary target
- Ransomware is now extortionware!

ACKNOWLEDGING THE THREAT

- According to Law360, law firm data breaches surged in 2020, and "Small and boutique firms experienced the most data security incidents."
- The ABA's 2019 Tech report reminds us that Law firms are low-hanging fruit because they "obtain, store and use highly sensitive information." As a result, they aren't devoting the attention and resources needed to be secure
- The ABA's 2021 Cybersecurity report states that up to 50% of firms have experienced a data breach in their lifetime, and this number is growing
- While many people think of large firms when they hear the term "cybersecurity threat," small firms are just as vulnerable to these attacks

ARE YOUR CREDENTIALS EXPOSED?

Take action right now to check your credentials on the dark web:

FREE DARK WEB CREDENTIAL VERIFICATION ($97.00 VALUE):

https://www.computer-center.com/wssfc2022

The Computer Center

www.computer-center.com

THE SMALL FIRM'S 9-STEP DATA PROTECTION AND DISASTER RECOVERY CHECKLIST

- ✓ Take Inventory
- ✓ Who has access
- ✓ How is data accessed
- ✓ What is encrypted
- ✓ What is being backed up
- ✓ Protecting email
- ✓ Education
- ✓ Maintenance
- ✓ Canaries in coal mines

The Computer Center

www.computer-center.com

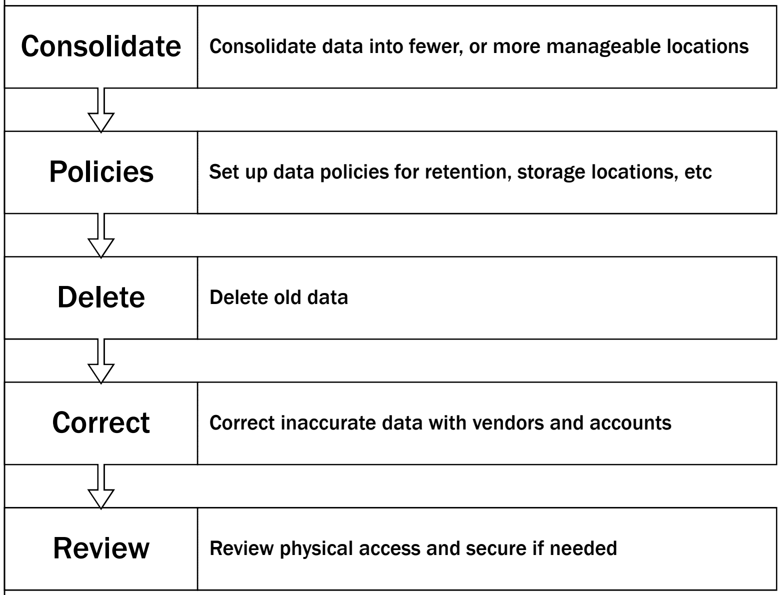
STEP 1: TAKE INVENTORY AND ASSESS YOUR ENVIRONMENT

WHERE IS YOUR DATA NOW?

- On firm computers
- On employee's personal devices
- In the cloud
- On mobile devices
- On home computers
- In your Practice Management Software
- In your emails
- OneDrive
- SharePoint
- Flash drive
- External Hard Drives
- Backup software
- Google Drive
- Dropbox
- Vendors
- A server
- Your Desktop
- My Documents Folders

The Computer Center

STEP 1: REMEDIATION



Consolidate: Consolidate data into fewer, or more manageable locations

Policies: Set up data policies for retention, storage locations, etc

Delete: Delete old data

Correct: Correct inaccurate data with vendors and accounts

Review: Review physical access and secure if needed

The Computer Center

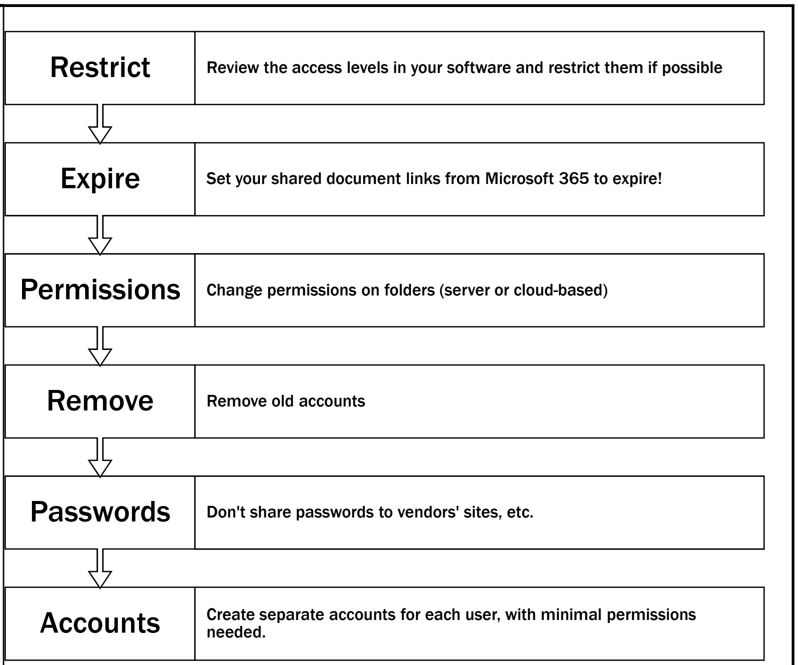
STEP 2. WHO HAS ACCESS TO THE DATA?

- Employees (past and present)
- Vendors
- Partners & contractors
- Clients

- What can they access?
- What privileges do they have?

www.computer-center.com

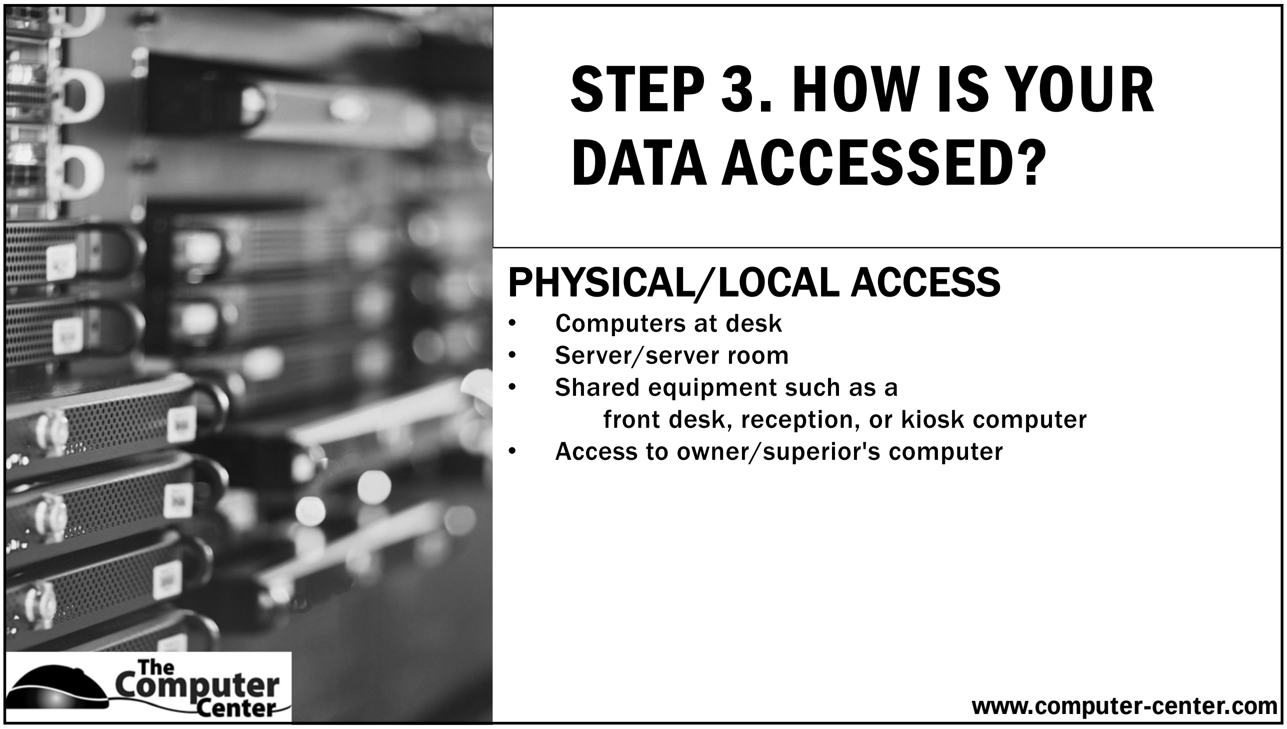
STEP 2: REMEDIATION



Restrict	Review the access levels in your software and restrict them if possible
Expire	Set your shared document links from Microsoft 365 to expire!
Permissions	Change permissions on folders (server or cloud-based)
Remove	Remove old accounts
Passwords	Don't share passwords to vendors' sites, etc.
Accounts	Create separate accounts for each user, with minimal permissions needed.

The Computer Center

www.computer-center.com

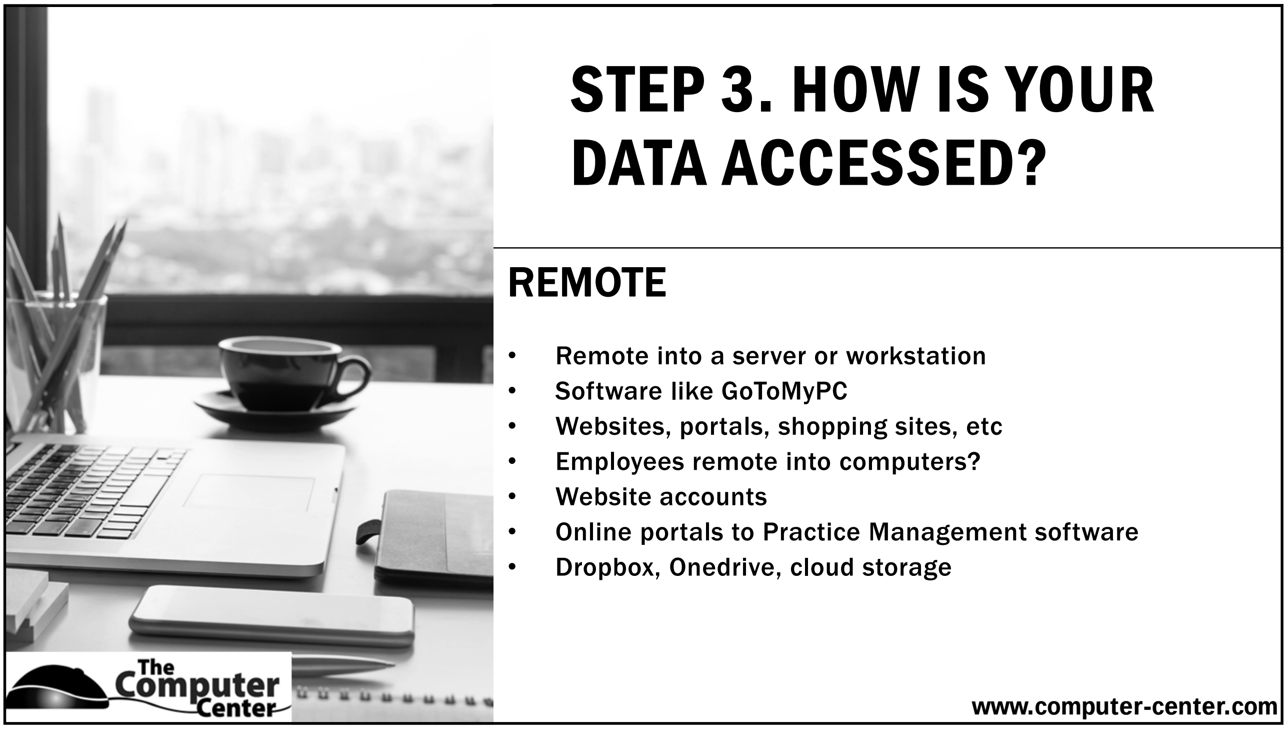


STEP 3. HOW IS YOUR DATA ACCESSED?

PHYSICAL/LOCAL ACCESS

- Computers at desk
- Server/server room
- Shared equipment such as a
  front desk, reception, or kiosk computer
- Access to owner/superior's computer

www.computer-center.com



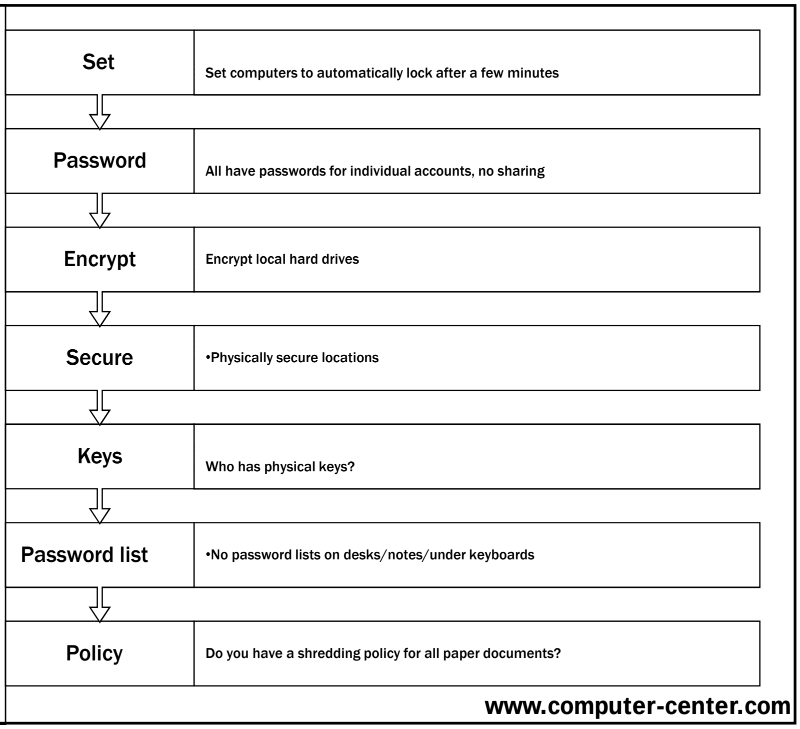
STEP 3. HOW IS YOUR DATA ACCESSED?

REMOTE

- Remote into a server or workstation
- Software like GoToMyPC
- Websites, portals, shopping sites, etc
- Employees remote into computers?
- Website accounts
- Online portals to Practice Management software
- Dropbox, Onedrive, cloud storage

www.computer-center.com

STEP 3: REMEDIATION



Set — Set computers to automatically lock after a few minutes

Password — All have passwords for individual accounts, no sharing

Encrypt — Encrypt local hard drives

Secure — •Physically secure locations

Keys — Who has physical keys?

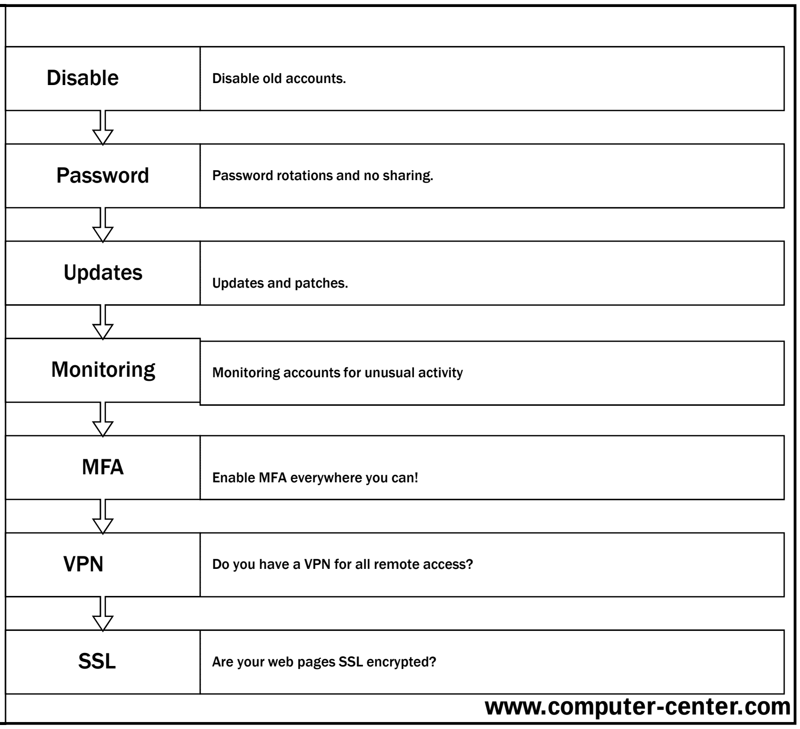
Password list — •No password lists on desks/notes/under keyboards

Policy — Do you have a shredding policy for all paper documents?

The Computer Center

www.computer-center.com

STEP 3: REMEDIATION



Disable — Disable old accounts.

Password — Password rotations and no sharing.

Updates — Updates and patches.

Monitoring — Monitoring accounts for unusual activity

MFA — Enable MFA everywhere you can!

VPN — Do you have a VPN for all remote access?

SSL — Are your web pages SSL encrypted?

The Computer Center

www.computer-center.com

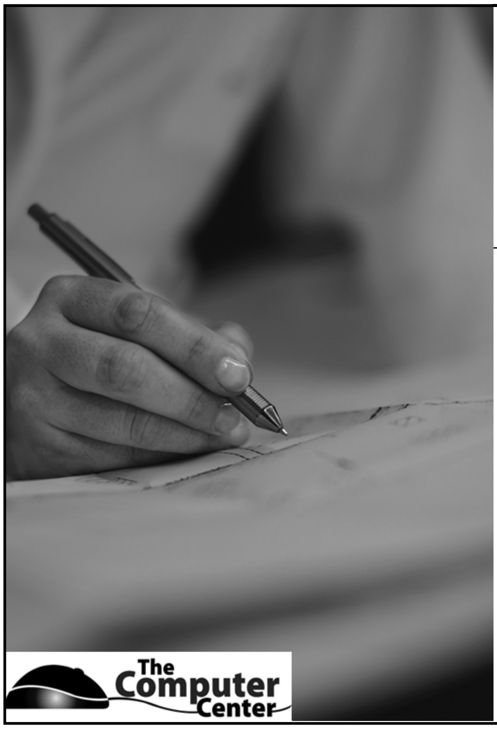
STEP 4. WHAT ABOUT ENCRYPTION?

Breach of Security – Wisconsin Statute § 134.98(1)

(a)1. Entity means a person, other than an individual, that does any of the following:

Conducts business in this state and maintains personal information in the ordinary course of business.

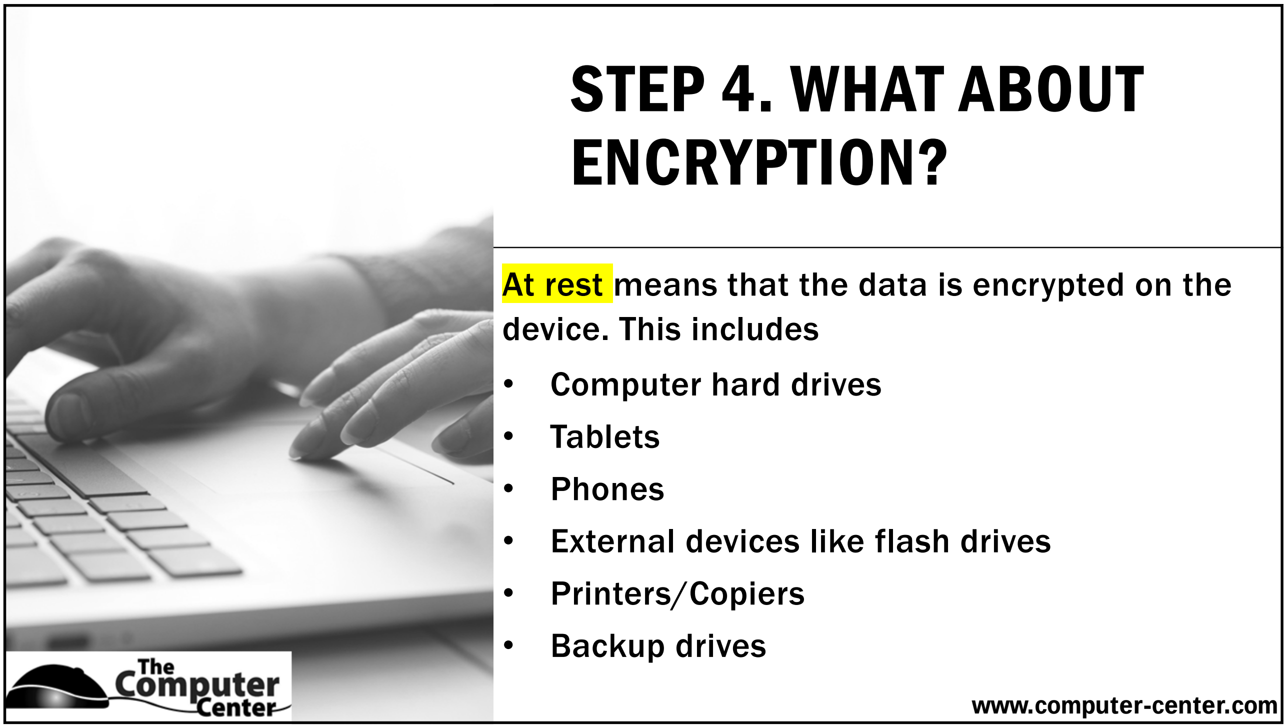
(b) "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, ***if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable*** (emphasis mine).



STEP 4. WHAT ABOUT ENCRYPTION?

There are two types of encryption we are going to discuss:

1. At rest
2. In transit

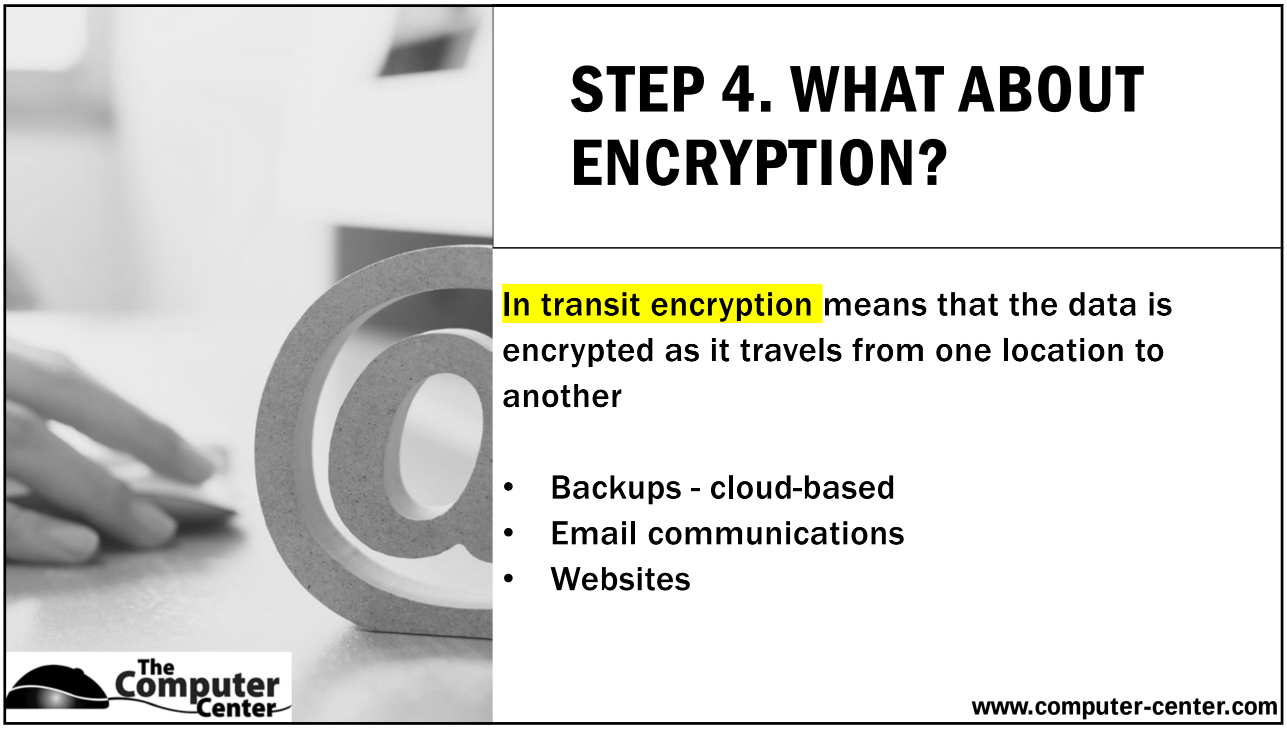


STEP 4. WHAT ABOUT ENCRYPTION?

At rest means that the data is encrypted on the device. This includes

- Computer hard drives
- Tablets
- Phones
- External devices like flash drives
- Printers/Copiers
- Backup drives

www.computer-center.com



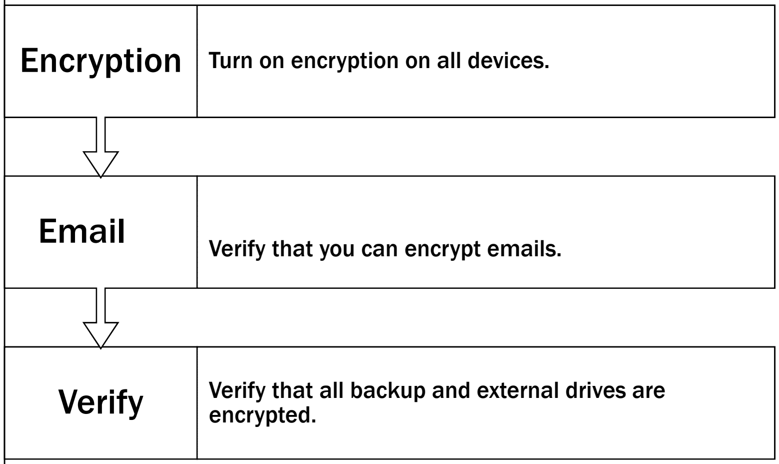
STEP 4. WHAT ABOUT ENCRYPTION?

In transit encryption means that the data is encrypted as it travels from one location to another

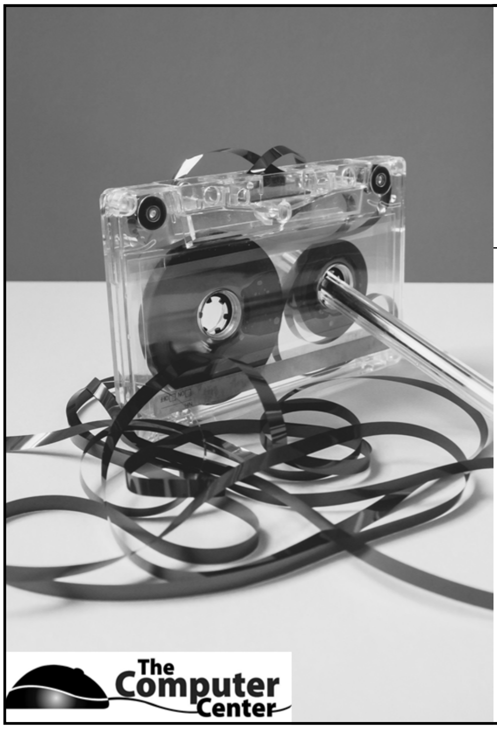
- Backups - cloud-based
- Email communications
- Websites

www.computer-center.com

STEP 4 : REMEDIATION



Encryption	Turn on encryption on all devices.
Email	Verify that you can encrypt emails.
Verify	Verify that all backup and external drives are encrypted.



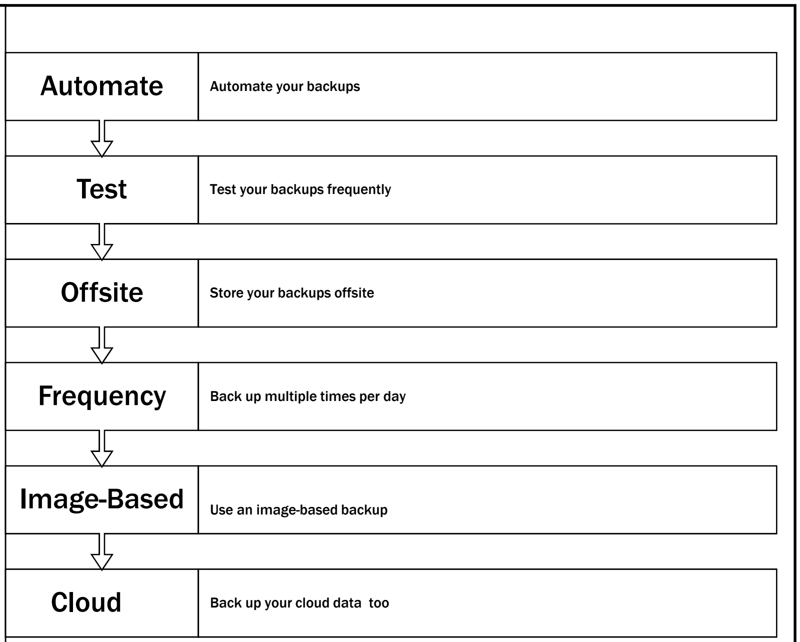
STEP 5. WHAT’S YOUR BACKUP PLAN?

CREATE A BACKUP PLAN FOR ALL YOUR FIRM'S DATA

Redundancy, Redundancy, Redundancy!
-**Department of Redundancy Department** *(and your IT guys)*

- **What is being backed up now?**
- **What is NOT?**
- **How quickly can you recover from a data loss?**

STEP 5 : REMEDIATION



Automate	Automate your backups
Test	Test your backups frequently
Offsite	Store your backups offsite
Frequency	Back up multiple times per day
Image-Based	Use an image-based backup
Cloud	Back up your cloud data too

www.computer-center.com

STEP 6. PROTECT YOUR EMAIL

TWO MAIN THREATS

- Protect data from accidentally going out
- Block incoming threats

www.computer-center.com

STEP 6. PROTECT YOUR EMAIL

For this part of the checklist

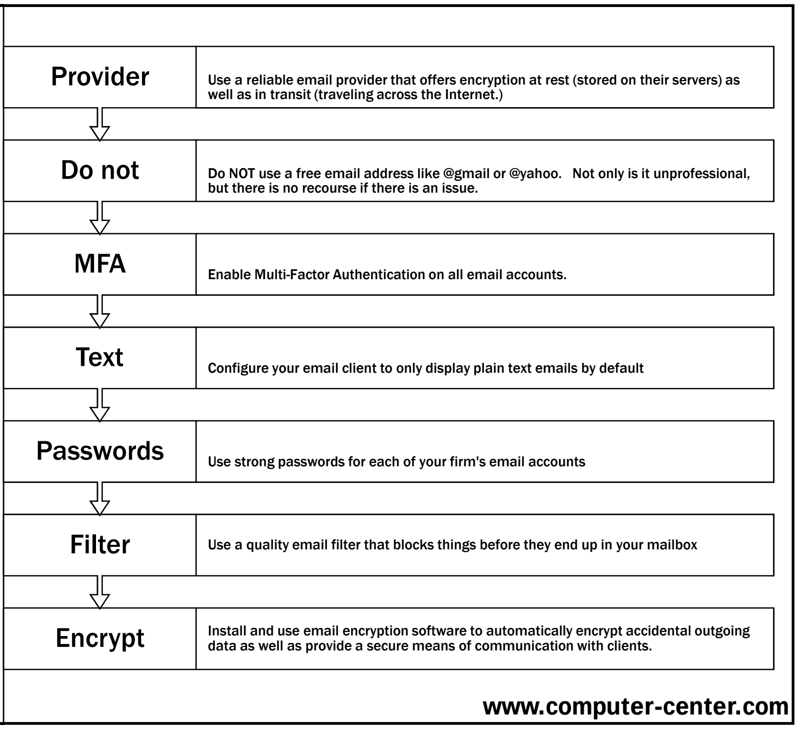
- Review all your email accounts
- Who has access to them

Review whether or not you need:

- encryption
- spam filtering
- archival

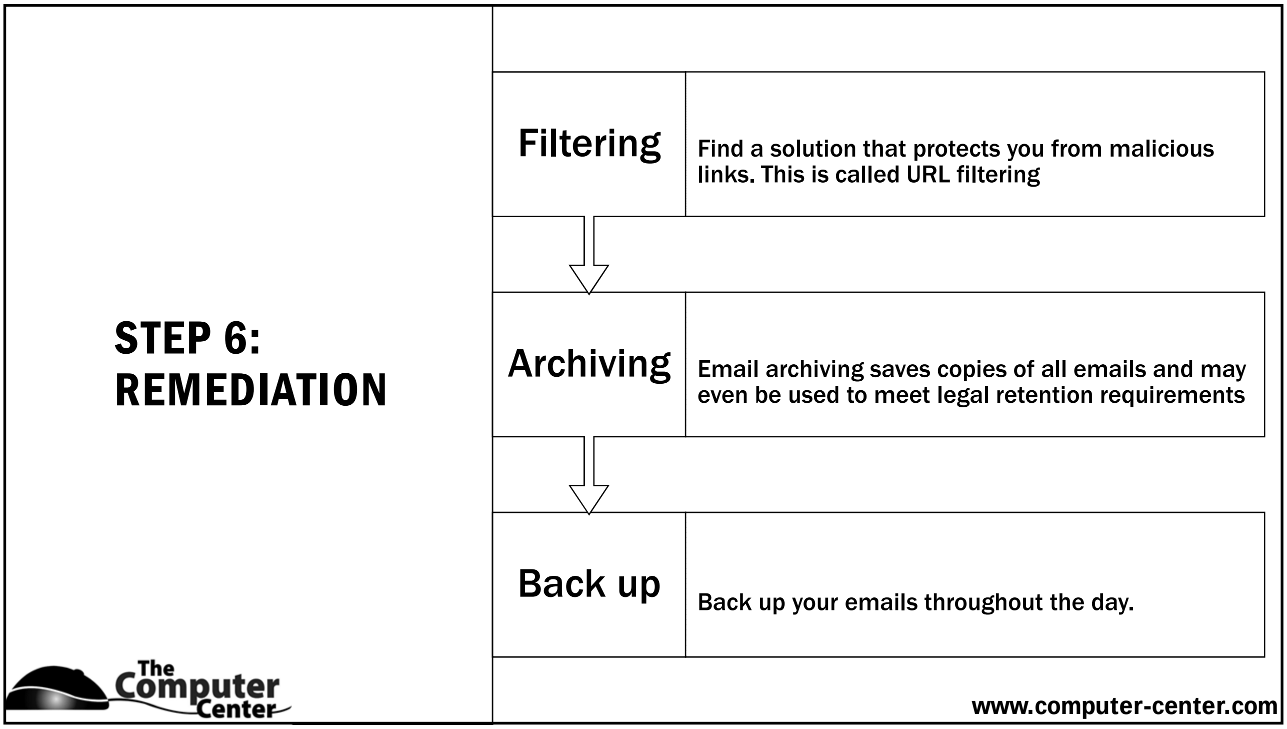
www.computer-center.com

STEP 6 : REMEDIATION



Provider	Use a reliable email provider that offers encryption at rest (stored on their servers) as well as in transit (traveling across the Internet.)
Do not	Do NOT use a free email address like @gmail or @yahoo. Not only is it unprofessional, but there is no recourse if there is an issue.
MFA	Enable Multi-Factor Authentication on all email accounts.
Text	Configure your email client to only display plain text emails by default
Passwords	Use strong passwords for each of your firm's email accounts
Filter	Use a quality email filter that blocks things before they end up in your mailbox
Encrypt	Install and use email encryption software to automatically encrypt accidental outgoing data as well as provide a secure means of communication with clients.

www.computer-center.com



STEP 6: REMEDIATION

Filtering

Find a solution that protects you from malicious links. This is called URL filtering

Archiving

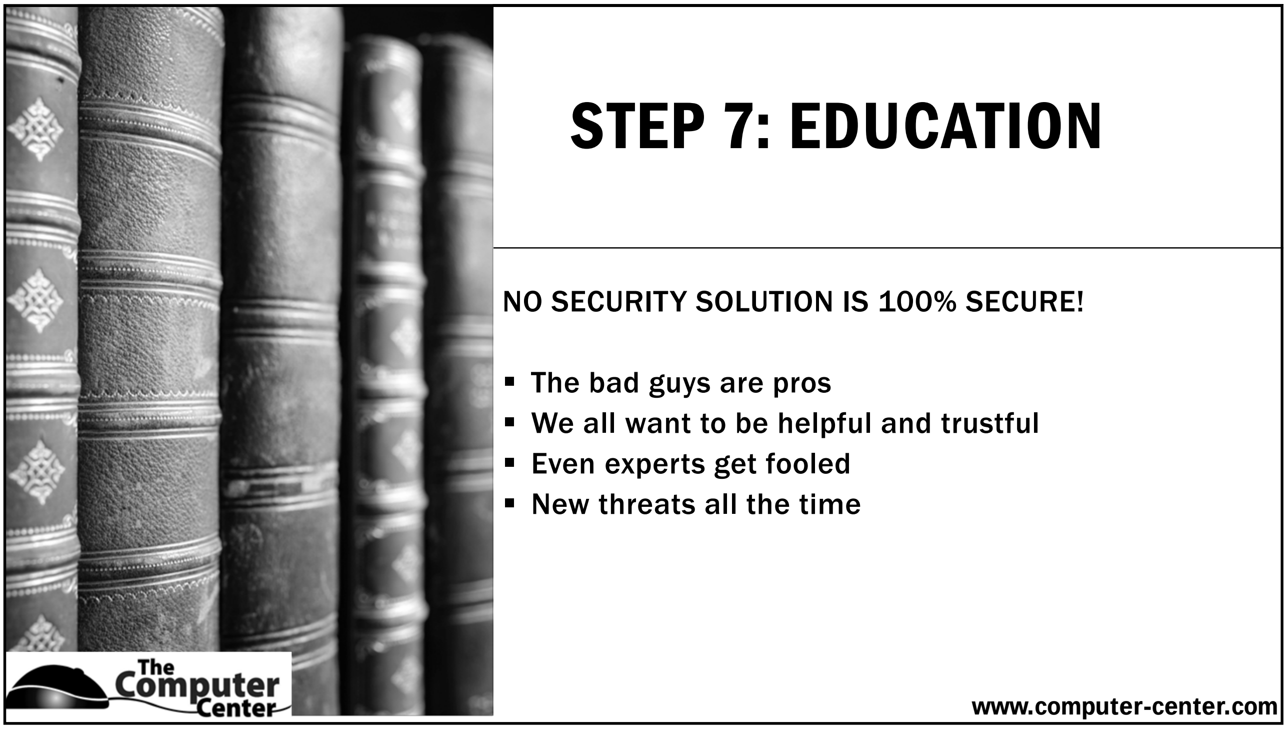
Email archiving saves copies of all emails and may even be used to meet legal retention requirements

Back up

Back up your emails throughout the day.

The Computer Center

www.computer-center.com



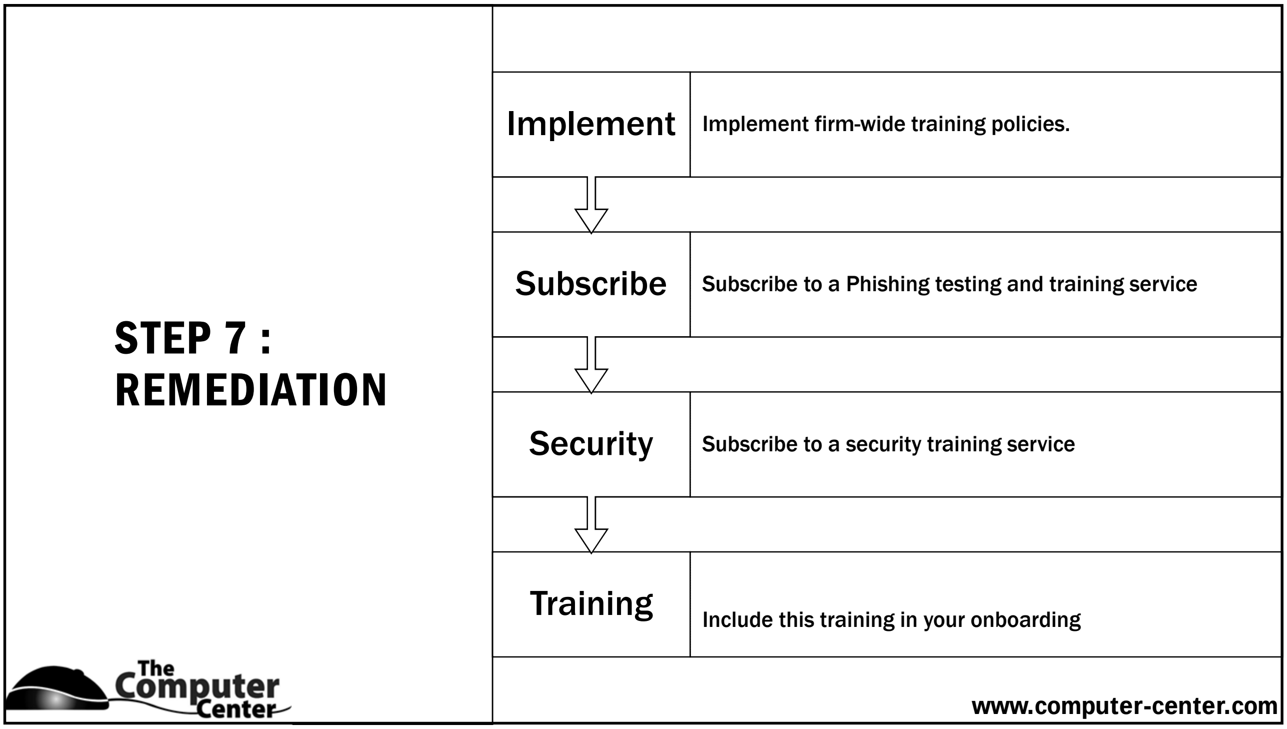
STEP 7: EDUCATION

NO SECURITY SOLUTION IS 100% SECURE!

- The bad guys are pros
- We all want to be helpful and trustful
- Even experts get fooled
- New threats all the time

The Computer Center

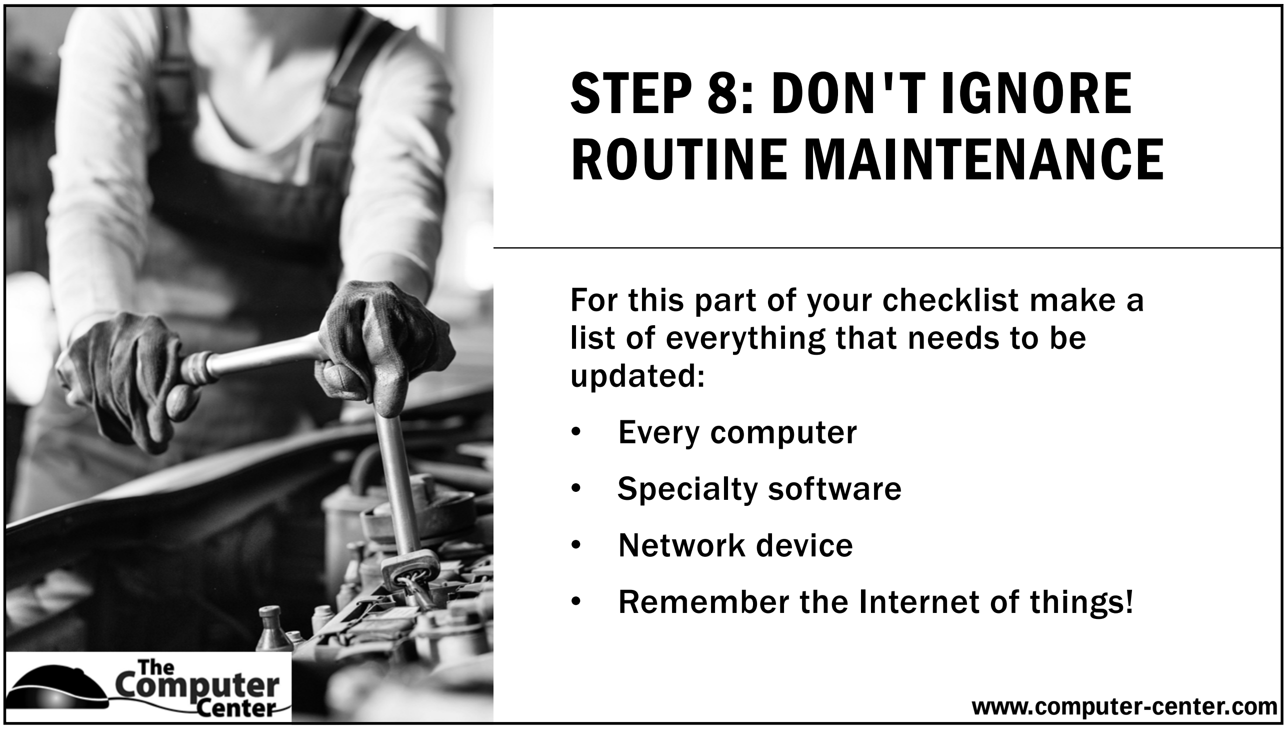
www.computer-center.com



STEP 7 : REMEDIATION

Implement	Implement firm-wide training policies.
Subscribe	Subscribe to a Phishing testing and training service
Security	Subscribe to a security training service
Training	Include this training in your onboarding

www.computer-center.com



STEP 8: DON'T IGNORE ROUTINE MAINTENANCE

For this part of your checklist make a list of everything that needs to be updated:

- Every computer
- Specialty software
- Network device
- Remember the Internet of things!

www.computer-center.com

STEP 8: REMEDIATION

Windows	Enable Windows automatic updates on all computers.
Updates	Say "Yes" when you are prompted for an update.
Practice Management	Keep your Practice Management and other specialty programs on the latest versions.
Install	Keep your computers on overnight to allow patches to install.
Rebooting	Rebooting can trigger a pending installation, restart before you leave at night.
Patching	Work with an IT company with Patch Management Services
Backups	Check that any backups ran successfully (and test them)
Antivirus	Is all antivirus software running still?

The Computer Center

www.computer-center.com

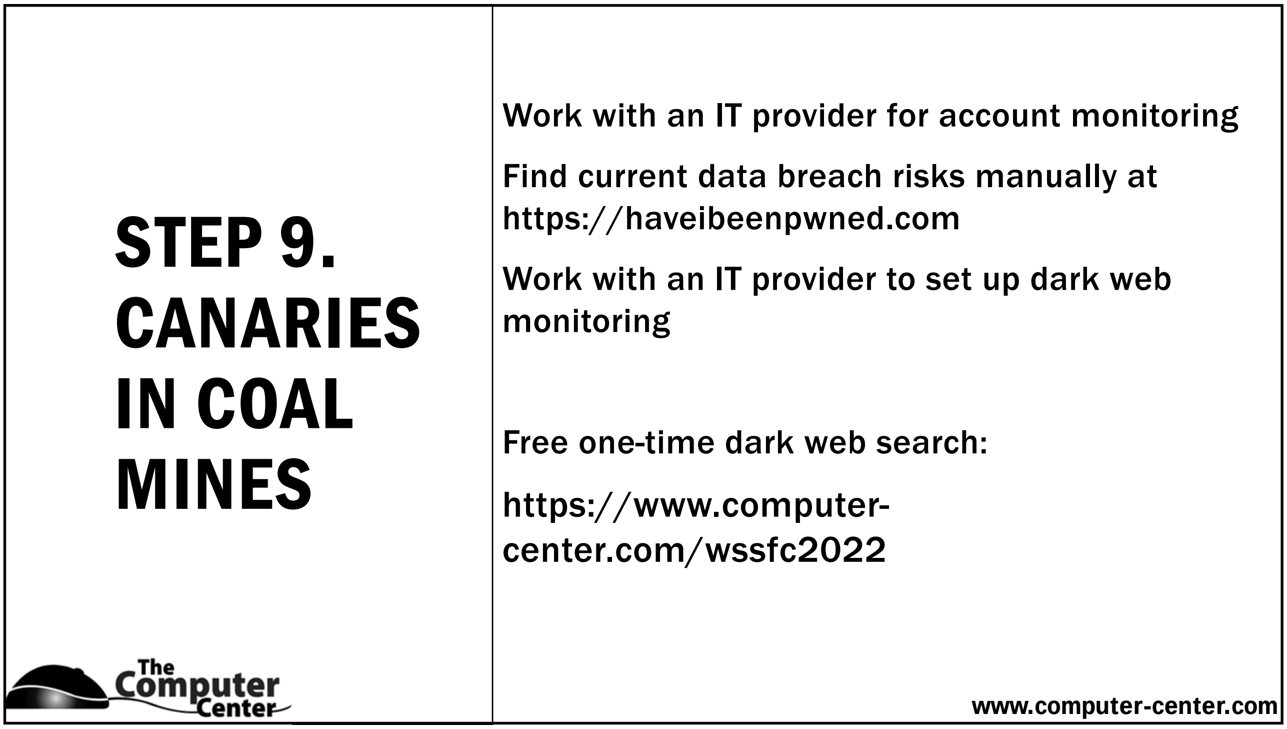
STEP 9: CANARIES IN COAL MINES

What early warning systems do you have in place?

- What reports do you/can you get?
- How do you know when something fails?
- Who is watching your accounts?

The Computer Center

www.computer-center.com



STEP 9. CANARIES IN COAL MINES

Work with an IT provider for account monitoring

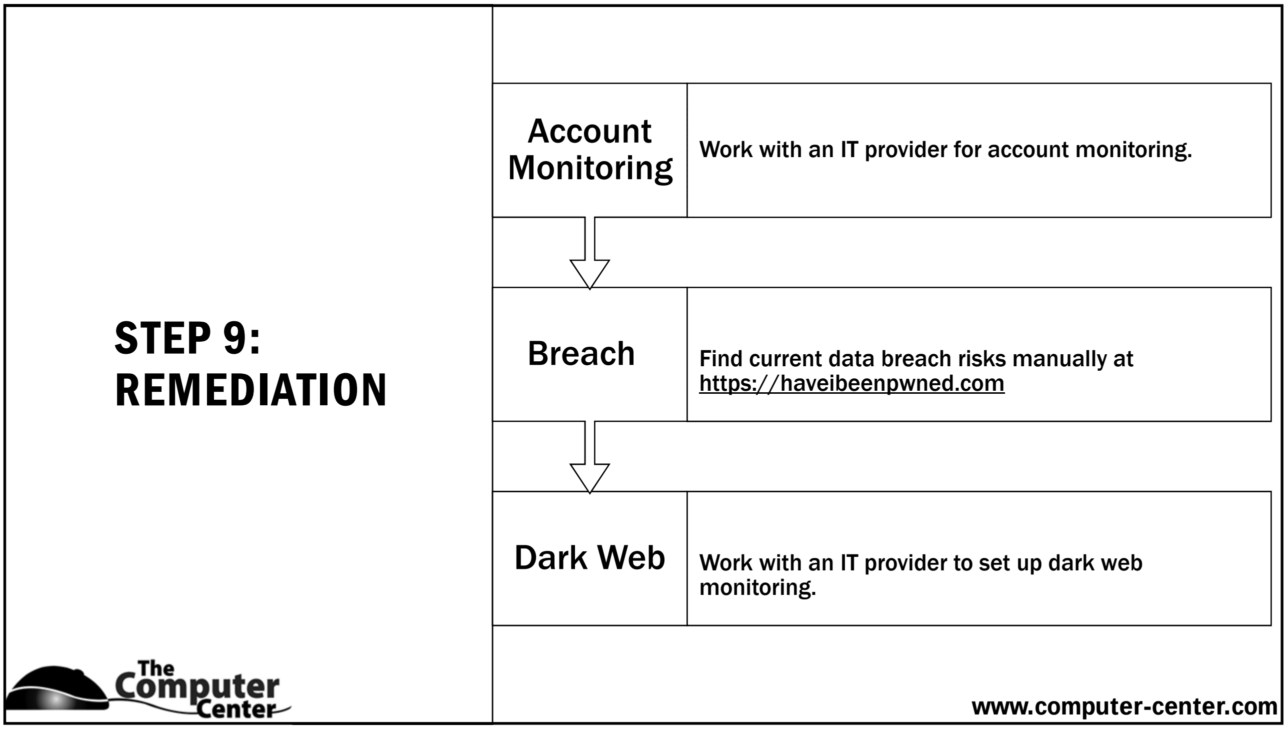
Find current data breach risks manually at https://haveibeenpwned.com

Work with an IT provider to set up dark web monitoring

Free one-time dark web search:

https://www.computer-center.com/wssfc2022

www.computer-center.com



STEP 9: REMEDIATION

Account Monitoring

Work with an IT provider for account monitoring.

Breach

Find current data breach risks manually at https://haveibeenpwned.com

Dark Web

Work with an IT provider to set up dark web monitoring.

www.computer-center.com

KEY TAKEAWAYS!

- Regardless of size, you are a target
- There’s a responsibility to protect data
- Avoid data breaches in the first place
- Take inventory & know your environment
- Plug as many holes as possible
- Take a Zero Trust approach
- Start monitoring accounts, dark web
- Work with an IT provider – prevention is less costly than remediation

QUESTIONS?

James Pearson

James.pearson@computer-center.com

Remember your free dark web scan
https://www.computer-center.com/wssfc2022