HANI ESHACK | CRITICAL IT SOLUTIONS | DMV
240-442-2960
WWW.CRITICALITSOLUTIONS.COM
INFO@CRITICALITSOLUTIONS.COM

CYBER-SECURING *our* FUTURE

QUARTERLY

ed. 3

CONTENTS

INTRODUCTION

Hello,

By picking up or viewing this magazine, you've already taken the first step to becoming more cyber-secure in your everyday life! **Critical IT Solutions** is happy to bring you the latest updates in the cybersecurity industry EVERY QUARTER because the more you know, the better protected you'll be - in your personal *and* professional life!

Think about the state of the internet when you were born versus where it's at today. Pre-internet and old dial-up computer users remember how it was before smartphones were in every pocket, tracking your every move and helping people navigate every aspect of their busy, modern lives.

Technology is not just here to stay. It is constantly advancing and evolving. How is that changing our approaches to cybersecurity?

That's what we're here to investigate for you.

LET'S GET STARTED

ABOUT US

For a sense of cybersecurity now and going forward, this is Cybersecuring Our Future Quarterly.

Hi there! I'm a cybersecurity expert with **Critical IT Solutions, LLC** who is dedicated to fighting the never-ending threat of cyberattacks on behalf of you and your data. We're dedicated to keeping your private information, private!

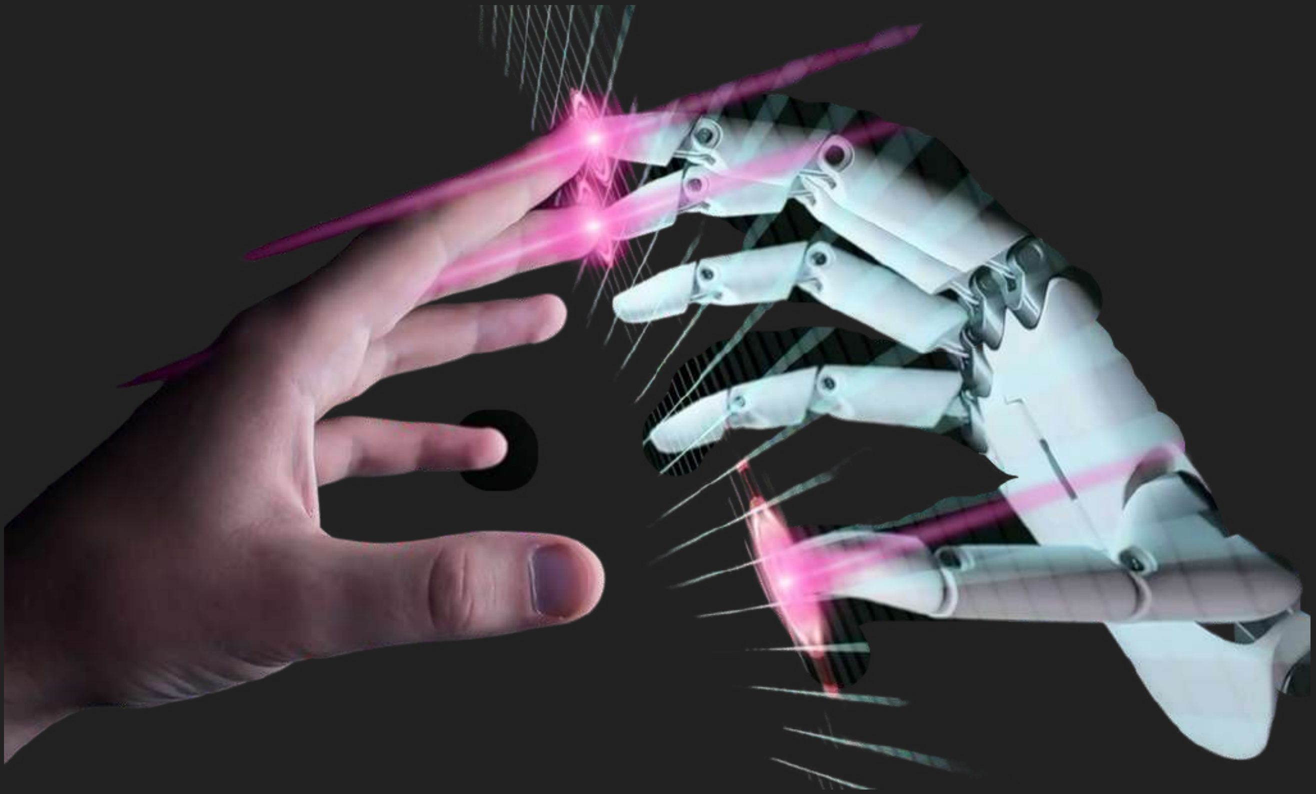
First, I want to thank you for picking up this magazine and joining the fight against cyber-threats to you and your business! Education is the first (and most important) step toward preventing insider and outsider threats from attacking your personal data.

That's what we do here at Critical IT Solutions. We future proof your IT for future ready business.

Bringing you this magazine every quarter is my way of bringing accessible cybersecurity tips and industry knowledge right to your front door — and your coffee table!

“Technology is best when it brings people together.”

- Matt Mullenweg, Founder of WordPress



SMART CARS GET DUPED

new security flaw found in millions of vehicles

Cars can do almost anything these days. You can cool off while playing music on Bluetooth. You can chat with the console to ask for directions. They know when you're straying over the yellow lines, and some cars can even predict and then *stop* a collision!

With all that automation and advanced technology, it shouldn't surprise you at this point that cybercriminals are finding ways to exploit and hack into your smart cars. They can remotely unlock your doors or track your GPS location, if they know how to do it.

Recently, experts identified at least 20 flaws in the API security that's used in **16 major car manufacturers.**

Mercedes, BMW, Ferrari, Jaguar, Porsche, Toyota, Landrover, and Rolls Royce were amongst the car models at risk. Altogether, millions of vehicles could be in danger because of these vulnerabilities.

If these cars are exploited, hackers would be able to...

- take over accounts as either an employee or customer via a remote code execution (RCE)
- sneak into your single sign-on accounts and use internal apps
- find your sales documents, including your name, address and phone number
- find the car's unique VIN
- get your location
- take over everything from golf carts to ambulances

They could do something as physically dangerous as stopping your car'se enginer, to something as distressing as identity theft. Even cars aren't safe from the Dark Web!

> ”
>
> MILLIONS COULD BE AT RISK

YOU CAN SLEEP EASY.

These 16 affected manufacturers have released patches for the API vulnerabilities. The mere existence of these security flaws, however, demonstrate how wide a reach that the Internet has over our daily lives and how threat actors will look for a way to exploit every inch of it.

This also shows why we need to make software updates automatically or ASAP, to patch dangerous vulnerabilities before they're exploited. Make sure you're keeping an eye on your manufacturers' announcements about potential threats to your internet-connected devices, and when new updates come out to keep you safer.

WHAT IS API?

An *Application Programming Interface* lets software communicate with each other. API exploits take advantage of API vulnerabilities, which are basically weak spots in the armor.

These vulnerabilities can be manipulated and exposed so that a cybercriminal can steal data or affect internal processes on the target system.

TOP THIRD-PARTY RISKS TO YOU:

1. Financial/ reputational

Risks that would affect your revenue, etc.

2. Legal/regulatory

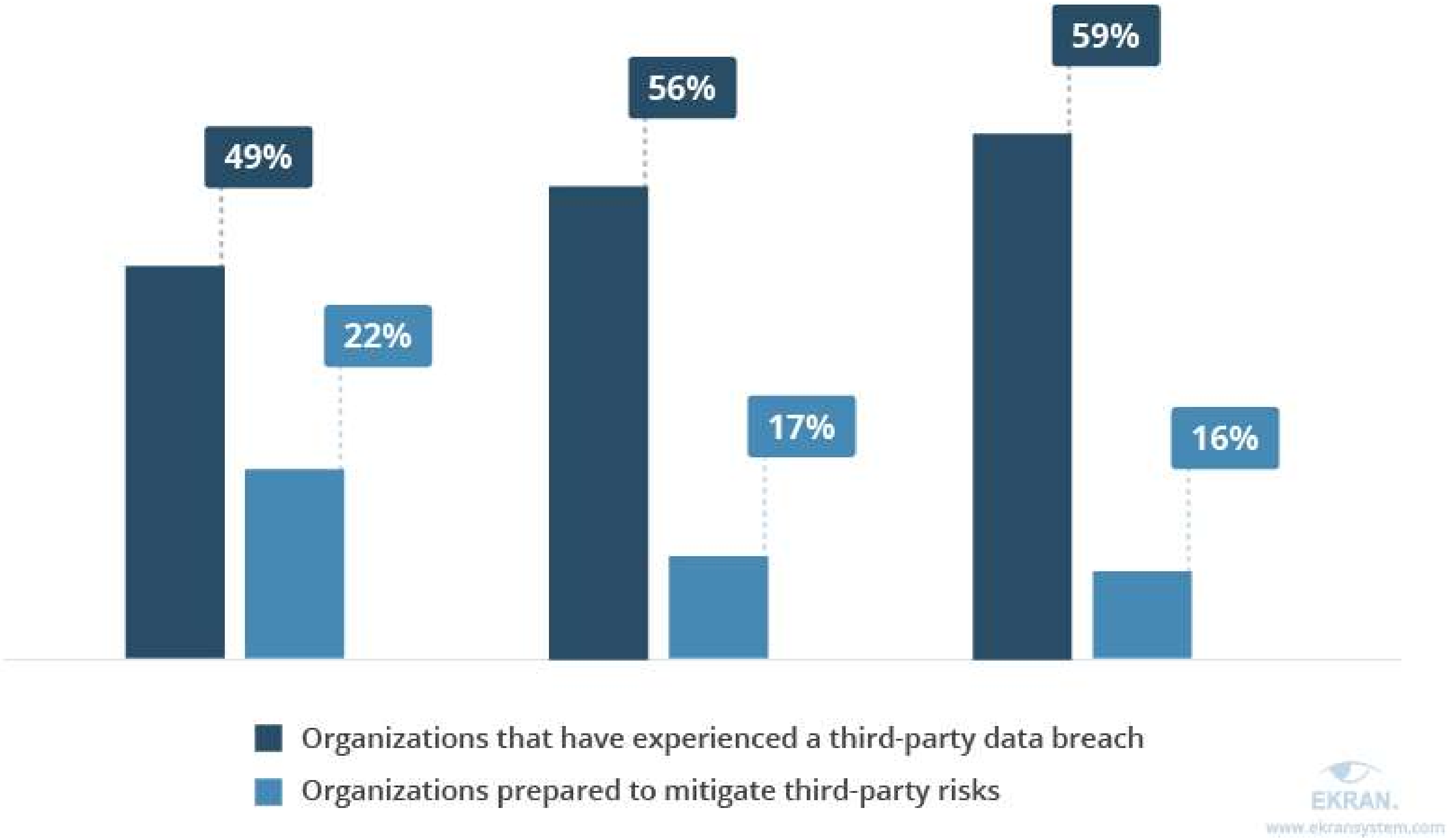
Risks that would affect your compliance with cybersecurity laws.

3. Operational

Risks that would affect your ability to do business.

State of third-party data risk management

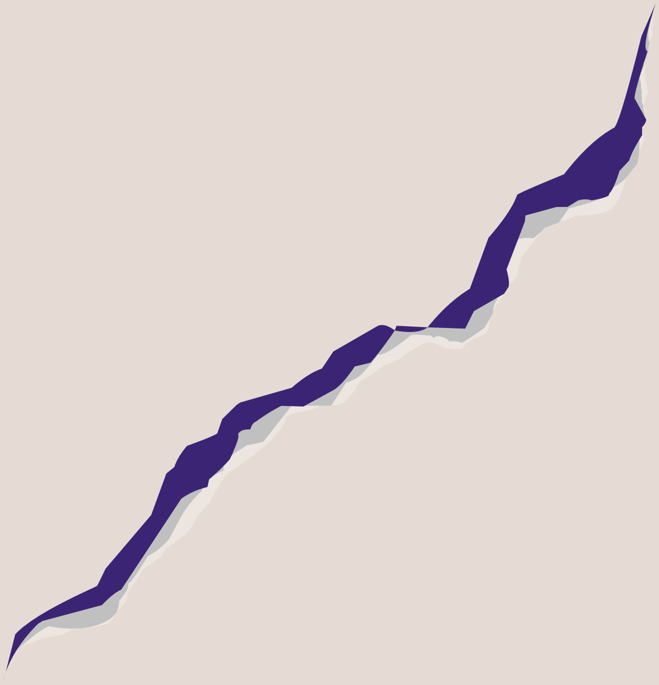
According to the Data Risk in the Third-Party Ecosystem studies in 2016-2018



MANAGING THIRD-PARTY RISKS

Global reliance on software as a service (SaaS) tools only grows with each new technology that we integrate into our lives.

- ✓ **80% of companies share their cloud data** with third parties. That's a whole lot of invisible people with access to your information!
- ✓ Remain aware of who has access to view the data you store on various software. **If you're uncomfortable, make a change!**
- ✓ Pivoting to better-protect your data may involve **internal and external changes** to your security posture as it currently stands.
- ✓ If a hacker steals your data from a third-party, they could ransom the company **or use it to phish you** directly for more information.
- ✓ Making changes to manage third-party risks may stymie productivity, but that's a minor obstacle compared to **long-term data security.**
- ✓ **Use the insights you gather** to make better decisions about the future of your data's privacy.
- ✓ Develop strategies to **identify, assess, monitor and mitigate risk** most effectively,



"The most common system or platform to get hacked is the system you didn't even know you had."

- Bengt Berg

Head of Compliance Management Services at Cybercom

PROTECT PERSONALLY IDENTIFIABLE INFORMATION

In 2021, the FTC reported 1.4M cases of identity theft.
In 2022, they received 603,591 complaints **in just the first six months.**

How are you keeping your name off that list this year?

CRASH COURSE IN PII

Personally Identifiable Information

PII encompasses data that can be tied back to who you are, like your name, home address, phone number and Social Security number. All PII, regardless of how easy it is to tie back to you, must be protected.

PII is the most commonly compromised data

PII theft encompasses 44% of cyber-attacks, likely because it is the most expensive data that they could steal. It can be sold, sell it, used to break into and buy goods off of your accounts, and leveraged to extort the victim directly.

In 2021, the cost of compromised credentials totaled over $4M

Criminals can sell your private information for hundreds of dollars on the Dark Web, where it goes for an average of about $200 per record. That's what makes it such a lucrative and attractive target, and why it's the most common kind of data taken.

Hackers make their fortune by learning to breeze past bare-minimum security measures and get into the accounts that really matter. Equip all of your Internet-connected devices with auto-scanners and firewalls that detect unusual network activity, so you can take immediate action against the intruder.

Two-factor authentication requires you to verify your identity through some unconnected means, so even a hacker with your password wouldn't be able to seize your accounts. Instead, you'll get an alert about an attempted breach and can take action immediately.

CASE STUDY

inside the recent breach on T-Mobile

Recently, T-Mobile customers learned that their personally identifiable information (PII) may have been exposed in a data breach on the company. The telecom provider noticed the suspicious activity on January 5th, but its origins stretch back to last November 25th.

Upon discovering the breach, T-Mobile immediately launched an investigation into the attack which they have allegedly since contained.

37M users had their data stolen, information which included their names, addresses, email addresses, phone numbers, birthdays and even T-mobile account information. This is more than enough to mount significant social engineering attacks and attempts at brute-force break-ins.

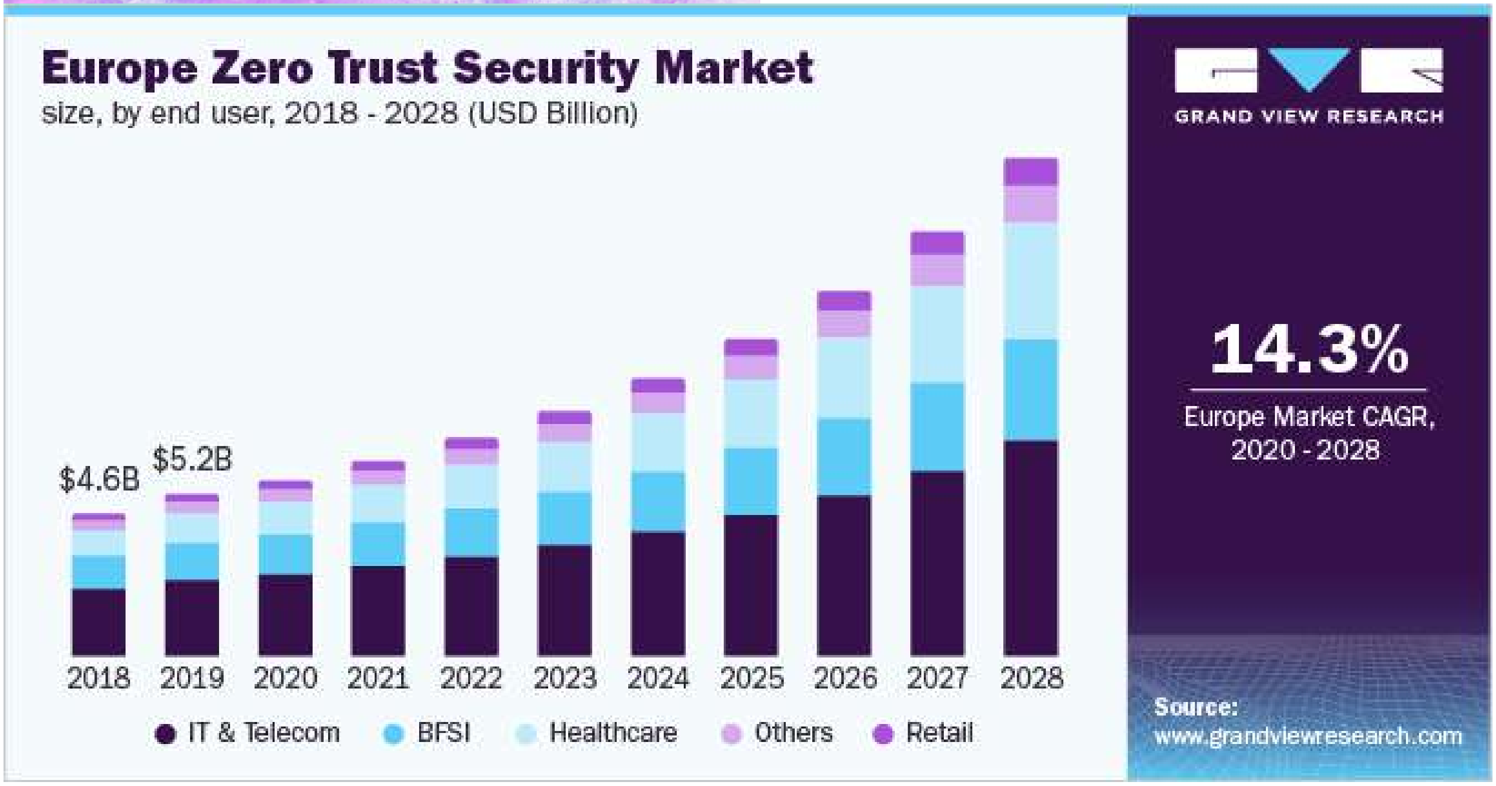
PII theft is a major security concern for individuals and businesses alike. Its devastating consequences for those who are affected include financial loss, identity theft and other forms of fraud. It is important to be aware of the risks associated with PII theft and take steps to protect yourself against becoming a victim.

If you were one of the 37M affected, take action immediately!

Change your T-mobile privacy settings to include new, strong passwords and two-factor authentication. Monitor bank accounts for suspicious activity in the coming months; and avoid clicking on links in emails or text messages from unknown sources. Keep your personal information secure and remain aware of the latest security threats to keep yourself safe from further damage as a result of this data breach!

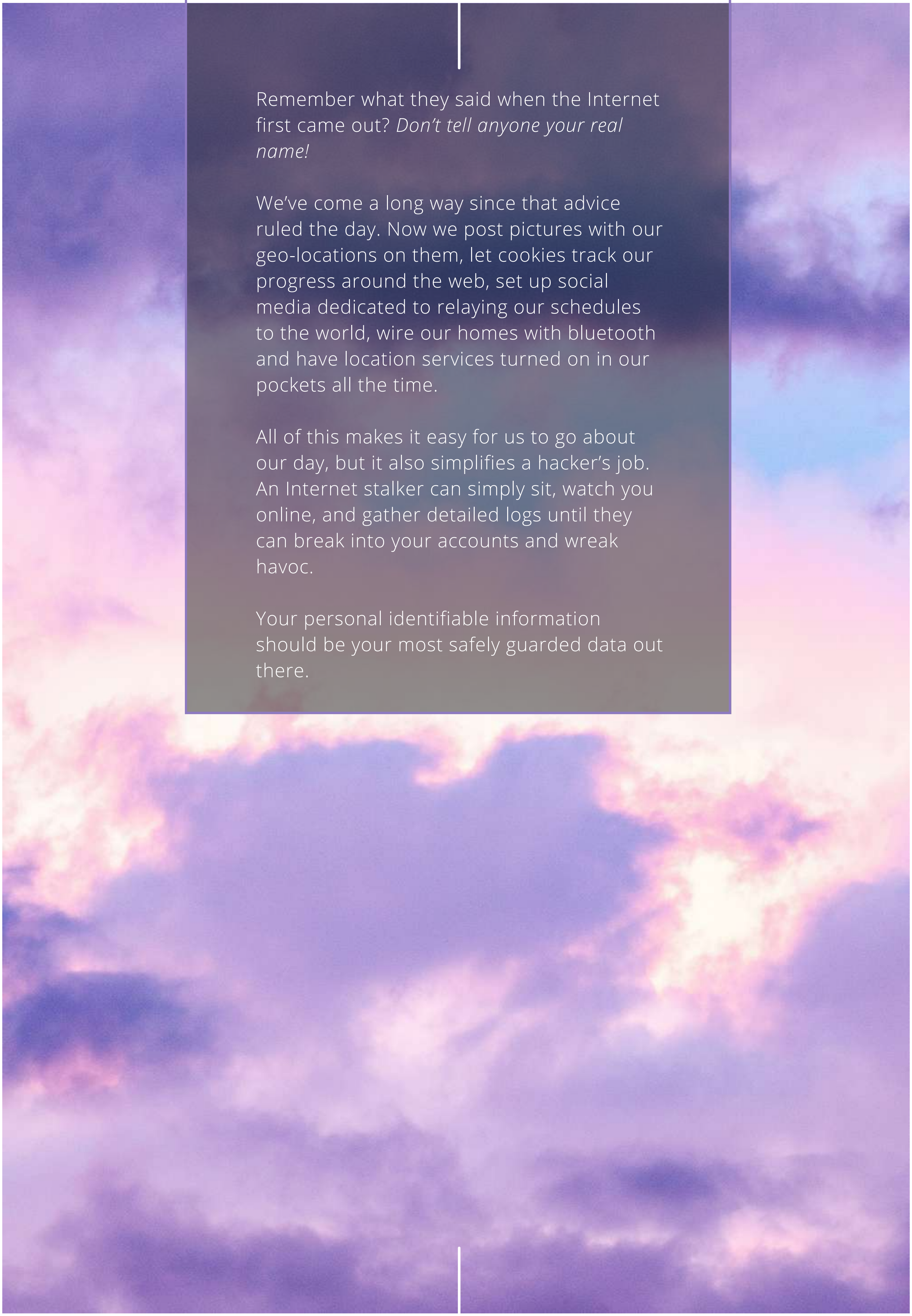
ZERO TRUST

Zero-trust frameworks assume no user, device or service is trustworthy until they've been verified



With the Zero-Trust framework, organizations can protect their data by using multiple layers of security controls and continuous monitoring services on their networks. This approach helps reduce the risk of unauthorized access and data breaches.

The Zero-Trust framework also provides more granular control over user access, allowing you to limit access based on user roles and permissions. Zero-Trust ensures only authorized users can get to sensitive data, while protecting against malicious actors who may try to gain unauthorized access.



Remember what they said when the Internet first came out? *Don't tell anyone your real name!*

We've come a long way since that advice ruled the day. Now we post pictures with our geo-locations on them, let cookies track our progress around the web, set up social media dedicated to relaying our schedules to the world, wire our homes with bluetooth and have location services turned on in our pockets all the time.

All of this makes it easy for us to go about our day, but it also simplifies a hacker's job. An Internet stalker can simply sit, watch you online, and gather detailed logs until they can break into your accounts and wreak havoc.

Your personal identifiable information should be your most safely guarded data out there.

"Amateurs hack systems. Professionals hack people."

- Bruce Schneier,

WHAT YOU NEED TO KNOW

ABOUT PHYSICAL DEVICE SECURITY

CASE STUDY : WHEN CYBER-CRIME MEETS THE REAL WORLD

Has there been a crazy rise in stolen phones in your area the past couple of years?

It seems like phone theft is more popular than ever, even in places where you wouldn't have been in danger of it before.

The Federal Communication Commission released an official statement, calling it an "epidemic."

PHONE ROBBERY COULD RESULT IN LOST PRODUCTIVITY, LOST DATA, STOLEN IDENTITIES AND FRAUDULENT BANK CHARGES.

Recuperating from the damage costs half of victims approximately $500 to get back all their lost data, and **1 in 3 victims would pay one thousand dollars to get their data back.**

Nearly 70% of people would risk their physical safety to get their property back, too!

Take the proper steps to prevent theft! Keep your devices securely on your person, or better yet, leave it at home.

If something bad *does* happen, report it to the authorities and your IT service providers ASAP. Then remotely lock and wipe your device on a computer.

5 TIPS FOR BETTER PHYSICAL SECURITY

***30M people have their phones stolen** every year in the United States.*

*2M laptops are stolen annually and **only 2% are ever found.***

A lot of cybersecurity awareness revolves around the digital security of all your devices...but how well do you take care of their physical security?

Data breaches don't just happen when your computer gets infected with malware or you fall for a phishing scam. How often have you done the "phone, keys, wallet" check before you leave a venue? Thieves can steal your laptop out of your bag or your phone from your pocket. Then, they can crack your password and steal all your data directly!

#1 **Lock up important devices when you're not using them**, whether that's leaving your cubicle to use the bathroom for a few minutes or keeping your home office locked when you throw a party. **Insider threats are responsible for 60% of data breaches.** Coworkers, business partners, and third-party vendors frequently pass your workstation and could look at files if they're not stored in a locked drawer or secured in some other way.

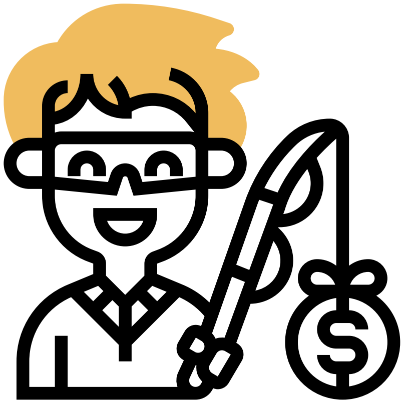
#2 Just as you wouldn't splay somebody else's contracts on the desk during a meeting, you should **clear your immediate area of confidential files before joining virtual meetings**. Workplaces have a ton of meetings online nowadays, and it's easy to overlook this simple step when you're busy.

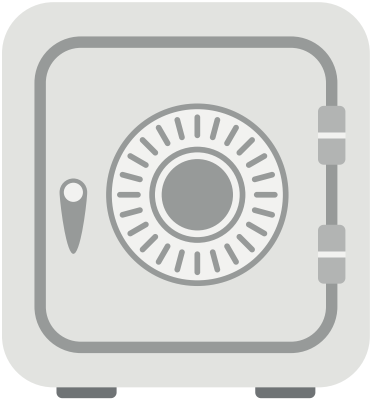
#3 **Leave it home if you're not going to use it.** Although we can't all stand to have our cell phones away from our person for that long, maybe you can re-think bringing your laptop on vacation or leaving the backpack with your tablet in it hanging on the coffee shop chair while you order. Thieves can steal your device, and then take out your hard drive to read on a different machine, without having to guess your log-in!

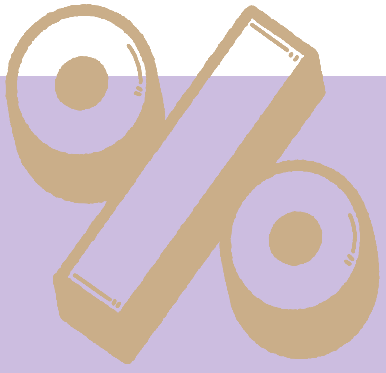
#4 Keep your eyes on ONLY the files you're supposed to have access to. **You are responsible for abiding your clearance level.** You are just as capable of committing insider threats as anyone else in the organization — even just by accident!

The physical security of your devices is just as important as their cybersecurity. Understanding some of the ways that threat actors compromise devices by direct hand, helps you see simple ways to protect your tech on a daily basis.

Human error is responsible for 95% of data breaches. You can bring that number down by taking little steps to preserve your devices' and data's security every single day.







10% of data breaches begin a physical compromise, rather than originating online.

Protecting our networks is a TEAM EFFORT!

65% of employees admit to taking risks with physical security.

Source: ENISA Threat Landscape 2020

"Even at home with well-intended, loving individuals, it's important to practice cyber hygiene."

- Rex Tolman, VP of Enterprise Security

WHY TAKE CYBER HYGIENE SERIOUSLY?

Verizon:

Ransomware attacks have grown more popular this year than it has in the last five years combined.

ISACA:

Most organizations have noticed more cyber attacks lately and are particularly worried about social engineering.

Cofense:

Phishing messages sit for up to an hour in 82% of employee email inboxes.

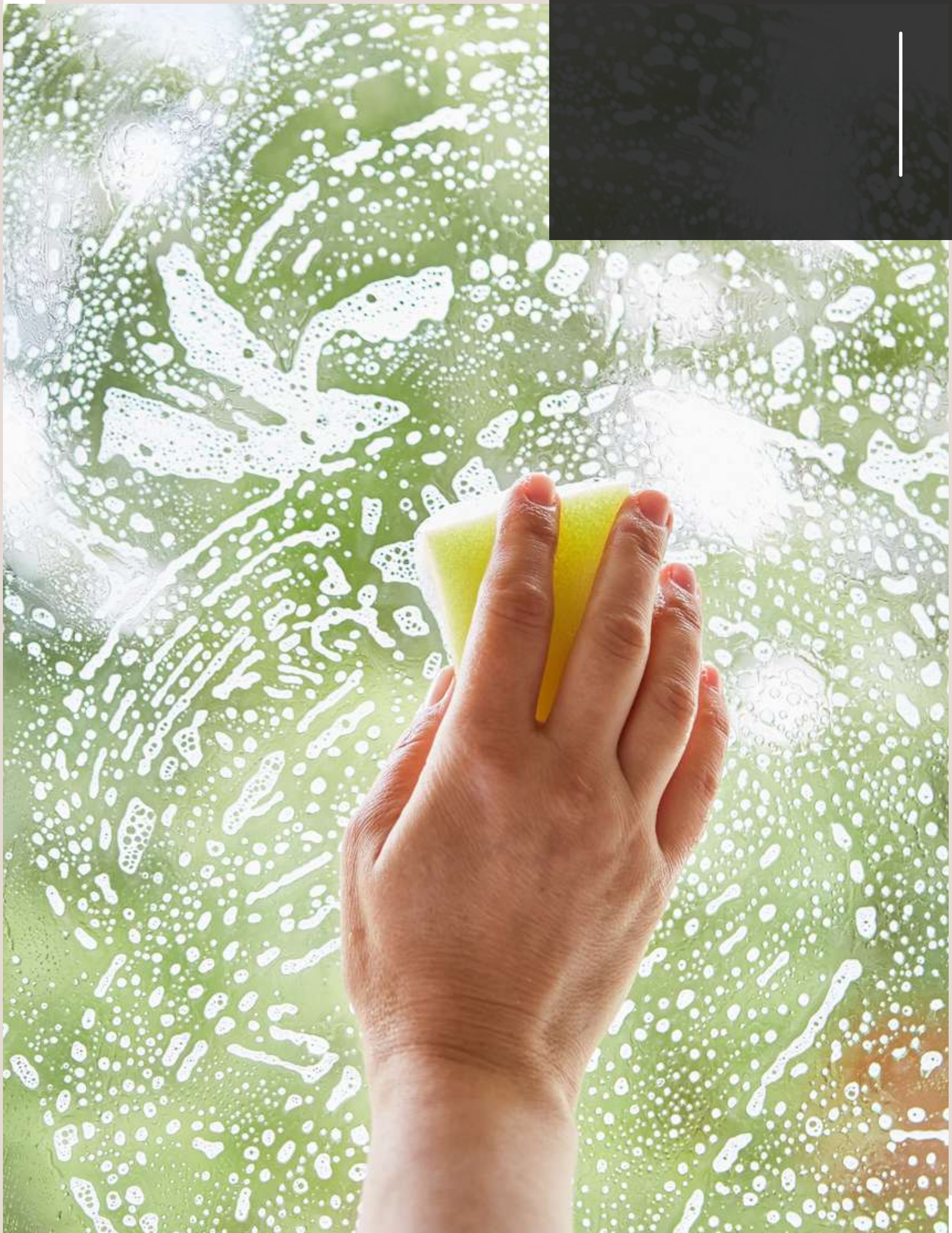
Ernst & Young:

Telecommunications has been a huge target for hackers, increasing 75% in 2021.

Gartner, Inc.:

By 2025, half of all businesses will face software supply chain attacks — a sign this danger isn't going away soon.

SPRING CLEANING CHECK-LIST



To help you spring clean your technology and cyber footprint, we have developed a checklist to help you through the process. Just like spring cleaning your house, you can assignsome of these tasks to your family!

- □ Review your passwords, updating them as needed, and ensuring they are strong
- □ Shred old and unnecessary paperwork
- □ Review your social medias' privacy settings
- □ Organize folders of files that you want to keep or delete
- □ Review and update spam filters
- □ Review your contact list for people to update or delete
- □ Remove apps or programs that you don't use anymore
- □ Remember to use MFA whenever it is available!

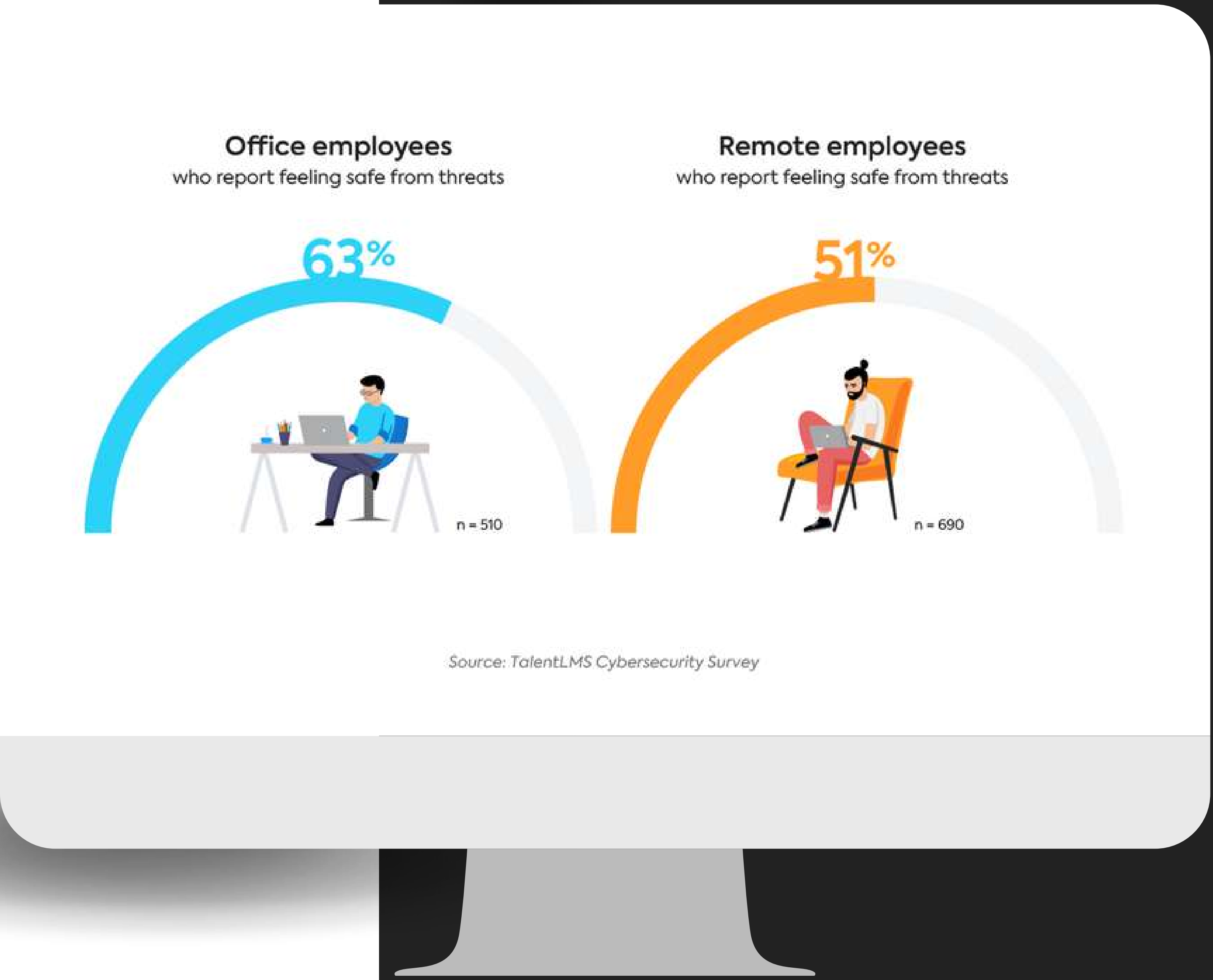
- Search yourself online to see what comes up □
- Don't just delete apps; delete your profiles too □
- Review photos or videos and delete ones that you don't want viewable □
- Set your devices and software to update on a regular basis □
- Properly store and lock up sensitive paperwork □
- Dispose of old electronic equipment □
- Test and validate your backup routines □
- Use a password manager if you haven’t in the past □

. If cleaning is not normally your idea of a good time, we hope that you’ll find this technology and cyber spring-cleaning checklist a way to speed up the process.

Have fun getting rid of some clutter!

CYBER-HYGIENE MATTERS

Cyber-hygiene refers to all of the security defenses and personal action plans that you incorporate to protect the health of your systems and devices.



Source: TalentLMS Cybersecurity Survey

Making cyber-hygiene a daily routine can help assuage your worries about threat actors AND improve the long-term security of your networks and devices.

HOW TO COMPLETELY WIPE YOUR PHONE CLEAN

Do you plan to give away or sell your phone? Make sure it's clean first!

If you're one of those people who jump on the latest and flashiest phone as soon as it comes out, then you need to be VERY careful what you do with your old devices.

Or maybe your family or friends hand down phones when someone else's gets lost or broken, or your win new a smart device at some raffle event, or you just want to upgrade to better processors and higher speeds...

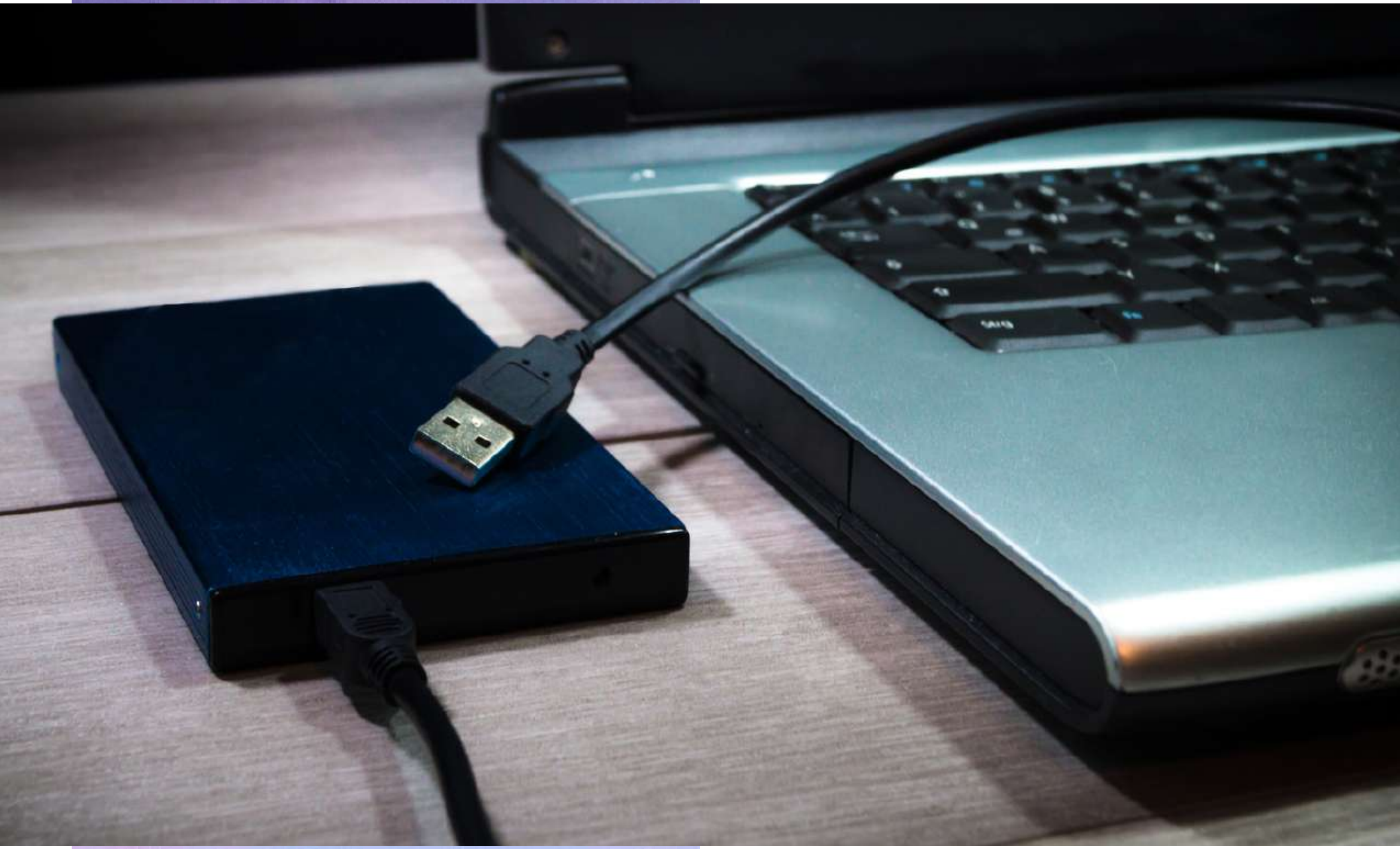
These are just a few of the MANY reasons that we get rid of our old phones, tablets and laptops.

Whether you're giving your old devices away or selling them to a stranger, be VERY careful that it's COMPLETELY clean of your data.

Just deleting files won't cut it - these are all recoverable if someone knows what to do!

Instead, **restore devices to factory settings before selling or giving them away.**

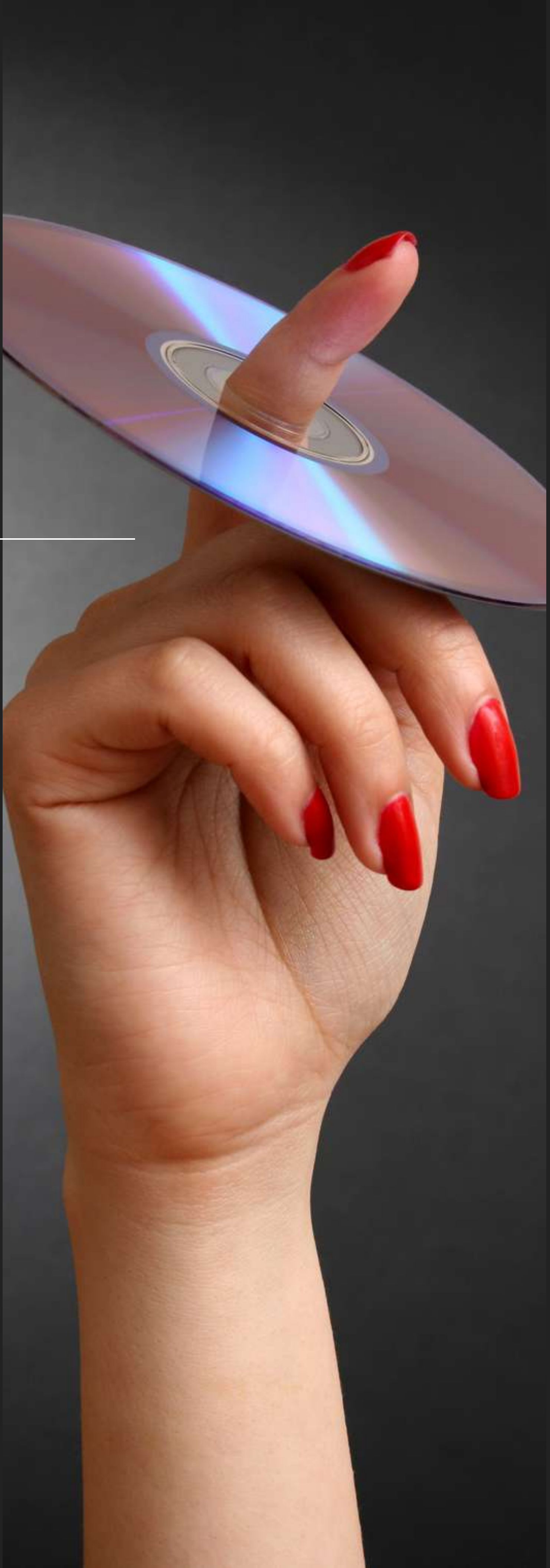
This will make it as though the device has never been used. Even if they go snooping, the new owner won't be able to find any of your history or info on it.



"It wasn't raining when Noah built the ark."

- Howard Ruff

SAFE BACKUP AND RECOVERY



CRASH COURSE IN THE CLOUD

People talk a lot about "saving to the Cloud," but what does it actually mean? Where does all that data go?

The cloud is a collection of many people's information, all amassed and stored on remote servers somewhere in the hub of your chosen provider.

These servers are encrypted and safeguarded with more powerful defense mechanisms than most people can manage on their own. They store all of this data in a massive library that knows just where to pull your files when you need them.

You can access your information from many different devices, and you don't have to be connected to your home network to do it.

If you want to collaborate on Google Docs with a colleague, you can both log in and make edits at the same time. Even if you made that JPG at three in the afternoon from your home office, you can access it from the other side of the planet on your smart phone. This has obvious benefits in today's modern world!

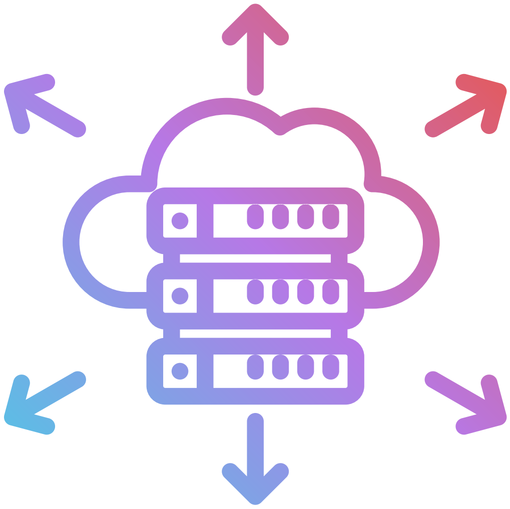
So why do some people stay with legacy systems?

- Reliance on the Internet means a slowdown in your day if the power goes out
- It can be difficult to trace who has your data and where else it may be being sold or accessed
- Conversion can be difficult,; whether you're switching Cloud providers or simply trying to open a file in an unsupported format
- Workarounds are time-consuming and hard to find
- You must rely on someone else to prevent hiccups and combat breaches
- Contracts can be difficult to understand and get out of

More and more people are relying on remote storage spaces, like the cloud, because physical storage is often incompatible with the modern business owner’s needs, such as managing huge swaths of data from any location.

Cloud computing can also save your business on ***30 - 40% of their IT costs!***

Despite this, the cloud is not infallible. The server on which you choose to store your data can be compromised too, which would put all of your data at risk.



If your cloud gets hacked, then the threat actors will have access to the same landing login pages as you do...if you can log in from anywhere, so can they!

.

For this reason, you need to *back up your back ups.*

That's right. Save your backup files to a second source so that you won't be cut off from your files if your first cloud gets breached or corrupted.

Set up monitoring that alerts you to suspicious activity or unauthorized account access, so that it rings like a store alarm if someone breaks in.

Then, at least once a month, test that your cloud storage has the latest and most up to date files. Then try and retrieve files from the backup; if they’re unreadable or corrupted in some way, then you have time to correct the mishap before you really need them!

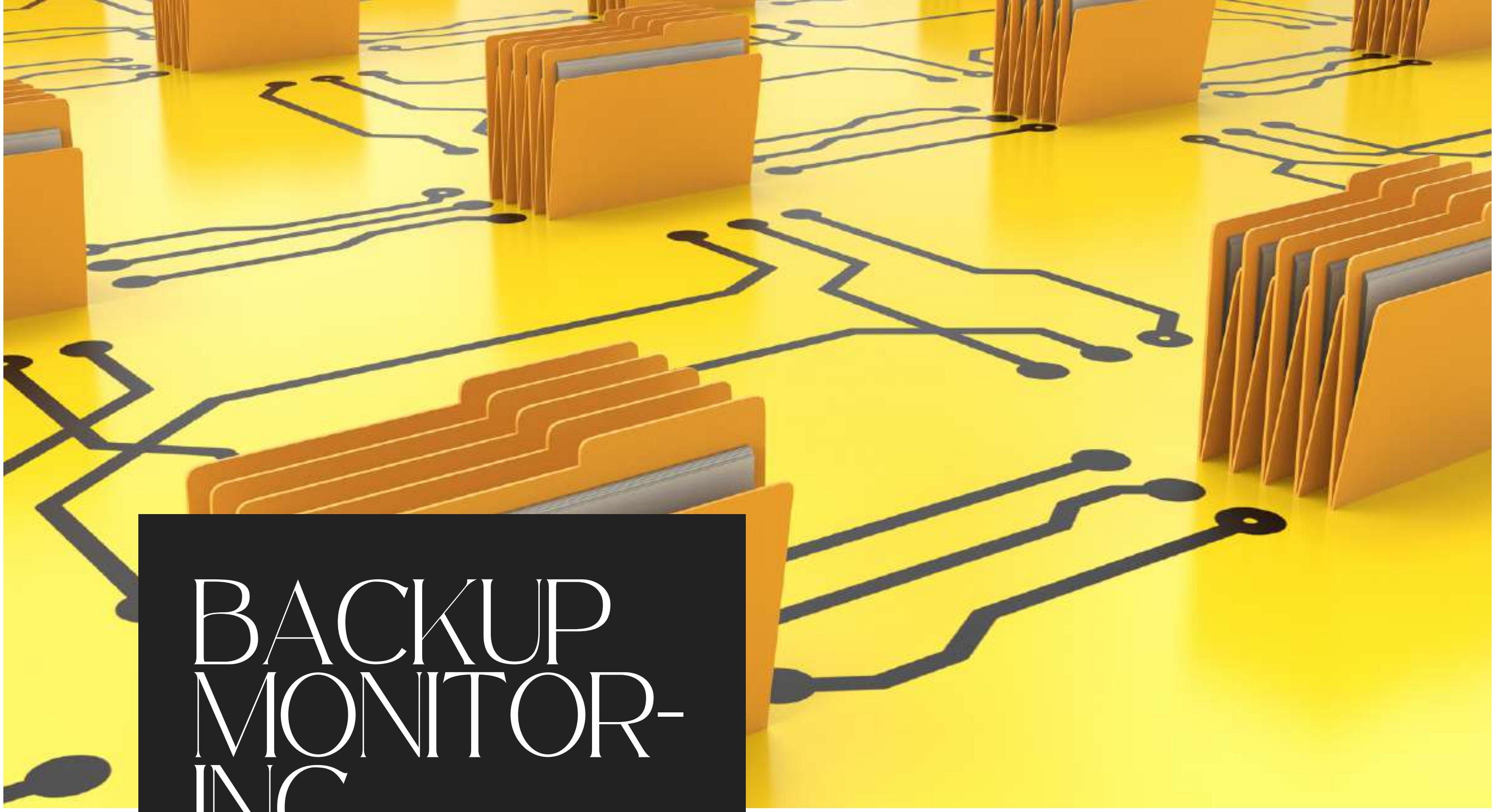
REAL FACTS ABOUT THE CLOUD:

01 The cloud stores 60% of international professional data.

02 The global public cloud market is worth tens of billions of dollars.

03 80% of modern companies use multi-cloud storage systems.

04 There are 3.6B cloud users around the world.



BACKUP MONITORING

2.5	*quintillion bytes of data are created daily*
10%	*of users back up their data every day*
20%	*of users could lose all their data in a crash*

HOW TO PROTECT YOUR STORAGE SYSTEMS

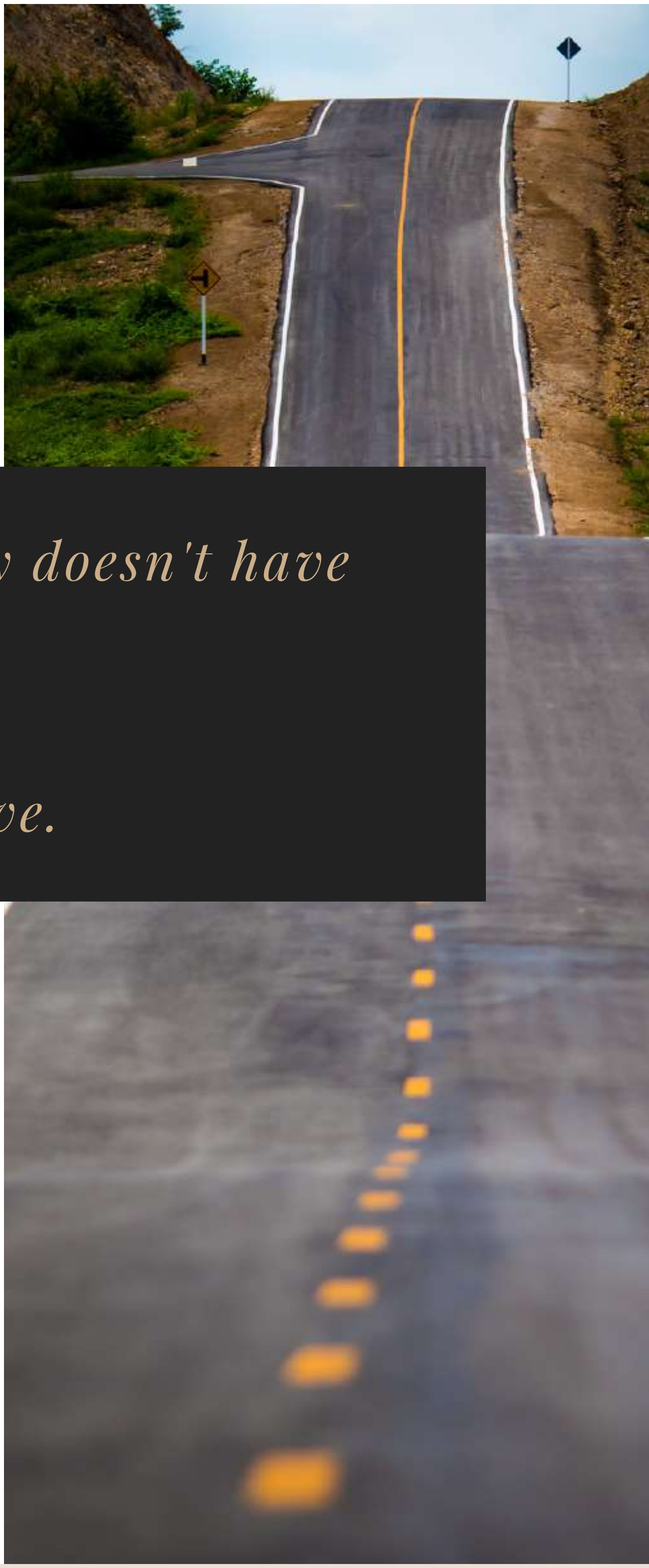
If you've ever had an application crash, untimely power outage, or file theft as a result of a data breach, then you've already learned the hard way how important it is to back up your files on a routine basis.

Save your work regularly, or better yet, use applications that automatically save to your preferred storage system, like the Cloud, to guarantee you're always working with the latest version.

Then, monitor these backup systems to make sure they can open readable, uncorrupted files. This will give you time to fix it before an actual emergency happens!

Use continuous monitoring to alert you to suspicious activity on your backup systems too.

AUTHENTICATION RECOVERY



What do you do if you can't remember or access your MFA?

Multi-factor authentication makes you prove your identity in addition to using a strong password.

What happens if you don't remember, or can no longer access, your MFA?

> *The road to account recovery doesn't have to be an odyssey.*
>
> *Make it a breezy Sunday drive.*

Many websites will give you a list of short "recovery codes" that you can use to get into your account if you forget or can't access your log-in for some reason (e.g., if you were getting SMS messages but have since changed your number).

Sometimes called "backup codes," these make it more difficult for hackers to pretend they "forgot" the password and lock you out.

Authentication recovery keeps your accounts safer!

"If you spend more on coffee than on IT security, you will be hacked."

- *Richard Clarke*

PRODUCTIVITY GUIDE

step 1

Begin your day by creating a digital to-do list using tools like Todoist, Microsoft To Do, or Google Keep. Prioritize tasks based on urgency and importance. Regularly review and adjust the list as tasks evolve.

step 2

Use automation tools like Zapier or IFTTT to connect and automate repetitive tasks between your apps. For example, automatically save email attachments to a cloud storage folder.

step 3

Opt for unified communication platforms like Slack or Microsoft Teams. These tools integrate chat, video calls, and file sharing, reducing the need to switch between apps. Set specific times to check messages to avoid constant interruptions.

step 4

Familiarize yourself with keyboard shortcuts for your most-used software. This minimizes mouse movements, speeding up routine actions. A tool like KeyRocket can suggest shortcuts as you work.

step 5

Schedule tasks, meetings, and breaks on a digital calendar like Google Calendar or Outlook. Set reminders to keep you on track. A well-maintained calendar helps visualize time allocation and reduces overcommitting.

step 6

Utilize apps like RescueTime, or Forest to monitor and limit distractions. Set specific intervals for deep work and short breaks, following techniques like the Pomodoro Technique. This ensures regular focused work periods.

step 7

Use cloud storage solutions like Dropbox, Google Drive, or OneDrive to automatically backup and sync your files. This ensures data security and accessibility from any device. Regular backups prevent data loss and save time in emergencies.

HOW TO KEEP YOUR BUSINESS CYBER SECURE

short and sweet

STEP BY STEP

01

Implement Multi-factor Authentication (MFA)

Always use MFA for accessing sensitive business accounts. It adds an extra layer of security by requiring multiple forms of verification.

02

Regularly Update & Patch Systems

Ensure all software, including operating systems and third-party applications, are up-to-date. Apply security patches promptly to close vulnerabilities.

03

Educate Employees on Security Protocols

Offer cybersecurity training for employees to recognize threats like phishing. Encourage them to report suspicious activities immediately.

04

Backup Data Regularly

Schedule automatic backups for essential business data. Store backups both onsite and offsite, ensuring they're encrypted and protected.

05

Implement a Firewall and Anti-malware Solutions

Use a robust firewall to block malicious traffic. Install and update anti-malware software to detect and remove threats.

IN AN EVER-CHANGING
THREAT LANDSCAPE,
YOU NEED UP-TO-DATE
SECURITY AWARENESS!

LET'S CYBERSECURE
OUR FUTURE,
TOGETHER.

CYBERSECURITY YOU CAN TRUST!

We believe in providing YOU the best-in-class security suite to keep you cyber-secure in the face of an ever-changing threat landscape.

Call us today at **240-442-2960** and let us help you wrap a security blanket around your business.

Critical IT Solutions, LLC
12305 Cypress Spring Road
Clarksburg, MD 20871