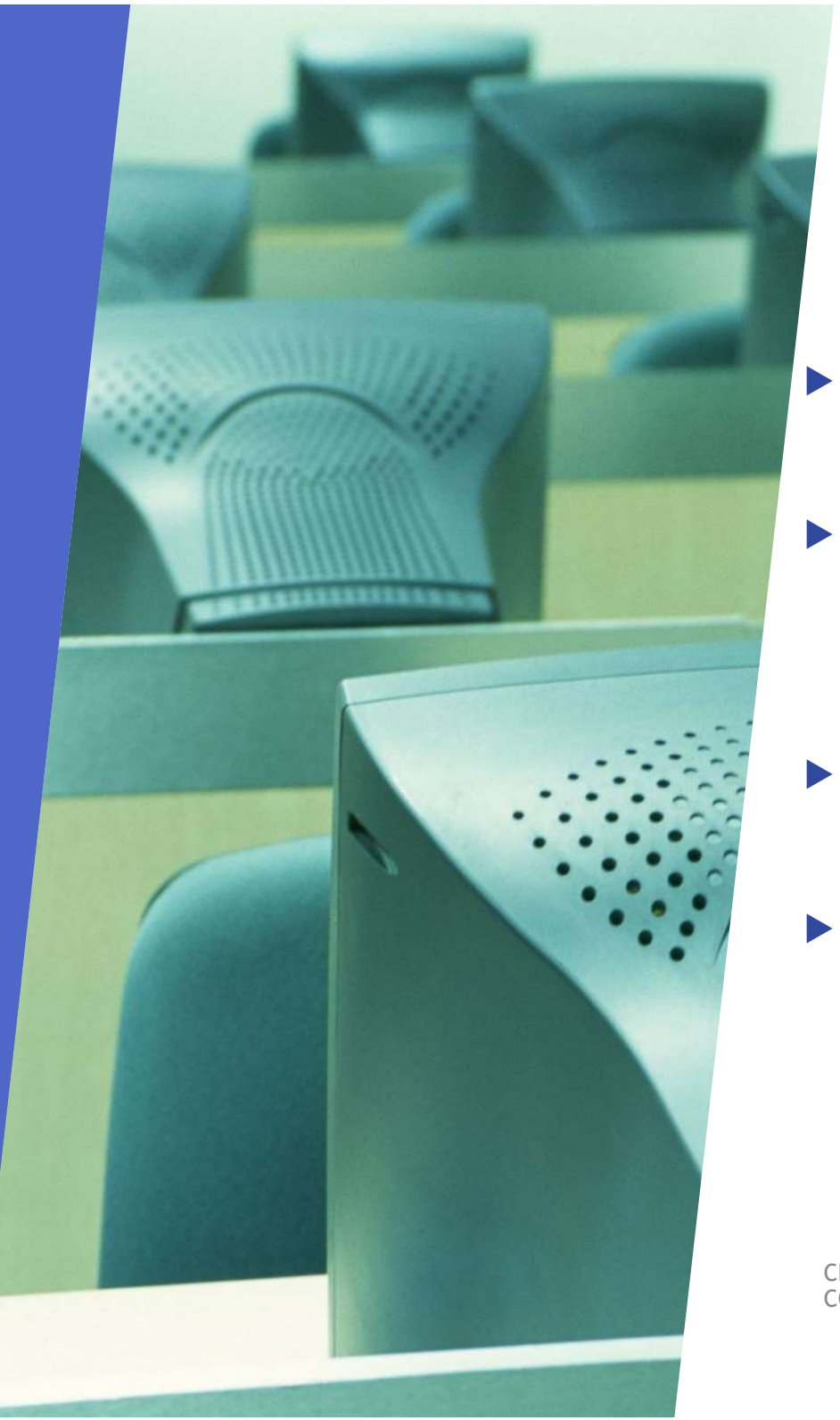
CYBERSECURITY, PRIVACY AND DATA PROTECTION

NOVEMBER 9, 2023

Presented by:
WANDA BORGES, ESQ.
BORGES & ASSOCIATES, LLC
wborges@borgeslawllc.com

JOSEPH MOLINARO, ESQ.
LAW OFFICES OF JOSEPH MOLINARO, LLC
jam@molinarolaw.com



FEDERAL REGULATIONS

- Computer Fraud and Abuse Act [18 U.S.C. 1030] (1986)
- Cybersecurity Information Sharing Act [part of PL114-113 "Consolidated Appropriations Act, 2016)
- Federal Trade Commission Act [15 U.S.C. 45] (1914)
- Identity Theft and Assumption Deterrence Act [18 U.S.C.1028(a)(7)] (1998)

NEW YORK STATE REGULATIONS

- **NYDFS Cybersecurity Regulations [23 NYCRR Part 500] ("NY Cyber Regs")**
- **NY "SHIELD" Act [New York Stop Hacks and Improve Electronic Data Security)**

Other State Data Privacy Regulations

- California
- Colorado
- Connecticut
- Indiana
- Iowa
- Montana
- Tennessee
- Texas
- Utah
- Virginia

- 11 other states with active bills

ABA MODEL RULES OF PROFESSIONAL CONDUCT

- **Model Rule 1.1**
  - **COMMENT 8 "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject"**

CASELAW

- Earlier cases – United States v. Morris (1991) [released one of the first internet worms], United States v. Swartz (2011) [theft of millions of academic articles], Nosal [ex-employee](2012) – government's finding "Hackers" be criminally liable under the CFAA
- Van Buren decision [593 U.S. ----141 S.Ct. 1648 (2021) – clarified the limit to finding culpability under the CFAA
  - Discussed "exceeding authorized access" in contrast with "without authorization"
  - Distinguished by several cases
- ZAP Cellular Inc. v. Weintraub [2022 WL 4325746](EDNY Sept. 2022) – unlike Van Buren where a police officer had authorization but exceeded that authorization, in ZAP, Defendant Weintraub qualified as an "outside hacker…without any permission at all…"

RECENT CASE

- March, 2023
- NYS Attorney General settled with the law firm of Heidell, Pittoni, Murphy & Bach, LLP
  - $200,000 fine for breach of personal and healthcare data
  - Violated state laws and HIPAA
  - Failed to protect consumers' personal and private health information

CORE CONCEPTS

- **Fundamental Issues of securely sending, receiving and storing client and law office data and communication**
- **Cybersecurity Features of various technologies to protect client and law office electronic data and communication**
- **Threats of cyberattacks and steps to take to prevent those attacks resulting in inadvertent disclosure of confidential client and law office information**
- **Security measures to protect client and law office electronic data and communication when working remotely or when using personal or business mobile devices**

ETHICAL RESPONSIBILITY TO PROTECT THE CLIENT

- Confidentiality obligations and how they apply to securing, protecting and maintaining clients' confidential, privileged and proprietary electronic data and communication
- Obligation to secure and protect escrow funds from cyber threats, cyber attacks and data breaches
- Professional responsibility to safeguard and secure clients' electronic data and communication

ETHICAL RESPONSIBILITY TO PROTECT THE LAW OFFICE

- Confidentiality obligations and how they apply to securing, protecting and maintaining law office's confidential, privileged and proprietary electronic data and communication (including remote work)
- Obligation to secure and protect escrow funds from cyber threats
- Professional responsibility to safeguard and secure law office's electronic data and communication

ETHICAL RESPONSIBILITY TO SUPERVISE

- Relating to Electronic data and communication, attorneys have an ethical obligation and professional responsibility to supervise
  - Employees
  - Vendors
  - Third parties
- Attorneys have an ethical obligation and professional responsibility to supervise law office staff in securing, maintaining and destroying confidential, privileged and proprietary client and law office electronic data and communication

ADDITIONAL DUTIES

- Attorneys have a duty to safeguard against inadvertent disclosure of confidential data and communication by electronic means.
- Duty extends to
  - Client
  - Court
  - Opposing counsel
  - Third Parties
- Attorneys have a duty to refrain from revealing confidential information by electronic means
  - E.g. – Social Media

UNDERSTANDING TECHNOLOGY

SECURITY MEASURES

- Secure Internet Access
- Encryption of Files
- Address cyber security risks
- Understand and use security measures

CYBER SECURITY FEATURES

- Encryption
- Authentication/ Multi-Factor Authentication
- Passwords
- Virtual Private Networks
- Firewalls

REDUCING THE POSSIBILITY OF CYBER ATTACKS

- Hardware issues:
  - Computer "hygiene"
  - Mobile devices
- Software issues:
  - Platforms
  - Networks
  - Remote connections

QUESTION EVERYTHING

- When choosing Vendors, Third Parties and Technology Staff, ask appropriate questions about
  - Remote security management
  - Virtual private networks
  - Firewall settings
  - Mobile device security
  - "dark web" monitoring
  - Backup systems

UNDERSTANDING THE MAJOR CYBERSECURITY THREATS

FIVE MOST COMMON CYBERSECURITY THREATS

- Malware (includes Phishing, Ransomware, Trojan horses, crypto mining) – generically - Hacking
- Debit, Credit Card or Wire Transfer Fraud
- Data Breaches
- Compromised Passwords
- Business Email Compromise
  - Unauthorized Email and Social Media Access

PREDOMINANT CYBER THREATS

- **RANSOMWARE – a type of malicious software, or malware, designed to block access to a computer syste until a ransom is paid. Ransomware is typically spread through phishing emails or by unknowingly visiting an infected website.**

- **TROJAN -A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.**

PREDOMINANT CYBER THREATS

- **CRYPTOMINING –enables the third party to open a gateway into your system permitting malicious third parties to access – most often targeting financial information – In 2021 generated the most internet traffic out of any individual category.**

- **PHISHING/BUSINESS EMAIL COMPROMISE – seemingly legitimate emails from colleagues, coworkers or customers. Once opened, enables the third party to access your entire system (contacts, passwords, etc.)**

RANSOMWARE

- Ransomware is a type of malicious software, or malware, designed to block access to a computer system until a ransom is paid
- Ransomware is generally downloaded inadvertently
  - Visiting a website you may see a message that says
    - "Your computer is infected with a virus. Click here to resolve the issue"
    - "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine"
    - "All files on your computer have been encrypted., You must pay $500 within 72 hours to regain access to your data"
    - Taken from U.S. Dept. of Homeland Security
- Ransomware may be hidden in a link from a company or person that you know
  - Clicking on the link will immediately infect your computer
- NEVER PAY THE RANSOM!!!!!!!
  - Paying the ransom doesn't work and will likely cause more damage

CISA Ransomware Prevention Best Practices

- **CISA [Cybersecurity and Infrastructure Security Agency] is a standalone United States federal agency, an operational component under Department of Homeland Security oversight. The following are excerpts from the CISA Ransomware Guide**
- **Maintain offline, encrypted backups of data and regularly test your backups**
- **Create, maintain, and exercise a basic cyber incident response plan and associated communications plan**
- **Conduct regular vulnerability scanning**
- **Regularly patch and update software and OSs to the latest available versions**

CISA Ransomware Prevention Best Practices

- Ensure devices are properly configured and that security features are enabled
- Employ Best Practices for use of RDP and other remote desktop services
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB
- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity
- Implement filters at the email gateway to filter out emails with known malicious indicators and block suspicious Internet Protocol (IP) addresses at the firewall

CISA Ransomware Prevention Best Practices

- Implement Domain-based Message Authentication, Reporting and Comformance (DMARC) policy and verification
- Consider disabling macro scripts for Microsoft Office files transmitted via email
- Ensure antivirus and anti-malware software and signatures are up to date
- Only allow authorized software to run
- Implement an intrusion detection system (IDS)
- Consider the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) with which your organization interacts
  - Adversaries may exploit the relationships you have with your third parties and MSPs

CISA Ransomware Prevention Best Practices

- Ensure your organization has a comprehensive asset management approach
- Restrict usage of PowerShell
- Secure domain controllers (DCs)
- Retain and adequately secure logs from both network devices and local hosts
- Baseline and analyze network activity over a period of months to determine behavioral patterns

FRAUDULENT WIRE TRANSFERS

- **FRAUDULENT WIRE TRANSFERS – often the result of social engineering**
  - **Social Engineering - is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information**
- **Check Twice before Sending Wire or Delivering Goods**
  - **Large quantities of supplies may be ordered from a purportedly known customer to be paid by wire transfer**
  - **A wire transfer is supposedly sent to you. A copy of a bank confirmation of transmission is provided but the money is never received – Goods have been already delivered**
  - **OR**
  - **Your company is given wire instructions (but they are false). Make sure the instructions given to you are not fraudulent or you could send payment to a thief**

LEGITIMATE EMAIL SENT [redacted]

wanda Borges<wborges@borgeslawllc.com>
4/5/2022 5:19 PM

Dear Ed:

Here is the wire transfer information.
[redacted] Bank
[redacted] La Jolla Village Drive, [redacted]
San Diego, CA 92122
Bank ABA #: [redacted]
Account Name: Liquidating Trust
Account Number: [redacted]
Swift Code: [redacted]

FRAUDULENT EMAIL SENT [redacted]

wanda Borges<wborges@borgeslawllc.com>
4/6/2022 3:51 PM

Dear Ed:

The account sent you yesterday was for ACH payment only, i only just received word today, the below is the correct wire info

Please see below requested Wire information:

Bank Name: Chase Bank
5114 BROADWAY OAKLAND CA 94611
Account Name: [redacted] LLP
Account Number: 765787095
Routing number: 322271627
Swift code: CHASEUS33

Please let me know when received. Also, when can we expect payment to be released?

EXAMPLE OF BUSINESS EMAIL COMPROMISE

Click on Release, to free these messages to your inbox and to Verify your Mail Account : Deliver Messages

	Subject:	Subject:	Date:
Release	Re:Enquiry/Consultation	RE: Send PI Asap for payment	10/12/2021 5:19:49 p.m..
Release	Re: Balance Payment	RE: T/T Payment Copy	10/12/2021 5:19:49 p.m..
Release	Re: Account Statement	RE: New Purchase order	10/12/2021 5:19:49 p.m..
			Deliver all messages (3)

RECENT EXAMPLE OF CRYPTOMING

Action required: Online banking system update

If you've already responded, you can ignore this notice.

Dear CUSTOMER:

We are pleased to inform you, of our new planned online banking system. We earnestly ask you, to start the procedure of confirmation of data, to authorize an automatic update of your online banking account, to the latest version released and enjoy all the benefits of the new version.

Kindly Follow Here to get started.

Sincerely,
Bank of America.

Keep your account information up-to-date. In the event of unusual activity, we'll need to know the best way to reach you.

EXAMPLE OF SPEARPHISHING ATTEMPT TO GAIN ACCESS

Actual email text received on 9/16/2021 [lawfirm name has been changed]

FIGMENT, DISNEY & JUSTIN, LTD

You have an encrypted message from Figment, Disney & Justin, LTD.

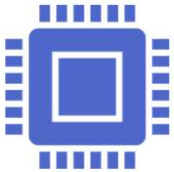
Click here to open your message. After that, open the attachment to decrypt your message and reply to the sender.

This email is confidential and may be privileged. If you are not the intended recipient, please contact the sender immediately.

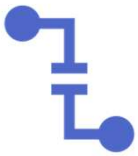
If you require assistance opening this message, please click here to open.

This message was sent using Figment, Disney & Justin Secure Server System, and is subject to terms at: https://fdjlaw.com/disclaimers

THE MIGRATION TO REMOTE WORK



Most firms migrated their workers to remote protocols as the COVID pandemic began to unfold



In the haste to ready servers and data centers, security gaps were left in systems

Proliferation of mobile devices contributed to security oversights

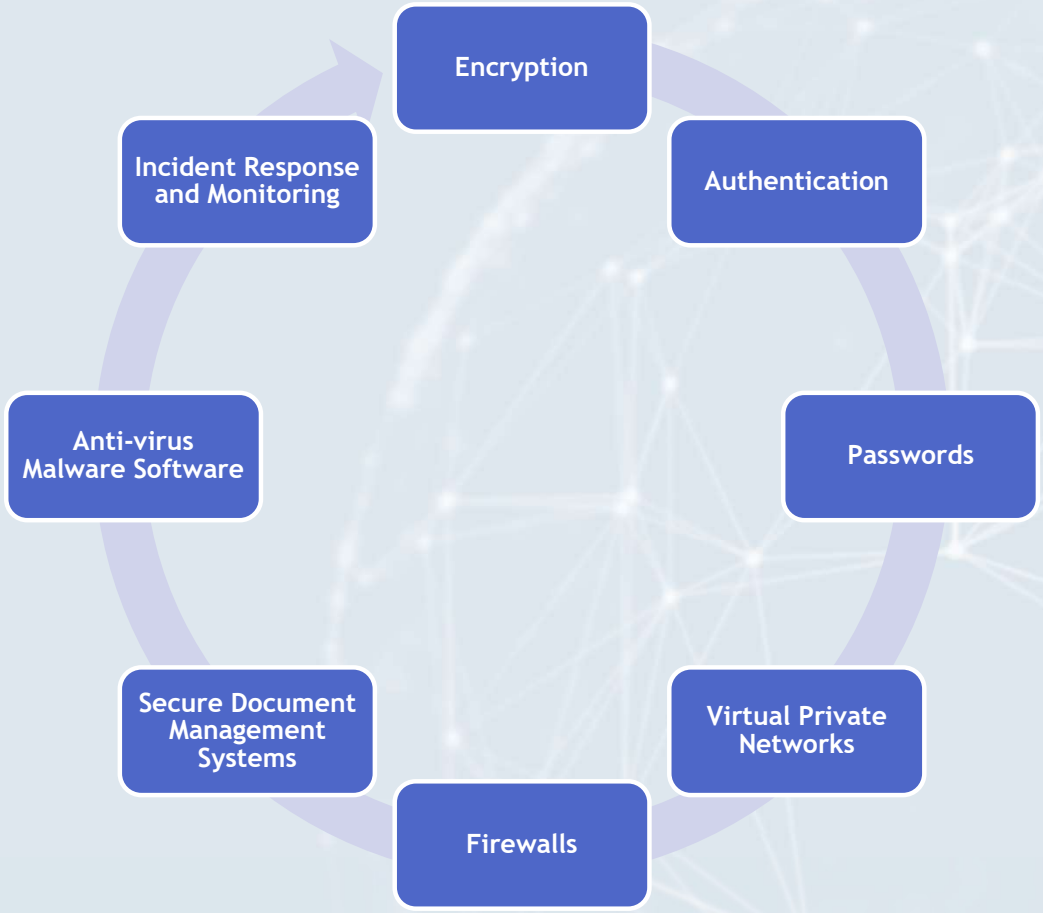
iPads, iPhones, Laptops were overlooked

VULNERABILITY TO CYBERFRAUD WHETHER IN-OFFICE OR WORKING REMOTELY

REMOTE WORK ENVIRONMENT SUSCEPTIBLE TO HACKING

- **Remember that working remotely presents challenges for you, your IT systems and IT staff – so you need to be very self-aware**
- **Increase awareness of information technology support mechanisms for employees who work remotely**
- **Make sure all employees have clear and concise instructions**
  - **All laptops/computers MUST have a strong password**
  - **All computers/laptops should have device encryption installed**
    - **BitLocker is available on all Windows 10 but must be set up – not automatic**
  - **Employees should only work from home or other SAFE environment**
  - **What employees should do if laptop/equipment is lost, stolen or breaks**
    - **You may not want outsiders working on laptops that have remote access**
    - **Verify all Corporate information provided by customers**
- **Monitor Employees**
  - **Log in check or monitoring logins**

TECHNOLOGY AND OTHER TOOLS AVAILABLE TO PROTECT THE PHYSICAL OR REMOTE LAW OFFICE



COMPUTER SAFEGUARDS

- **Encryption**
  - **Enable full disk encryption**
  - **Available on all computers, including laptops with Windows 10 or higher, but MUST BE ENABLED**
- **Antivirus/malware software**
  - **Many available for free but worth paying for full antivirus protection**
    - **Caution: don't allow staff to add any antivirus programs as they may cancel each other out**
- **Passwords**
  - **Unique and complicated**
  - **Password Manager**
- **Multi-Factor Authentication**

REMOTE ACCESS

- **Numerous Remote Access Apps Available**
  - **Chrome Remote Desktop**
  - **Team Viewer**
  - **Remote PC**
  - **GoToMyPC**
  - **LogMeinPro**
  - **AnyDesk**
  - **Splashtop**

- **Key Factors to Look For**
  - **VPN**
  - **Password**
  - **Multi-Factor Authentication**

SAFEGUARDS FOR WORKING REMOTELY

- Only use law firm approved devices while working remotely.
- Only allow authorized persons to use devices
- Don’t lend your device to anyone you don’t absolutely trust
- Lock device with PIN code.
- Make sure browser and email are using encryption when connecting to internet.
- If device supports VPN capabilities, you may be required to use them.
- Protect device by regularly updating OS and applications.
- Never allow others to connect their devices (phones/USB drives) to your laptop.

Protecting Your Personal Computer

- Always be sure your devices have the latest patches and are running the latest versions of any programs installed.
- Enable automatic updates on your computer and mobile devices.
- If you are no longer using a program, uninstall it.
- If you are logging in to a file server remotely, disconnect when you are not using it
- Keep your browser Plug Ins up to date.
- Consider using browser in "Private Mode" to protect information:
  - Will not record and track websites you visit
  - Will not cache website content
  - Usually wipes any cookies stored on your system
- Firewalls
  - Make sure Firewall is enabled
  - DO NOT DISABLE FIREWALL
- Perform daily backup

Passwords

Tips for strong passwords:

- **Make passwords long – every character makes it stronger & more secure**
- **Hard to guess – avoid public information, like birth date, pet's names or anything you may have shared on social media**
- **Easy to remember (perhaps a unique word written backwards exchanging numbers for letters)**
  - **N01tcarfn12023#"**
- **Use a Pass Phrase – multiple words with letters, numbers, symbols**
  - **Example "Karaoke1ng@CLLAnextMay"**
- **Use a unique different password for each account.**
  - **If one account gets hacked, your others will be safe**

Passwords (cont.)

- Use password manager – program that securely stores passwords and you only have to remember one strong password.
  - Check with IT team if authorized
- Password is secret – don't share with anyone else.
- For sites that require security questions, use questions that only you know answers to. Try to use information not publicly known.
- Use two-step verification process when possible; security codes that are emailed or texted.

Ways you can support Data Security

- Recognize sensitivity of information we are working with.
  - Expected to know and respect boundaries
- Only use systems authorized by law firm to handle sensitive information.
- Do not copy or store to unauthorized system or account, such as personal laptop or email account.
- Only used licensed software.
- If physical form of personal information is maintained, keep documents in a folder and store in locked cabinet when leaving.
- Use screen lock on computer when leaving computer.

Data Storage and Sharing

- Designated secure storage location
- Apps and Services
  - OneDrive
  - Dropbox
  - ShareFile
  - WeTransfer
- USB or external hard drops
  - These should be password protected and encrypted
- NOT on personal laptops
  - If one does not want to use an external hard drive or USB then laptop should be backed up to a Cloud service

Cloud Services

- Outside service provider to store, manage or process our data.
- Back up data to an off-site location
- Reason it's called "The Cloud" is because you never know where the data is stored.
  - Creating documents on Google Docs
  - Sharing files via Drop Box or Microsoft's One Drive
  - Storing pictures in Apple's iCloud
- Cloud services help us to be more productive but have risks.

Steps to Follow when Procuring a Cloud Storage Provider

- Various Cloud Services Available
  - Oracle Cloud
  - AWS (Amazon Web Services)
  - Microsoft Azure
  - Google Cloud Platform
  - Carbonite – perfect for home computers and/or small offices
- What to look for
  - Encryption of files being sent to the cloud and being retrieved from the cloud
  - Length of time files are maintained by the cloud

INADVERTENT DISCLOSURE/LAW OFFICE FAILURE

- Ethical obligations surrounding Inadvertent disclosure of confidential data and communication by electronic means
  - Duty to Client
  - Duty to Court
  - Duty to Opposing Counsel
  - Duty to Third Parties
- Duty to Refrain from Revealing confidential information by electronic means
  - E.g. Social media

DATA BREACH/CYBER ATTACK/CYBER THREAT

- Disclosure Responsibilities
  - Duty to Client
  - Duty to Court
  - Duty to Opposing Counsel
  - Duty to Third Parties
- FTC Safeguards Rule Amendment
  - Non-Banking Financial Institutions required to report cyber incidents affecting 500 or more people
  - Law firms generally not required to comply with the Safeguards Rule
  - Exemptions include
    - fewer than 10 employees including any independent contractors of the covered entity or its affiliates located in New York or responsible for business of the covered entity;
    - less than $5,000,000 in gross annual revenue in each of the last 3 fiscal years from New York business operations of the covered entity and its affiliates
    - less than $10,000,000 in year-end total assets

CYBER INCIDENT RESPONSE PLANNING

- Conduct Risk Assessments
- Avoiding Data Loss
  - Detecting Data Intrusion
  - Establishing, Securing and Updating Backup systems
  - Monitoring for cyber threats
- Data Recovery
- Post-Breach Investigations

Law Office Electronic Data and Communication Policies and Protocols

- Create, Adopt and Update Electronic Data and Communication Protection Policies
- Cybersecurity Insurance
- Create, Adopt and Update Cyber incident response plans for law office
  - Awareness of security best practices and industry standards
  - Evaluate how to best protect client and law office electronic data and communication

BEST PRACTICES FOR INFORMATION SECURITY [Adapted from AG directive]

- **Maintain a comprehensive information security program that includes regular updates to keep pace with changes in technology and security threats and reporting security risks to the firm's leadership**
- **Encrypt all private collected, used, stored and/or maintained**
- **Implement centralized logging and monitoring of network activity, including logs that are readily accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged**
- **Establish a reasonable patch management program, including appropriate monitoring of required updates, supervision of the program, and training for employees**
- **Develop a penetration testing program that includes regular testing of law office network security**
- **Update its data collection and retention practices, including only collecting data to the minimum extent necessary to perform legitimate business functions and permanently deleting all such data when there is no longer a reasonable business or legal purpose to retain such information.**