# Cybersecurity for Lawyers

## Ethical and Regulatory Issues in the Practice of Law

James Goepel, CMMC Information Institute

# Presenter

**Jim Goepel**
Co-Founder CMMC Information Institute

- **Law** – Represented government contractors and cybersecurity companies, including Unisys and Johns Hopkins University Applied Physics Laboratory.
  - Education: JD and LLM from George Mason University
  - Former Cybersecurity Professor: Drexel University Thomas R. Kline School of Law

- **Cyber/Technology** – GC and Director of Education and Content for cyberGRC platform. Former GC and CTO for cybersecurity tools vendor. Former CEO, cybersecurity consulting firm. Former infosec and IT person for US House of Representatives. Founding Director and Former Treasurer, CMMC Accreditation Body. Created and taught CMMC Registered Practitioner training program.
  - Education: BS in Computer Engineering from Drexel University.
  - Certifications: CMMC Provisional Instructor, CMMC Provisional Assessor, Certified CMMC Professional, Certified CMMC Assessor
  - Former Cybersecurity Professor: Drexel University LeBow College of Business

- **Books** – Data Privacy and Cybersecurity Law (LexisNexis); CUI Informed (CMMCInfo); CUI Demystified (CMMCInfo)

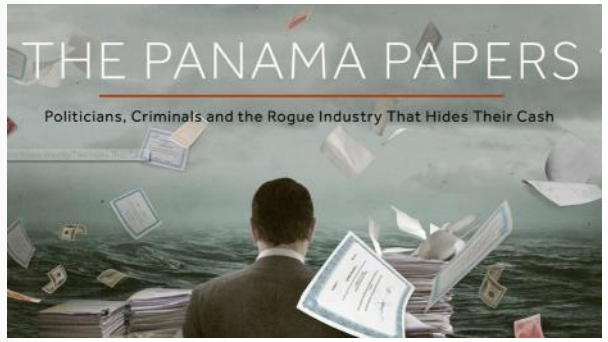
# Cybersecurity Impacts you Personally

- Everyone is being attacked. Constantly.
- Many attacks are crimes of opportunity rather than targeted attacks.
  - Automated online scanning
    - In 30 days, more than 5 million attacks against 10 honeypots
    - 52 seconds before first login attempt
    - US logins in less than 20 minutes
    - Ireland data center was the longest, with 1 hour 44 minutes before first login attempt
  - Malware-as-a-service
  - Phishing attacks

DLA PIPER

Cravath

BAKER WOTRING LLP




MOSSACK FONSECA

Weil

Wiley Rein LLP

# Cybersecurity impacts you professionally

Not only are law firms not immune, they are actively targeted.



PUBLIC CONTRACTING INSTITUTE

# ABA Model Rule of Professional Conduct 1.1

"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Comment 8 to Model Rule 1:

"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." (emphasis added)

# VSB Professional Guidelines Rule 1.1

"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Comment 6 to Rule 1.1:

"To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education in the areas of practice in which the lawyer is engaged. **Attention should be paid to the benefits and risks associated with relevant technology**." (emphasis added)

# ABA Model Rule of Professional Conduct 1.4

Attorneys must:

- reasonably consult with the client about the means by which the client's objectives are to be accomplished;
- promptly comply with reasonable requests for information;
- keep clients reasonably informed about the status of a matter; and
- explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.

Communication today is typically conducted via E-mail and digital files.

# VSB Professional Guidelines Rule 1.4

(a) A lawyer shall keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

(c) A lawyer shall inform the client of facts pertinent to the matter and of communications from another party that may significantly affect settlement or resolution of the matter.

# ABA Model Rule of Professional Conduct 1.6(c)

"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." [emphasis added]

Comment 18 lists several factors to be considered in determining reasonableness, including:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

# VSB Professional Guidelines Rule 1.6(d)

> "A lawyer shall make **reasonable** efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule." [emphasis added]

Comment 19 lists several factors to be considered in determining reasonableness, including:

- the sensitivity of the information
- the likelihood of disclosure if additional safeguards are not employed
- the employment or engagement of persons competent with technology,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software **excessively** difficult to use). [emphasis added]

# Pulling the Model Rules and VSB Guidelines Together

Attorneys clearly have ethical obligations to:

- ensure that the tools used in the process of providing services are reasonably secure; and,
- ensure they are educated on the risks and benefits associated with different technologies used in their practice.

# ABA Formal Opinion 483

Lawyers have an obligation "…(i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." (Page 5, first full paragraph)

"As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach." (Page 6, first full paragraph)

"The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach." (Page 6, first full paragraph)

# Ultimate Goal: Defensibility

- Incident response plans are a bad place to start
- Instead, define the firm's approach to risk management and use that to inform the incident response plan.
- Define:
  - The firm's attributes, including:
    - locations
    - business units/practice areas
    - clients/client types
    - impending changes/initiatives
    - types of information handled/processed
    - IT systems
  - Legal and regulatory requirements that come from these attributes

* Mead et al – Defensibility: Changing the way Organizations Approach Cybersecurity and Data Privacy

# Using the Firm's Attributes to Define Risk Management Approach

- Prioritize the firm's various attributes
- Describe their interrelationships (e.g., systems supporting clients/business units)
- Choose a mechanism for characterizing risks (heat maps/gut instinct, metrics)
- Define risks associated with high-priority attributes (don't sweat the small stuff, at least not right away)
  - Geographic issues due to where the location of the firm's offices and/or the firm's clients
  - Legal and regulatory risks associated with the types of information/nature of the work
  - Threats that are unique to a particular attribute type
- Characterize risk appetite – how much residual risk are you willing to accept?
- Characterize risk tolerance – how much can you deviate from that risk appetite?

* Mead et al – Defensibility: Changing the way Organizations Approach Cybersecurity and Data Privacy

# Define

- Risk Management Approaches:
  - Risk enhancement – seek out certain kinds of risks
  - Risk transfer – insurance, contractual requirements
  - Risk avoidance and mitigation – tools, policies, and procedures
- Policies, Procedures, Plans:
  - IT policies
  - Data classification and usage policy
  - System security plan
  - Business continuity and disaster recovery plan
  - Incident/breach response plan
  - Disaster recovery plan
  - Vendor risk management plan
    - Vendor questionnaires

* Mead et al – Defensibility: Changing the way Organizations Approach Cybersecurity and Data Privacy

# Or…

- Leverage analyses performed by the United States Government for its similar information
- Align your information security program to National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171
  - Designed to protect the government's most sensitive, but unclassified, information (controlled unclassified information, or "CUI"), including:
    - Legal work product and privileged information
    - Patent applications
    - Law enforcement information
    - Business information
    - Naval nuclear propulsion information
    - Critical infrastructure information
    - Security vulnerability information
- NIST SP 800-171 does not alleviate the need to perform the legal/regulatory review; that is baked into the framework

# Sample Legal/Regulatory Concerns

- California Consumer Privacy Act (CCPA) – Grants California residents new rights regarding their personal information and imposes various data protection duties on for-profit entities conducting business with California residents.
- 23 NYCRR 500 – Imposes requirements on "Covered Entities," including filing annual certification of compliance signed by Board of Directors or other senior person.
- DoD's CUI Requirements – DFARS 252.204-7012, -7019, -7020, and -7021
- Employers' duty of care with employee information – PA, NY, KY, Mass, 11th Cir., etc.
  - Dittman et al. v. Univ. Pitts. Med. Ctr. 649 Pa. 496 (Pa. 2018).
  - Ramirez v. Paradies Shops, LLC 69 F.4th 1213 (11th Cir. 2023)
- Federal Rules of Civil Procedure

# Pennsylvania Employers' Duty of Care

- Dittman v. UPMC, 2018 Pa. LEXIS 6051 (Pa. Nov. 21, 2018)
- Employers have an affirmative duty to keep employee records safe.
  - The Court determined that, as a threshold matter, it was not creating a new duty, but rather was "appl[ying] an existing duty to a novel factual scenario."
  - The Court also reasoned that UPMC engaged in affirmative conduct when it required the plaintiffs to submit their PII, which triggered a duty on UPMC's part to exercise reasonable care to protect the employees from risk of harm.
  - The Court also rejected UPMC's argument that it could not be liable under general tort law principles because the actions of the third-party hacker were a superseding event (i.e. not foreseeable). The Court agreed with the plaintiffs, and growing public consensus, that "troves of electronic data stored on internet-accessible computers held by large entities are obvious targets for cyber criminals" and a reasonable entity in UPMC's position should have foreseen that "failure to use basic security measures could lead to exposure of the data and serious financial consequences…" [for the employees].

# Federal Rules of Civil Procedure 37(e)

(e) FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

# 23 NYCRR 500

- Also applies to "…a person that:
  - (1) is not an affiliate of the covered entity;
  - (2) provides services to the covered entity; and
  - (3) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity."
- Person means "...any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association."

This includes law firms.

# FAR and DFARS Clauses

As outside counsel to government contractors, you are a subcontractor. If you are receiving CUI or FCI, **you are subject to flow-down requirements**, including:

- FAR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
- DFARS 252.204-7000 - Disclosure of Information
- DFARS 252.204-7008 - Compliance with Safeguarding Covered Defense Information Controls
- DFARS 252.204-7009 - Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- DFARS 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS 252.204-7019 - Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7020 - NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7021 - Cybersecurity Maturity Model Certification Requirement

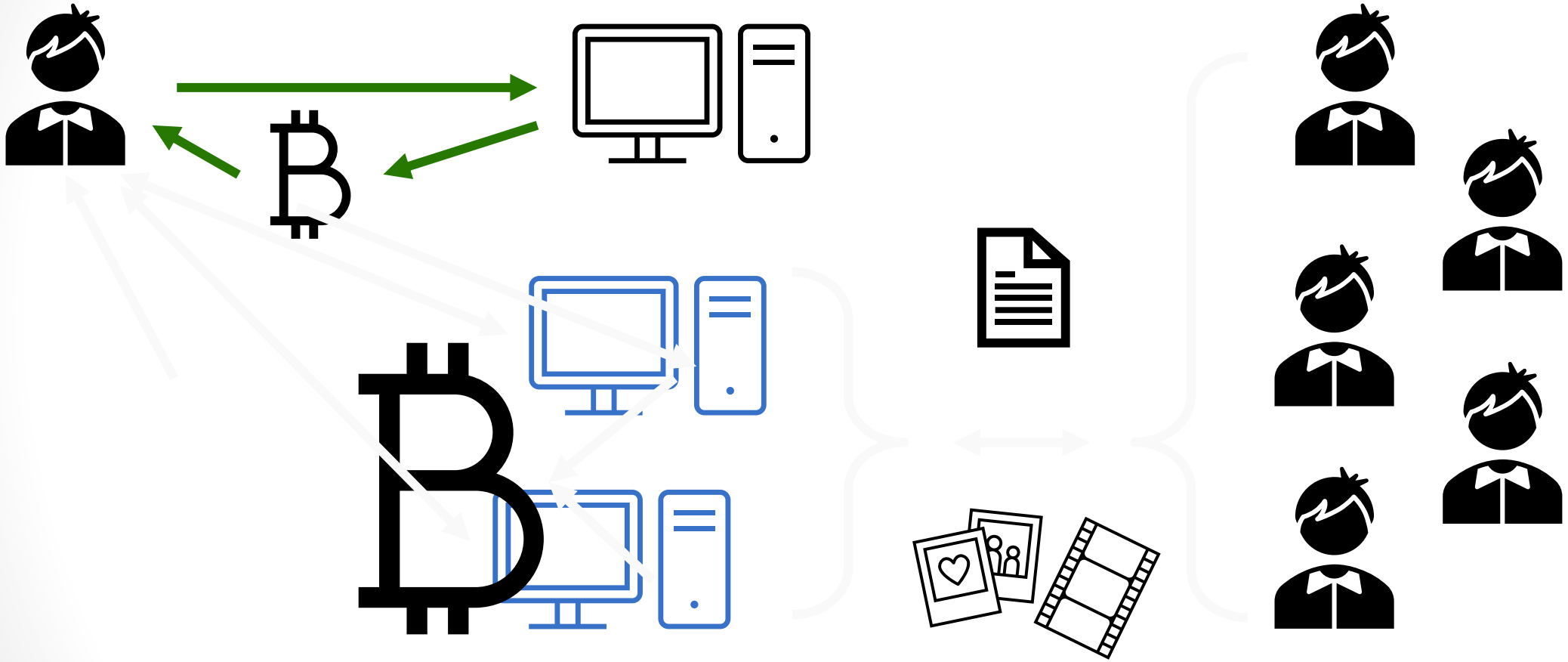
# Questions so far?

# Moving from Theory to Practice

# Threats and Risks

# Why do Criminals “Hack”?

# To Access Compute Resources



Combat this by: Whitelisting Software

# To Extort the Victims

- Ransomware
  - Your information is not exfiltrated
  - Information, including your client information, is encrypted with a key only the criminals possess
  - Pay a fee (typically cryptocurrency) to get the decryption key
  - Key is deleted after a period of time

- Highly disruptive
  - City of Baltimore shut down for multiple weeks
  - Large law firms and consulting companies have been hit and taken offline for multiple days

Defend against ransomware attacks by ensuring backups are working, conducted regularly, and that you have a strong incident response plan

- Instead of nightly/weekly, some systems create nearly instantaneous backups

# Extortion (continued)

- Ransomware 2.0
  - Encrypting your information, including your client information
  - Pay a fee (typically cryptocurrency) to get the decryption key
  - Key is deleted after a period of time

→ Slow “drip” of stolen information

Defend Against Ransomware 2.0 through backups and:

- Encrypting of data at rest and in motion
- Careful management of encryption key data
- Role-based access controls

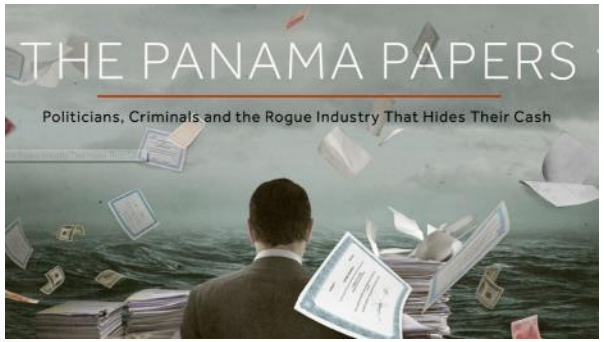
# A Note on Ransomware Payments

- US Department of Treasury Office of Foreign Assets Control – October 1, 2020
  - Under the authority of … the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. … OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

  - Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.

# To Commit Espionage and Foster Political Unrest

- Industrial secrets
- Military/government secrets
- Sow seeds of distrust and insurrection



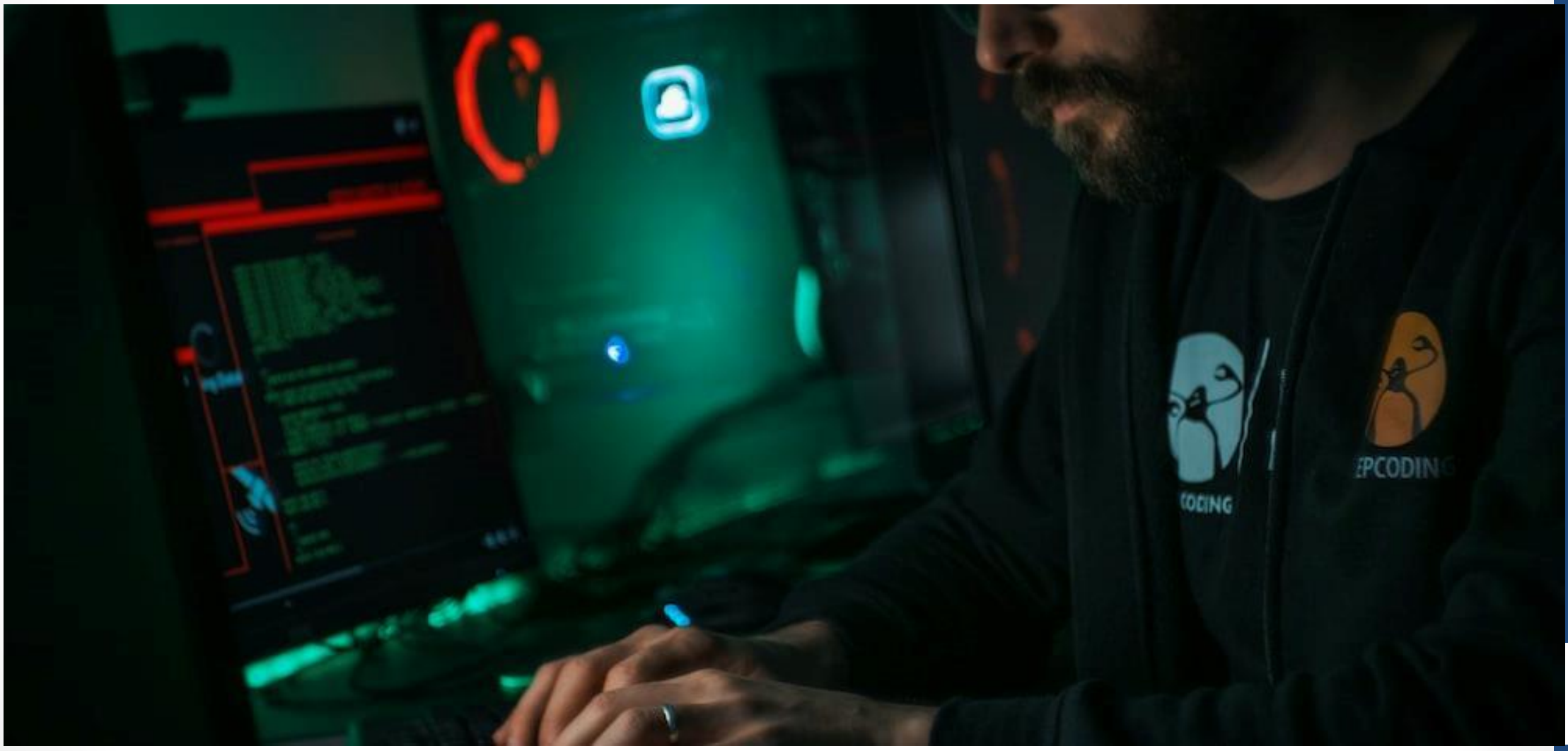

MOSSACK FONSECA

JONES DAY®

Hacker claims to have stolen files from law firm tied to Trump: WSJ | TheHill

# As a Basis for Island Hopping

# Common Attack Vectors



# How do they get in?

- Vishing, Phishing, and Spear Phishing
- Brute Force and Credential stuffing
- Exploiting vulnerabilities

# Phishing and Spear Phishing

Phishing: the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Spear Phishing: an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.



## Defending Against Phishing and Spear Phishing:

- Scanning incoming E-mails, chats, text messages, LinkedIn threads, etc. for malicious attachments and links.
- Being aware of the risks before clicking a link, opening an attachment, visiting a website, or responding to an "urgent" issue.
- Allowing antivirus software to run uninterrupted.





See: https://www.cnn.com/2019/10/27/business/phishing-bank-scam-trnd/index.html

# Vishing

Real Future: What Happens When You Dare Expert Hackers To Hack You (Episode 8) – YouTube (1:15 to 4:03)

Defending Against Vishing: Training, policies, and enforcement

# Brute Force and Credential Stuffing

**Credential Stuffing**

| | | |
|---|---|---|
| Bob's Kabab House | Along@srstlaw.com | 1234321 |
| Alice's Aardvarks | Sweber@srstlaw.com | ILuvAardvarks |
| Red's Rods and Reels | Bkilarney@srstlaw.com | IFish2! |
| Dandy Donuts | Along@srstlaw.com | IE@tDonuts |
| Sue's Sweets | Sweber@srstlaw.com | ILuvAardvarks |
| Netflix | Along@srstlaw.com | aaabbbccc |
| Netflix | Sweber@srstlaw.com | Password1! |

**Brute Force**

| | | |
|---|---|---|
| 123456 | admin | Password1! |
| 1234567 | charlie | princess |
| 123456789 | dragon | qwerty |
| 123123 | football | secret |
| 123qwe | iloveyou | sunshine |
| 11111111 | monkey | welcome |
| 2222222 | nothing | |
| 654321 | password | |
| 1q2w3e4r | password1 | |

Defending Against Brute Force and Credential Stuffing Attacks



Don't reuse passwords or logins



Don't use common passwords



Enable multifactor authentication anywhere you can

# Exploiting Vulnerabilities

## Limiting Vulnerabilities:

Ensure software is up to date (patched)

Retire equipment after its end-of-support date

Don't use unauthorized equipment

This applies to all equipment, including:

- Computers
- Mobile devices
- Printers

- Network equipment
- "Smart" devices
- Phones and alarms



https://splinternews.com/i-dared-two-expert-hackers-to-destroy-my-life-heres-wh-1793854995

# Basic Dos, Don’ts, and “Think Carefullys”

Do: Keep client information only on Firm equipment.

Do: Stop and think before you click on any link!

Do: Be suspicious of all attachments and E-mails from strangers.

Do: Use your work E-mail only for work.

Do: Limit use of work equipment for personal purposes.

Do: Use Multifactor logins wherever possible

Do: Keep software and equipment patched

Do: Encrypt portable media

Don’t: share accounts

Don’t: reuse passwords (do use a password manager)

Don’t: install unauthorized software.

Don’t: use public WiFi

TC: installing smart devices

TC: allowing outside devices onto your home or firm network

TC: buying generic “cyber insurance”

TC: assuming your IT staff is doing all of this

# Recommended Basic Firm Policies

**Passwords:**

- Must be at least 8 characters;
- Cannot be dictionary words or obvious/common variations of them
- NOTE: NIST SP 800-63C Appendix A says longer passwords are better, no need to reset passwords regularly unless you suspect a breach or that the password was reused elsewhere.

**Equipment:**

- Mobile device management allows Firm to force wipe of lost/stolen equipment
- Encryption is enabled for all data at rest.
- All portable media (e.g. USB drives, DVDs, external hard drives) must be encrypted.
- All equipment, media, or paper files containing client information, including case files, must be destroyed in accordance with the Firm's policy.

**Accounts:**

- Access to a particular client file/case is limited to only those who need access.
- All new software must be approved prior to installation. Only installed by those with administrator privileges.
- Employees will not have local administrator privileges.
- Employees with admin accounts must only use those on an as-needed basis.

**Training:**

- Annual (long-form) employee training on firm policies
- Regular (short-form) refreshers to keep information top of mind

# Consider Independent 3rd Party Assessment

- Smart practice for defensibility purposes
  - NIST Cybersecurity Framework
  - CIS Top 20 Controls
  - NIST SP 800-171
- CMMC certification will be required for those working with DoD contractors or as a DoD contractor (e.g., litigation support)

# Questions?