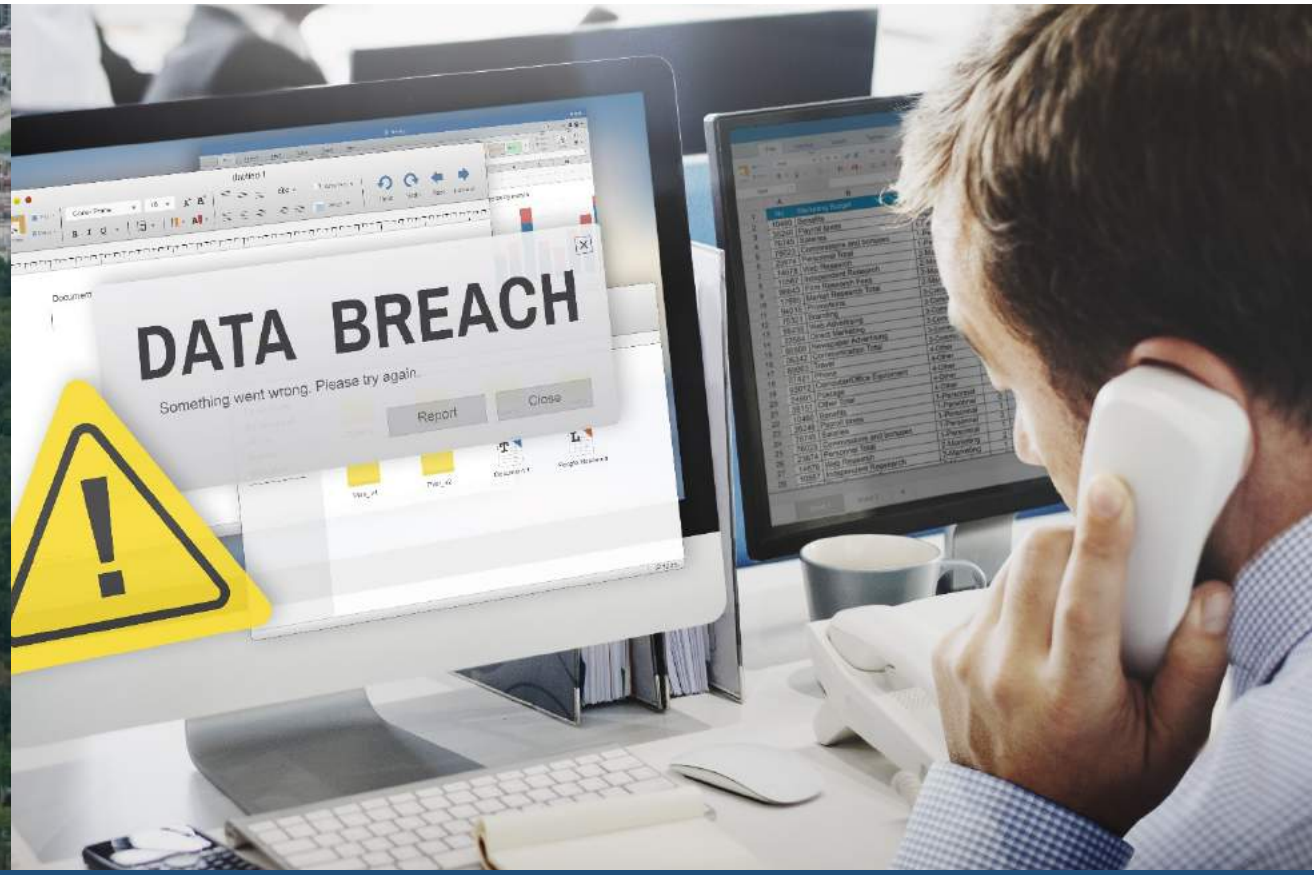
Headless Chickens and Zombie Data: Your Ethical Obligations for Disasters and Data Breaches



DC Bar

February 20, 2020

Sharon D. Nelson, Esq. and John W. Simek
President and Vice President, Sensei Enterprises, Inc. 703.359.0700 https://senseient.com

Hurricanes Irma (8/30/17) and Maria (9/16/17)

- Tom Bolt, managing partner at Bolt Nagi
- Law firm totaled
- Irma peeled roof off, Maria saturated everything
- Airport closed, hospital devastated
- Power out, no cell communication, no Internet
- Relocated to temporary office
- Helped clients, provided disaster recovery services
- Cloud backups, inventory and pre-storm photos
- Support of friends in ABA Law Practice Division

ABA Formal Opinion 482 – Ethical Obligations Related to Disasters (September 19, 2018)

- Model Rule 1.4 requires lawyers to communicate with clients
- After disaster, how will you communicate with clients?
- Electronic or paper lists of current clients/contact info
- Stored in easily accessible manner

Ethical Obligations Related to Disasters

- Can lawyer continue to serve clients?
- Must lawyer withdraw?
- Emergency contact info in engagement letter
- Always mindful during disaster of Rule 1.1 (Competence) and Rule 1.6 (Confidentiality)
- “Reasonable efforts”

What is Reasonable?

- The **first duty** is to preserve life
- The **second duty** is to preserve the essence of your firm, while attempting to **maintain client confidentiality**
- Dealing with fire – police – military or civic authorities

Mistakes from Katrina, Harvey, Irma and Maria

- No disaster recovery plan
- No off-site storage of backups
- Off-site storage at their homes a few miles away
- No plan for a lack of telephone communications
- No plan for a lack of access
- No plan for a failure of basic services – prolonged power outage

What Do You “Reasonably” Plan For?

- An alien attack?
- Being hit by a meteorite?
- Fires?
- Floods?
- Earthquakes?
- Terrorist attacks?
- North Korea nuclear strike?
- Extended power outage?

What Do You “Reasonably” Plan For?

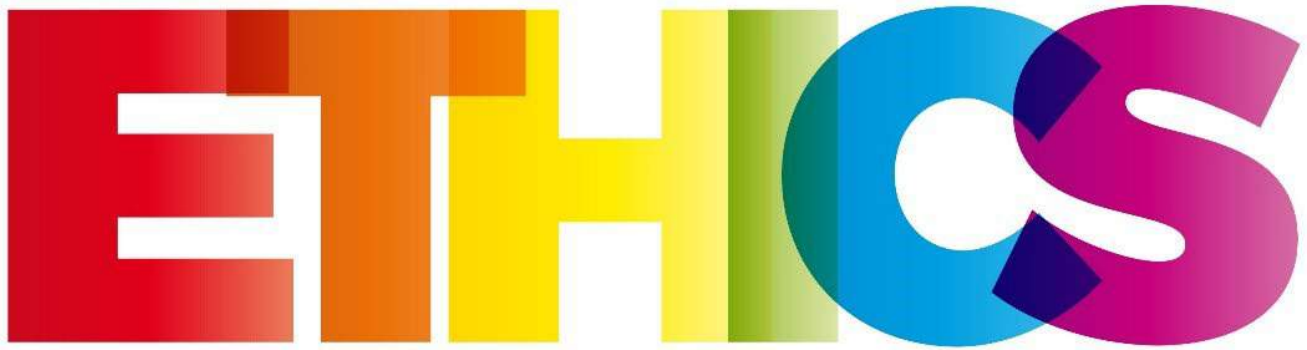
- Hackers?
- Disgruntled employees and sabotage?
- Plagues? Ebola? Biological attacks?
- Cyberwar?
- Ransomware?
- Total system meltdowns?

Ethical Obligations Related to Disasters

- May not have access to paper files
- Consider storing files electronically
- Cloud service (the usual choice)
  - Reputable company
  - Reasonable steps to ensure confidentiality and accessibility

Cloud providers

- Experience with law firms
- Encryption
- Multi-tenant
- Data location
- Redundancy/Availability
- Law enforcement access
- Exit strategy
- Read the ToS
- At LEAST have a backup in the cloud



Ethical Obligations Related to Disasters

- Notice of impending disaster
  - Transactional lawyers may want to complete impending transactions
  - Transfer funds to a trust account that will be accessible post-disaster
  - Contact financial institution – how will lawyers obtain access to their accounts?
- After disaster
  - Must notify clients/affected third parties for whom lawyer is holding funds if lawyer is unable to access funds

Ethical Obligations Related to Disasters

- Rule 1.16(a)(1) - Withdrawal required if representation will cause lawyer to violate rules of professional conduct
- Rule 1.16(a)(2) - Withdrawal if “the lawyer’s physical or mental conditional materially impairs the lawyer’s ability to represent the client” (severe injury/mental distress)
- Rule 1.16(b)(7) - Allows terminating representation if there is “other good cause for withdrawal.”

Ethical Obligations Related to Disasters

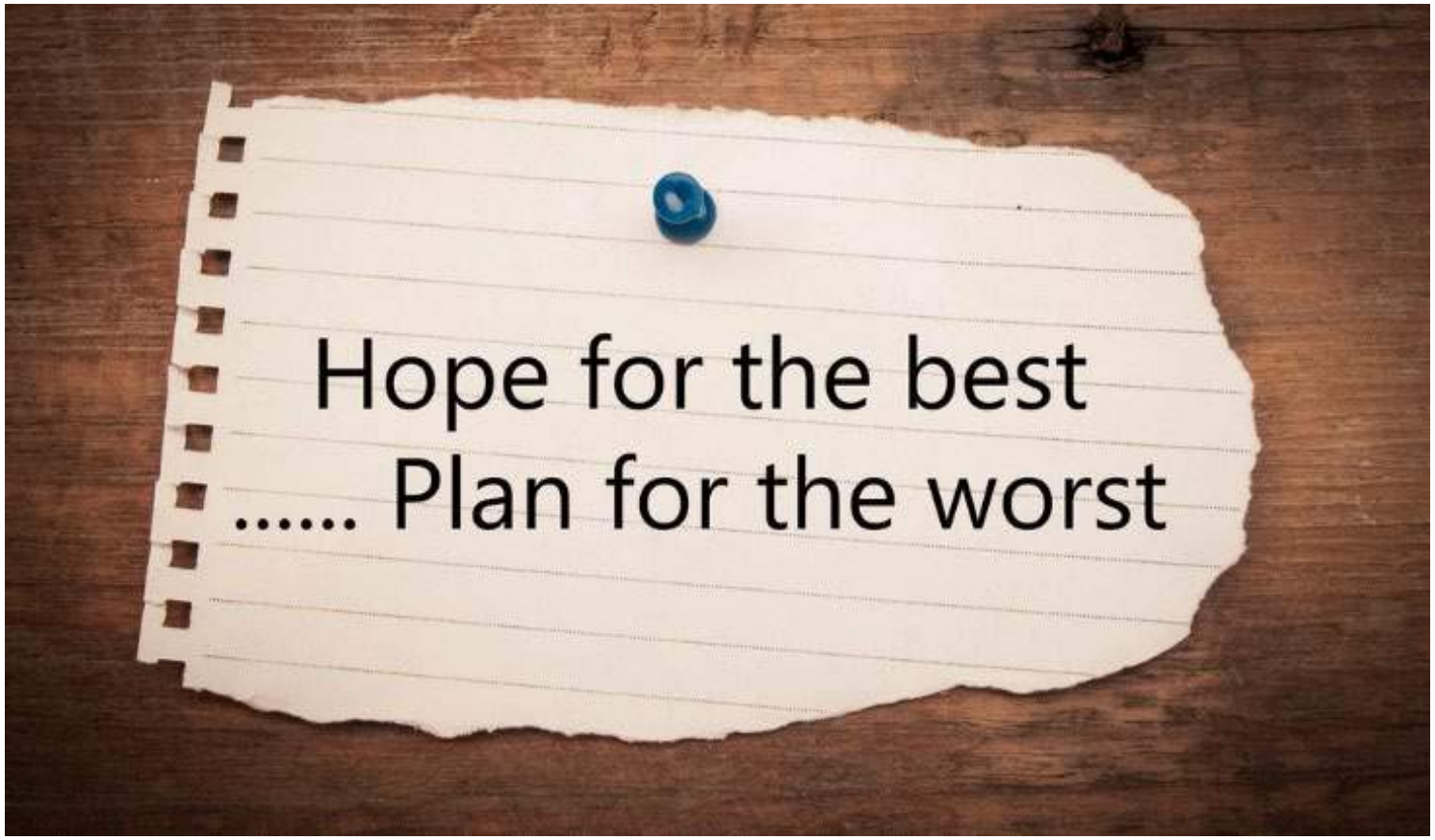
- Representation of clients displaced by disaster
- May be able to rely on versions of Model Rule 5.5(c) allowing temporary practice to “practice in” jurisdictions to which clients have relocated
- But NOTE that these rules vary

Ethical Obligations Related to Disasters

- Temporary practice by lawyer in another jurisdiction where lawyer has relocated
- Again, Model Rule 5.5 may authorize lawyer to practice temporarily where not licensed
- Again, NOTE that these rules vary
  - Some may require registration by relocated lawyer
  - ALL limit this authority to practice

Ethical Obligations Related to Disasters

- “Lawyers who maintain only paper files or maintain electronic files solely on a local computer or local server are at higher risk of losing those records in a disaster”
- Duty of communications means lawyers must notify current clients of the loss of documents with intrinsic value – original executed wills and trusts, deeds, negotiable instruments.

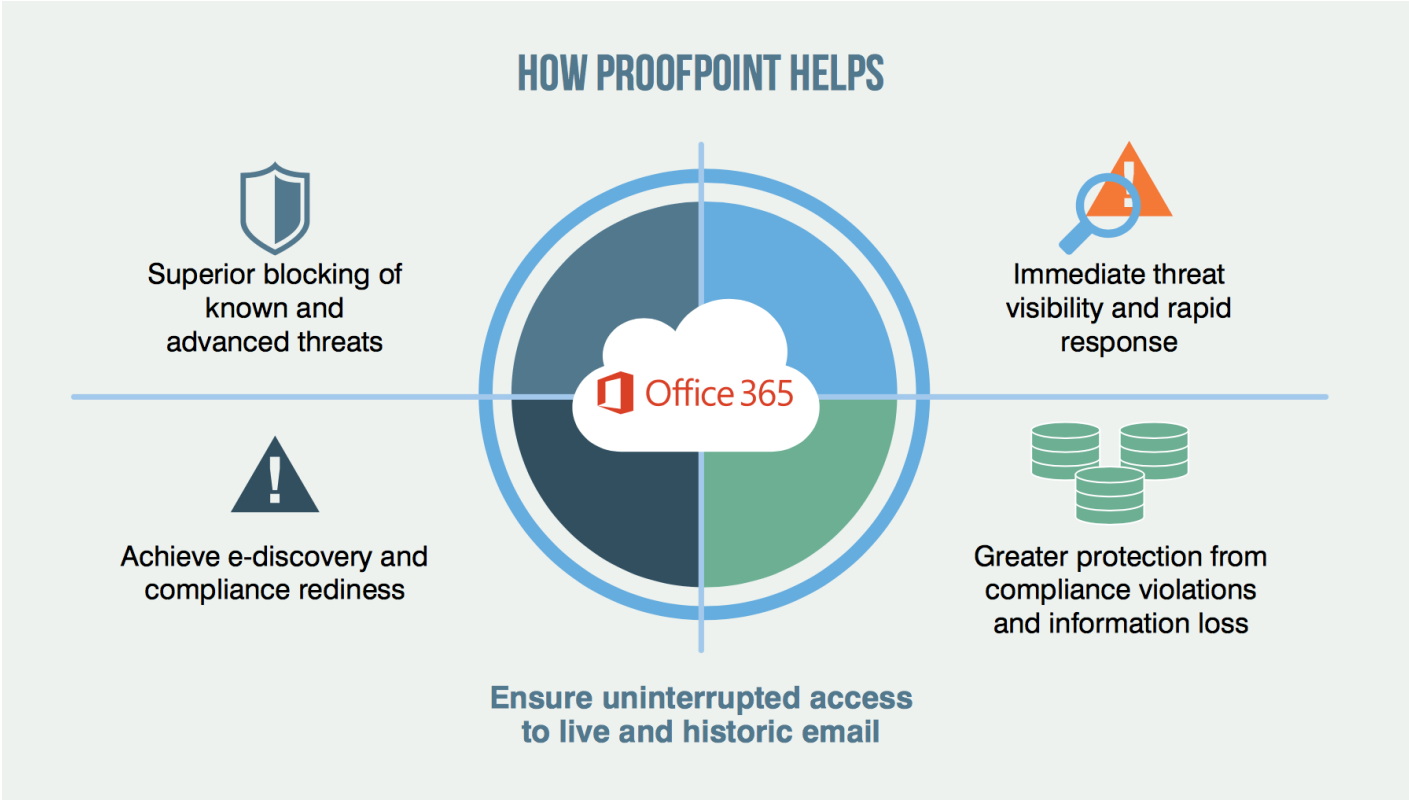


Ethical Obligations Related to Disasters

- Same duty applies to former clients based on Rule 1.15 (safeguarding client property)
- Must make reasonable efforts to reconstruct those documents or obtain copies from an external source

Your two best friends in a disaster

Use technology that helps you



- Mimecast and Proofpoint will make your email available in real-time and will sync with your Exchange server when it comes back online
- Other services will spool your email and make it available when you come back online – these are cheaper but not as robust
- Passwords should be stored (encrypted) in the cloud

Use technology that helps you

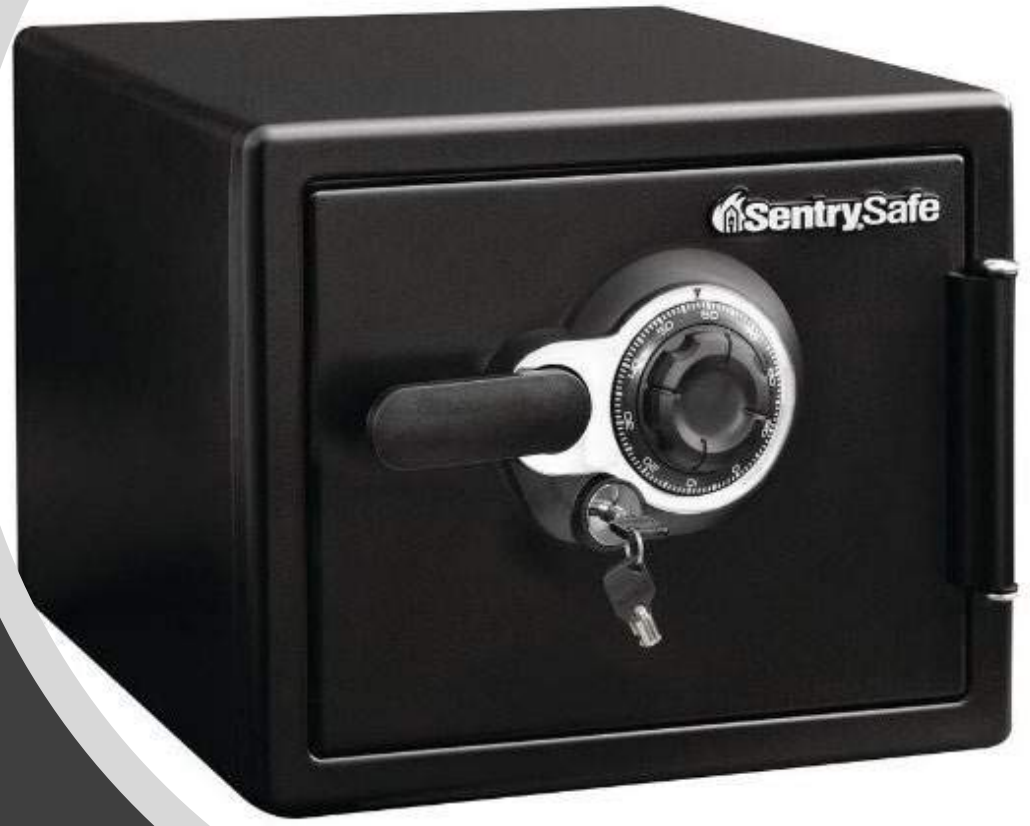
- Uninterruptable Power Supply (UPS) – all of your computers, severs, networking hardware, phone systems, etc. should be on a UPS
- Protects against power surges, dirty electricity and outage
- Allows proper shutdown of devices
- May give you sufficient power long enough to contact rescue personnel
- Software configurations of all network devices should be backed up and stored in a secure location

Technology

- Is it simply gone?
- Can you dry it out if it’s flooded?
- What if it was melted by fire?
- What can be recovered? Do you know a white lab?
- Can you outsource or lease short term?
- How can you get back to business temporarily and then long term?

Security

- If mobile devices lost in the disaster (should be encrypted) remotely wipe them
- Secure the office as soon as possible
- Looting and destruction are a fact of life
- Get waterproof and fireproof safes out of the office
- Change all passwords



Ethical Obligations Related to Disasters

- “Lawyers should maintain an electronic copy of important documents in an off-site location that is updated regularly.”
- May maintain solely as electronic copies except where law, court order or agreement require paper copies as long as files “are readily accessible and not subject to inadvertent modification or degradation.”
- Seriously consider revising engagement letters
  - Authority to maintain only electronic versions
  - Limited retention period

Get rid of
Zombie data!

Ethical Obligations Related to Disasters

- Solicitation and Advertising - must comply with Model Rules 7.1-7.3
- Live person to person contact generally prohibited
- OK to offer pro bono services to disaster victims – subject to authority to practice in jurisdiction
- Check rules in relevant jurisdictions

Law firm data breaches

- 2019 ABA Legal Tech Survey – 26% of respondents reported that their firm had been breached
- “I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.” Former FBI Director Robert Mueller, RSA Cybersecurity Conference, March 2012

ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack – 10/17/18

- For background, see ABA Formal Opinion 477R explaining lawyer's ethical responsibility to use reasonable efforts when communicating confidential client information via the internet.
- Opinion 483 – obligations after a breach and addresses only breaches that involve information relating to client representation.

ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack – 10/17/18

- **Does not address other laws re: privacy, data breach notifications, HIPAA, Graham-Leach-Bliley, etc.**
- Compliance with this opinion depends on nature of cyber incident, ability of attorney to know the facts about it, the attorney's roles, level of authority and responsibility in law firms operation

Cyber incident vs. data breach

- Cyber incident - Refers to any occurrence that threatens the confidentiality, integrity or availability of information. This might be the result of a cyber attack, perimeter breach or an insider threat (including policy violations).
- Data breach – data has been exfiltrated (taken) or unauthorized access to it

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- Rules 1.1 and 1.6 – Lawyers must use and maintain technology used to represent clients and must use it in a manner that reasonably safeguards information
- Competence obligation met through lawyer's own study or employing/retaining qualified assistance
- Obligation to monitor for a data breach
- Many cyber events are not breaches because client confidential information is not compromised
- What about ransomware? It depends.

Ransomware

- Encrypted data
- Loss of access
- User action?
- Cryptocurrency payment
- Recovery
- December 2019 – cybercriminals began “outing” data if ransom not paid – must ransomware now be treated as a data breach?

Obligation to monitor for a data breach

- Monitor access to data
- Unauthorized access
- Logging
- IDS/IPS
- Breached months before discovery

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

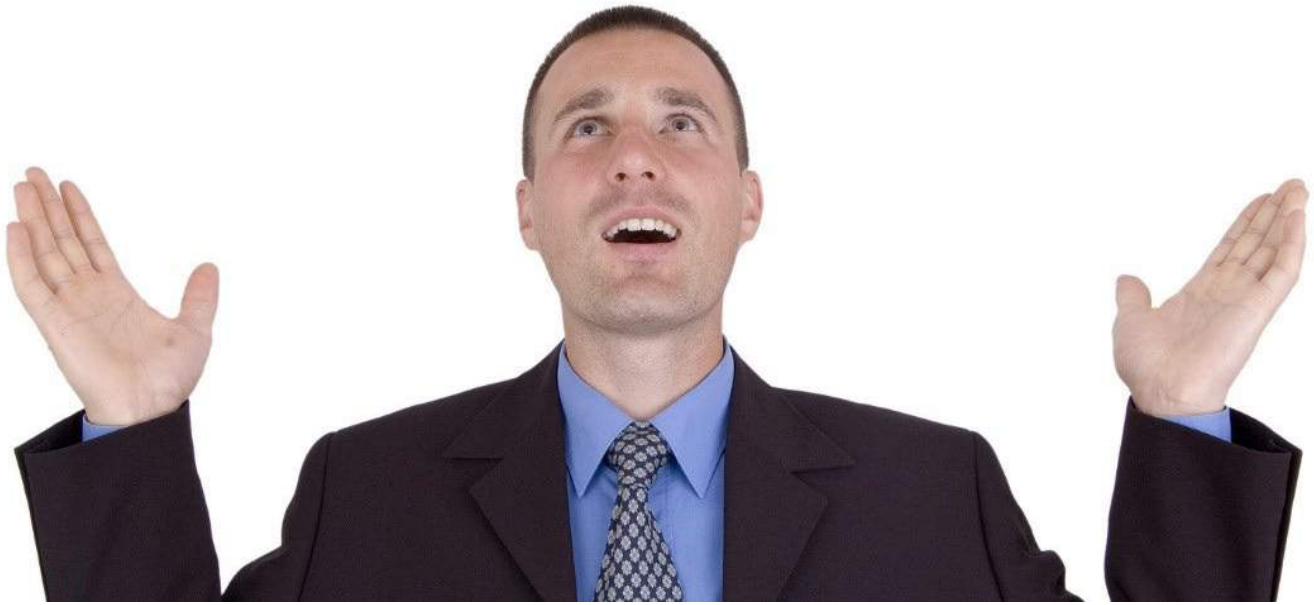
- Lawyers must employ ***reasonable efforts*** to monitor technology, resources connected to the internet, external data sources and external vendors providing data services
- Potential for ethics violation occurs when a lawyer doesn't undertake ***reasonable efforts*** to avoid data loss or to detect cyber-intrusion and that lack of reasonable effort causes the breach

Stopping the Breach and Restoring Systems

- When breach is suspected or detected, Rule 1.1 requires lawyers to act reasonably and promptly to stop the breach and mitigate damage
- How is beyond scope of the opinion
- Lawyers should have an Incident Response Plan
- IRPs minimize loss or theft of information and disruption of services

Incident Response Plan

- Only 31% of law firms have them (2019 ABA LTRC Survey Report)
- Faster you catch a cyberattack, the less it will cost you and the faster you can recover
- You are no stronger than your weakest link (usually your employees)
- With a good IRP, preparation is 2/3 of the effort – the remaining 1/3 is solving the problems when an attack occurs
- Without an IRP, the “headless chickens” reaction



Incident Response Plans

- Who is in charge?
- How to contact employees?
- Detect the problem(s)
- Remediate and document the problem(s)
- Assess (as reasonably as possible) whether data was compromised
- Communication with clients
- Recovery – new systems required? New policies?
- Likely to need experts to help

Your ethical “get out of jail free” card

- Comment 18 to Model Rule1.6(c) - If you make “reasonable efforts” to prevent unauthorized access or disclosure of information relating to the representation of a client, then no discipline
- Reasonable efforts depends on:
  - The sensitivity of the information
  - Likelihood of disclosure without additional safeguards
  - Cost of additional safeguards
  - Difficulty of implementing safeguards
  - Whether safeguard adversely affect the lawyer’s ability to represent clients

Reasonable security? It changes. Today?

- Backup
- Encryption
- Firewalls
- Policies
- Passwords
- MFA
- Least privileged access
- VPNs
- Physical security

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- Discretion to disclose information to law enforcement about a breach (in addition to what is mandated by law). Considerations:
  - Would the client object?
  - Would the client be harmed?
  - Would reporting the breach benefit the client by assisting in ending the breach or recovering stolen information?
- Without consent of the client, the lawyer may only disclose information which would assist in ending the breach or recovering stolen information

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- Rule 1.4(a)(3) Lawyer must keep client reasonably informed
- Rule 1.4(b) Must communicate to extent reasonably necessary to allow client to make informed decisions about the representation
- Under both, lawyer must communicate with current clients about a data breach
- Breach involves the misappropriation, destruction or compromise of client confidential information

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- Rule 1.15 Safeguarding property – applies to hard copy and electronic client files
- Nonetheless, it is Rule 1.4 which commands the lawyer to communicate a data breach
- What about former clients? Opinion says *ethics rules* do not require notice to former clients – but other laws or regulations might
- Practice tip: Return files to client at end of representation or have data destruction policies which clients agree to – engagement letter or at end of representation

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- Breach notification requirement
- Ransomware with no exfiltration of data? Notice not required unless data inaccessible for a material amount of time. Opinion doesn't consider recent developments "outing" data of those who don't pay ransom.
- Disclosure must be sufficient for client to make informed decisions about what, if anything, to do.
- Clients should be advised of lawyer's plan to respond to the data breach, including steps taken to enhance security
- Continuing duty to advise of progress post-breach
- PII? Triggers data breach notification laws in all 50 states, DC, Guam, Puerto Rico and the Virgin Islands

Steps after data breach

- Call data breach lawyer
- Review IRP
- Call digital forensics company to investigate/remediate
- Call FBI Regional Office
- Communicate with clients
- Need to alert bank? Insurance company?
- Follow data breach notification laws/privacy laws/regulations
- Policies and technology need to be upgraded?