

Ethical Considerations for In-House Counsel in a Connected World

Health Law Webinar

May 10, 2023

Fredrikson

Where Law and Business Meet[®]



MANKOFF

“No, Thursday’s out. How about never—is never good for you?”

Bob Mankoff/The New Yorker Collect/Conde Nast

Agenda

- Risk Landscape – Phishing, Ransomware and Wire Fraud, Oh My!
- Why Information Security and Ethics Matter to In-House Counsel – Trust me, they do!
- Sources of Ethical Obligations – "The Good Stuff"
- Additional Considerations – "The Practical Stuff"
- Recap – It's a Surprise



Risk Landscape

Over 23K People Compromised By Data Breach At Mid-Sized Firm... In Case You're Wondering How Bad These Can Get

There's no such thing as a 'small' data breach for firms.

By JOE PATRICE on May 18, 2022 at 2:44 PM

<https://abovethelaw.com/2022/05/over-23k-people-compromised-by-data-breach-at-mid-sized-firm-in-case-youre-wondering-how-bad-these-can-get/>

Law firm informs 255K of HIPAA data incident 10 months after hack

[Jessica Davis](#) September 9, 2022

<https://www.scmagazine.com/analysis/ransomware/law-firm-informs-255k-of-hipaa-data-incident-10-months-after-hack>

Bricker & Eckler Agrees to Settle Class Action Data Breach Lawsuit for \$1.95M

Posted By HIPAA Journal on Sep 20, 2022

<https://www.hipaajournal.com/bricker-eckler-agrees-to-settle-class-action-data-breach-lawsuit-for-1-95m/>

The Risks are Everywhere...

- **"Fact" A**

- *According to Gartner, estimated 20 billion connected devices as of 2020*
- *Predicted to quadruple by 2024-25*

- **"Fact" B**

- *Circa 2016, the Mobile Marketing Association of Asia estimated that only 4.2 billion people worldwide used toothbrushes*

- **Conclusion**

- *Dentists are losing the war against plaque and gingivitis!*

...and They are Significant!

IBM's "Cost of a Data Breach" Report for 2022 identified the U.S. as having the highest average cost for data breaches

A data breach in the US costs over twice the global average

For the 12th year in a row, the United States holds the title for the highest cost of a data breach, USD 5.09 million more than the global average.

\$9.44M

Average cost of a data breach in the United States

\$4.35M

Global average total cost of a data breach

Particularly for Outside Counsel

Legal sector is cyber “soft underbelly”

Latest News / By Caroline Hill - Editor-in-Chief / 2 May 2019







The legal sector is lagging financial services by a decade when it comes to cyber security, founder of the Security Awareness Special Interest Group Martin Smith MBE told delegates at this year’s Legal Leaders IT Forum.

Source legaltechnology.com

"Lawyers sling millions of gigabytes of confidential information daily through cyberspace, conducting much of their business via email or smartphones and other mobile devices that provide ready access to documents. But the new tools also offer tempting targets for hackers, who experts say regard law firms as ‘soft targets’ in their hunt for insider scoops on mergers, patents and other deals." Wall Street Journal, June 25, 2012.

Key Attack Vector – No. 1: Phishing

Phishing emails: More than 25% of American workers fall for them

    |  by **Hope Reese** in **Security** 
on December 9, 2020, 9:28 AM PST

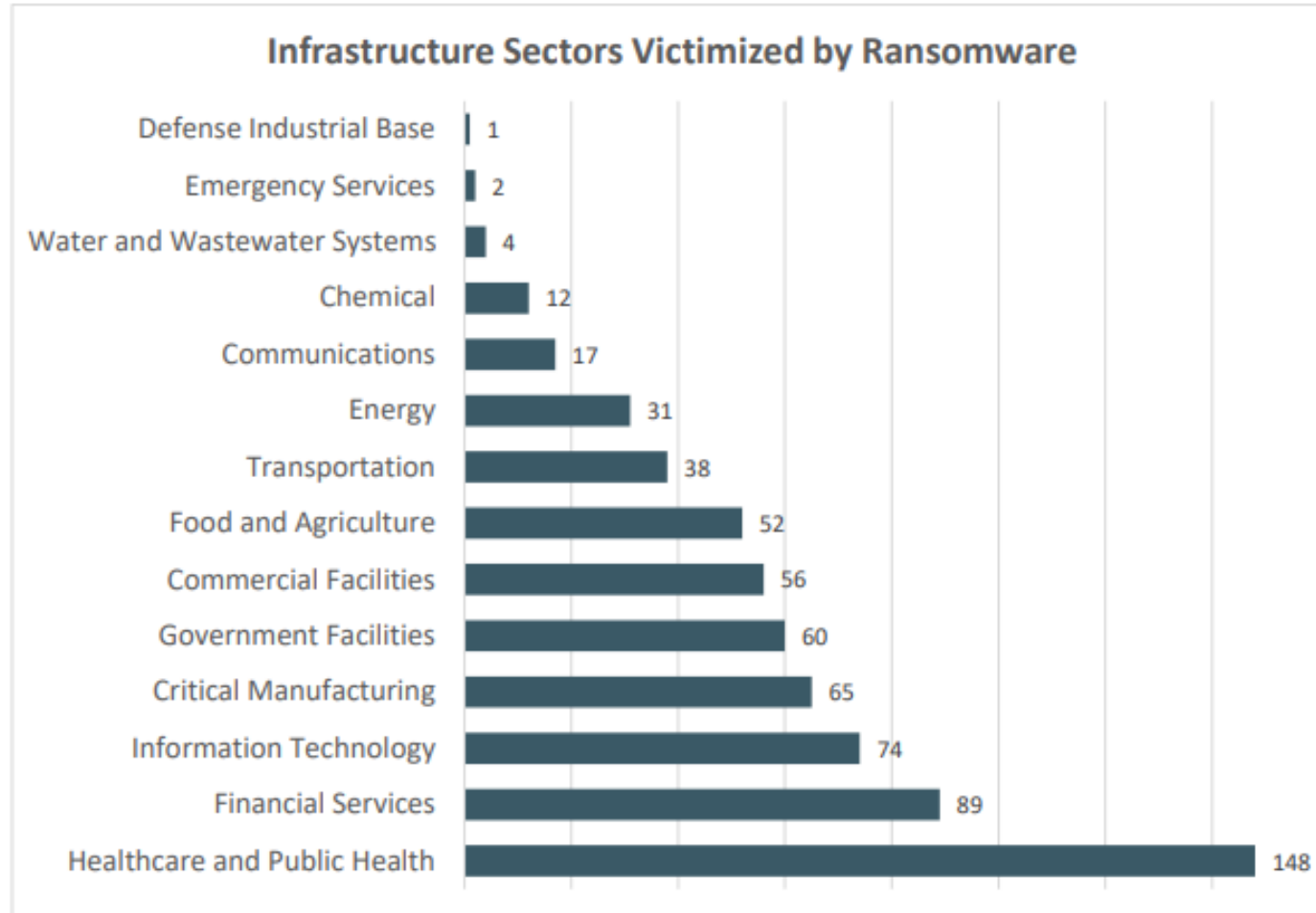
A new global report on phishing attempts shows how the workforce has responded to security threats since COVID-19, and the new vulnerabilities that have resulted from the remote work landscape.



Key Attack Vector – No. 2: Ransomware

- "So hot right now" – estimates place world-wide losses in 2021 at \$20 billion
- Number of incidents in 2021 doubled from 2020
- Double ransom scenarios becoming the norm, with threat actor exfiltrating data before releasing the ransomware
- Threat actor may deny access to websites and harass victim's customers and employees
- Large ransom demands – avg. \$1.2mm
- Average cost = \$4.54 million

FBI 2021 Internet Crime Report



Key Attack Vector – No. 3: Funds Transfer Fraud

- Funds transfer fraud – a/k/a business email compromise, “man-in-the-middle,” etc.
- Involves a threat actor compromising an employee’s (sometimes C-suite) email credentials and posing as the employee in order to divert or interrupt a payment stream
- Objective is typically financial – e.g., wire transfers, employee paycheck disbursements
- FBI estimates losses in 2021 to funds transfer fraud to be **\$2,395,953,296**



INTERPOL

THE ANATOMY OF BUSINESS EMAIL COMPROMISE

3 TOXIC INGREDIENTS



=

Millions in
illegal profits

Hacking

An email account is compromised through malware, employee intrusion, etc.

Social engineering fraud

The victim is manipulated into providing information or funds.


Money laundering

Multiple transfers are made involving foreign banks/institutions

#BECareful

And, Sometimes, An “Oldie but Goodie”

- Client sought representation from an Iowa attorney in connection with a large bequest—\$18.8 million—from long-lost Nigerian cousin
- Catch was that client needed to pay \$177,660 in inheritance taxes
- Iowa attorney charged 10% contingency to recover inheritance
- Iowa attorney solicited loans from other current and former clients to cover inheritance taxes: Promised to quadruple their investment
- Iowa Supreme Court suspended the lawyer's license for 12 months - grounds included violating duty of competence
 - *The best line from the opinion: The lawyer "appears to have honestly believed—and continues to believe—that one day a trunk full of...one hundred dollar bills is going to appear upon his office doorstep."*



Why Information Security and Ethics Matter to In-House Counsel

The Ethics Rules Apply to In-House Counsel

- **Model Rule of Professional Conduct 1.0(c):** "'Firm' or 'law firm' denotes a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization."
- **Comment 3:** "With respect to the law department of an organization, including the government, there is ordinarily no question that the members of the department constitute a firm within the meaning of the Rules of Professional Conduct."

In-House Counsel's Supervisory Authority

- **MRPC 5.1(a):** A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.
- **Comment 1:** This includes...lawyers having comparable managerial authority in...a law department of an enterprise...
- **MRPC 5.1(b):** A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

Supervisory Authority Responsibilities

- **MRPC 5.1(c):** A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:
 - *(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or*
 - *(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.*
- **MRPC 1.1:** Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer...must reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client[.]



"REMEMBER, WE'RE ALL IN THIS TOGETHER--EXCEPT FOR PURVISON, WHO WILL TAKE ALL THE BLAME."

Cartoonist: Harley Schwadron



Sources of Ethical Obligations

Duty of Competence

- **MRPC 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 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...
- **ABA Formal Opinion 477R:** Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.

"I'm here live; I'm not a cat."



What does this mean?

- "[L]awyers necessarily need to understand basic features of relevant technology...For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document."

- ABA Commission on Ethics 20/20 Report 105A

Case Study

Law firm's use of a spam filter that was configured to auto-delete emails as spam (with no manual review) and lack of appropriate email backup systems did not relieve the client of being responsible for an order assessing attorneys' fees that the client never received in time to file an appeal.

Based on this testimony, the trial court could conclude that Odom & Barlow made a conscious decision to use a defective email system without any safeguards or oversight in order to save money. Such a decision cannot constitute excusable neglect.

Emerald Coast Utilities Authority v. Bear Marcus Pointe, LLC, Case No. 1D15-5714, Fla: Dist. Court of Appeals, 1st Dist (2017).

Duty of Confidentiality

- **MRPC 1.6(a):** A lawyer shall not reveal information relating to the representation of a client.
- **MRPC 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.
- **Comment 18:** Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure...
- **ABA Formal Opinion 477R:** A lawyer should understand and use electronic security measures to safeguard client communications and information.

Duty to Safeguard

- **MRPC1.15(a):** A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property... Other property shall be identified as such and appropriately safeguarded.
- **Comment 1:** A lawyer should hold property of others with the care required of a professional fiduciary.

What are "reasonable efforts?" It depends!

- ABA Formal Opinion 477: "What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant, the methods of electronic communications employed, and the types of available security measures for each method."
- ABA Cyber Security Handbook: A "reasonable efforts" standard "rejects requirements for specific security measures...and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risk, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."

Relevant Factors for Determining “Reasonable Efforts”

- The sensitivity of the information
- Likelihood of disclosure w/o safeguards
- Cost of employing additional safeguards
- Difficulty of employing the safeguards
- The extent to which the safeguards adversely affect the lawyer's ability to effectively represent clients
- Instructions from clients (e.g., outside counsel guidelines)
- Applicable privacy laws
- Etc.

ABA's Guidance on What This Duty Means for Cybersecurity Practices

1. Understand the nature of the threats/risks
2. Understand how client confidential information is transmitted and where it is stored
3. Understand and use reasonable security measures
4. Determine how communications about client matters should be protected
5. Label client confidential information
6. Train lawyers and nonlawyers in information technology security
7. Conduct due diligence on vendors providing communication technology, accessing IT systems, or receiving sensitive data

Duty to Communicate

- **MRPC 1.4(a)(2):** A lawyer shall reasonably consult with the client about the means by which the client's objectives are to be accomplished...
- **ABA Formal Opinion 477R:** [A] lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client.

Duty to Communicate, Cont.

- **MRPC1.4(a)(3):** A lawyer must keep the client reasonably informed about the status of a matter.
- **MRPC 1.4(b):** A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representations.
- ABA says these provisions create an obligation for a lawyer to communicate with current clients about a data breach
- ABA defines a "data breach" as "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform legal services for which the lawyer is hired is significantly impaired."

Lawyers' Obligations Prior to and in the Event of a "Data Breach"

- Employ reasonable efforts to monitor for a data breach (includes breaches at vendors)
- Act reasonably and promptly to stop the breach and mitigate damage
- Investigate and determine what happened
- Promptly report the incident to affected clients who have a "reasonable possibility of being negatively impacted"
- Provide enough information that "affected clients can take steps to ameliorate the harm" and make "informed decisions"

Case Study on Duty to Report



Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Law Firm Sued By Insurance Co. For Concealing Data Hack

By Emma Cueto

Law360 (March 30, 2020, 11:58 AM EDT) -- A Kansas City personal injury firm was hit with a lawsuit by an insurance company that hired the firm to represent policyholders, with the company claiming the firm failed to protect sensitive information reportedly obtained by hacker group The Dark Overlord and did not warn either the company or clients that the information had been exposed.

Hiscox Insurance said in a complaint filed Friday that Warden Grier LLP kept it in the dark about the attack by The Dark Overlord, which is known for hacking into databases and demanding ransom to prevent the group from releasing the information it obtains.

"As per its contractual, legal, ethical, and fiduciary duties, [the law firm] was obligated to take adequate measures to protect sensitive[personal information] belonging to its clients, including Hiscox and Hiscox's insureds, and to notify Hiscox of any failure to maintain the confidentiality of PI belonging to Hiscox and its insureds," the complaint said.

Responsibility for Nonlawyer Assistance

- **MRPC 5.3(a):** [A] partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the [nonlawyer's] conduct is compatible with the professional obligations of the lawyer.
- **ABA Formal Opinion 477R:** Vendor diligence includes:
 1. *Reference checks and vendor credentials*
 2. *Review of vendor's security policies and protocols*



Practical Steps for Mitigating Risk

Vendor Management

- Adopt policies and procedures for reviewing contracts that involve access to confidential or sensitive information
- Require security protections that are commensurate with the type of information and the risks
- Account for disaster recovery and backups of data
- Ensure that security measures are employed for systems that store or transmit confidential information (e.g., require MFA where available)
- Require swift notification of any breach of security or unauthorized access of data
- Preserve the ability to routinely audit vendor practices
- Require the return or destruction of confidential information

Steps You Can Take

- Be smart with your device – use complex and long passcodes; use different passwords for your work systems than for your personal systems; be careful what websites you visit
- Avoid use of public Wi-Fi
- Only use secure or encrypted methods for communicating confidential information (e.g., don't send it to your Gmail account)
- Take extra physical protections to secure work devices
- Beware phishing attacks – even trusted contacts like your outside counsel can be spoofed!

And Require Your Outside Counsel to Do the Same...

Association of Corporate Counsel provides model information protection and security controls for outside counsel possessing company confidential information:

https://www.acc.com/sites/default/files/resources/advocacy/1454057_1.pdf



*Recap – Surprise! It's a Pop
Quiz!*

Hypothetical – Attorney A

Attorney A's laptop is stolen. Attorney A did not store confidential client information on the laptop, but only used the laptop to access such information remotely. Also, the laptop could not be accessed without biometric authentication.

Attorney A's business also installed software on the laptop that allowed it to be remotely locked down and erased.

As soon as Attorney A realizes that the laptop has been stolen, Attorney A contacts the business's IT department and receives confirmation almost immediately that the laptop has been located, locked down and wiped clean.

Hypothetical – Attorney A, Cont.

- Duty to report?
 - *Based on facts, no*
- Relevant ethical considerations?
 - *Duties of competence and confidentiality*
 - *No client information*
 - *Reasonable security*
 - *No unauthorized access*

Hypothetical – Attorney B

Attorney B loses smartphone, which he uses to email and text clients and to access applications related to clients. Smartphone only protected by 4-character password and does not have software that allows it to be remotely tracked, locked down and/or wiped clean.

Before going to bed, Attorney B remembers that Attorney left the smartphone in a tote bag at a restaurant. Attorney B immediately calls the restaurant, but it is closed. Attorney B retrieves the bag and smartphone the next morning. Manager tells Attorney, phone was locked in a cabinet overnight. Nothing appears to be missing.

Hypothetical – Attorney B, Cont.

- Duty to report?
 - *Based on facts, likely no*
- Relevant ethical considerations?
 - *No unauthorized acquisition/access*
 - *Possible issues with duty to safeguard and duty of confidentiality*
 - Weak passcode requirements for access
 - No remote wipe capability

Hypothetical – Law Firm C

Law Firm C has 4 members and specializes in corporate law. Receptionist regularly receives emails sent to the firm and routes to appropriate person. The Firm receives an email purporting to be from the Firm's IT provider. It looks genuine, so the receptionist clicks a link in the email to allow the IT provider to do routine maintenance of the Firm's server.

The Firm is infected with ransomware, which locks up computers/servers. The Firm pays the ransom demand and regains access to its data. In consultation with security experts, the Firm determines that no client information was accessed and none of the matters it handles have been negatively impacted.

Hypothetical – Law Firm C, Cont.

- Duty to report?
 - *Likely no. But if security expert could not preclude unauthorized access, disclosure would be required.*
- Relevant ethical considerations?
 - *No unauthorized acquisition/access*
 - *Possible issues with duty to safeguard, duty of confidentiality, and obligation to supervise*

Hypothetical – Attorney D

Attorney D is outside patent counsel for a life science company. On vacation, Attorney D checks work emails on a laptop over a public Wi-Fi network at a coffee shop. The laptop is not encrypted. Unbeknownst to customers, a hacker had set up a fake internet portal that resembles the one provided by the coffee shop. Attorney D accessed the fake portal.

The next day, Attorney D notices a sign at the coffee shop warning of the fake Wi-Fi. Attorney D returns to the office the following week and has the IT staff examine the laptop. The IT team concludes someone—not attorney D—accessed files on the laptop relating to the life science company's patents.

Hypothetical – Attorney D, Cont.

- Duty to report?
 - *Yes. Unauthorized access to client information was confirmed. Attorney D must report as soon as possible.*
- Relevant ethical considerations?
 - *Duty to safeguard – failure to take reasonable precautions to prevent unauthorized disclosure*
 - *Possible issues with duty of competence*

Questions?



"I guess it's ethical. Let me run it through my 'Ethics Check' app."

Cartoonist: Chris Wildt

Presenters



Megan Bowman
Attorney
612.492.7216
mbowman@fredlaw.com



Sten-Erik Hoidal
Attorney
612.492.7334
shoidal@fredlaw.com

Thank you!

Fredrikson

Where Law and Business Meet[®]