STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

AMC 2023

WALA Session 3

Cybersecurity for Law Firms:
What a Data Breach Means for Your Firm and Best Practices to Lower Risk and Mitigate Harm

Andrew J. Schlidt, Godfrey & Kahn, S.C., Milwaukee

About the Presenter...

Andrew J. Schlidt chairs the firm's Technology & Digital Business practice and is a member of its Data Privacy & Cybersecurity group. He draws on prior industry work as a technology consultant with Accenture and a Masters in Technology from Purdue. Clients trust Andy to support them in technology transactions and data strategies. He routinely negotiates a variety of technology deals, including transactions in digital transformation, data sharing, outsourcing, onshoring, cloud and XaaS platforms, strategic alliances and telecommunications (data center, broadband, fiber and wireless). Andy also provides strategic guidance on the practical application of “data law” in client environments, especially cybersecurity and privacy compliance. He serves as breach coach and counsel for clients in cyber preparedness and data breach response. Andy serves as the firm’s Privacy Officer, often advising clients in a similar capacity. He holds the Certified Information Privacy Professional/US (CIPP/US) certification from the International Association of Privacy Professionals (IAPP) and is Certified in Cybersecurity (CC) by the International Information System Security Certification Consortium (ISC)2. Andy is a legal advisor to technology companies as well as corporate users of emerging technologies. He has served on various Boards including the University of Wisconsin E-Business Consortium, Milwaukee War Memorial Center, Wisconsin Conservatory of Music, Nativity Jesuit Academy and two law firms. He is a member of ITechLaw, the International Association of Privacy Professionals, and the Federal Communications Bar Association.

Session Title: Cybersecurity for Law Firms: What a Data Breach Means for Your Firm and Best Practices to Lower Risk and Mitigate Harm

Outline Prepared By: Kate Campbell, Godfrey & Kahn

I. Current Threat Landscape
    a. Cybersecurity is important for law firms to consider
        i. Law firms are top targets
            1. They have volumes of sensitive information
            2. Threat actors know they face significant exposure and exponential loss if information is disclosed
        ii. There are legal and ethical obligations
        iii. Potential for significant losses
    b. Law firms are vulnerable to cybersecurity attacks through various vectors and by different attack types
        i. Vectors
            1. Physical security
            2. Phishing
            3. Social Engineering
            4. Vendor compromise
        ii. Attack types
            1. Ransomware
                a. Malicious software
                b. Locks down a system and files making them inaccessible unless a ransom payment is made
                c. Can be accomplished through security vulnerabilities or phishing schemes
            2. Email compromise
                a. Threat actor breaks into your email account
                b. Has access to entire inbox, can create rules to direct emails to folders so you have no idea
                c. Can send emails through your account without your knowledge
                d. Can be accomplished through security vulnerabilities or phishing schemes
            3. Wire fraud
                a. Fraudulent wire instructions are communicated to parties through a business email compromise or phishing scheme
                b. A party unknowingly sends money to a threat actor
            4. Rogue employees
        iii. Threat landscape continues to evolve
            1. Double and triple extortion

II. Legal Obligations Post-Breach

a. Breach notification laws
    i. Each state has its own data breach notification laws
    ii. The definition of personal information may vary across states
    iii. Each state will have its own standard for when notification is required
        1. Unauthorized access to personal information
        2. Unauthorized access to personal information PLUS risk of harm
    iv. Timing and the necessity to also notify the state's Attorney General varies across state laws
b. Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98
    i. Personal Information means an individual's last name and the individual's first name or first initial, <u>in combination with and linked to any of the following elements</u>, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:
        1. The individual's social security number.
        2. The individual's driver's license number or state identification number.
        3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
        4. The individual's DNA profile.
        5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.
    ii. Notice is not required if "the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."
    iii. Notice to be provided within a reasonable time, not to exceed 45 days after learning of the incident.
    iv. The Wisconsin Attorney General is not required to be notified.
c. You will need to do an analysis of every state's law in which an affected individual resides
d. You will need to consider any HIPAA obligations or outside counsel guidelines

III. Ethical Obligations for Lawyers
a. Applicable Ethical Rules
    i. SCR 20:1.1 <u>Competence</u>
        1. Edits to Model Rules in 2012 – Rule 1.1 – Obligation to "keep abreast of knowledge of the benefits and risks associated with relevant technology"
        2. "The essence of this comment is that lawyers need to understand how they use different types of technology and different types of

electronic devices to provide services to their clients and also understand the benefits and the risks of using these new technology advancements. As has been often stated, this comment does not mean that all lawyers must go back to school to obtain an electrical engineering or computer science degree, but it does mean that lawyers need to understand the different types of technology that they use to practice law." –Attorney Dean Dietrcih, *Wisconsin Lawyer Magazine*

ii. SCR 20:1.6 Confidentiality
    1. Edits to Model Rules in 2012 – Rule 1.6 – "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."

iii. SCR 20:5.1 Responsibilities of Partners, Manager, and Supervisory Lawyers

b. ABA Guidance
    i. ABA Formal Opinion 477R (Securing Communications)
        1. Lawyers have a duty to do the following related to email communications based on Model Rule 1.6(c) [which has not been adopted by Wisconsin]
            a. Understand the Nature of the Threat
            b. Understand How Client Confidential Information is Transmitted and Where It is Stored
            c. Understand and Use Reasonable Electronic Security Measures
            d. Determine How Electronic Communications About Client Matters Should be Protected
            e. Train Lawyers and Non-lawyer Assistants in Technology and Information Security
            f. Conduct Due Diligence on Vendors
    ii. ABA Formal Opinion 483 (Lawyer Obligations After a Cyber Breach or Attack)
        1. Lawyers have a duty to notify current clients of a data breach under Model Rule 1.4 "in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'"
        2. While notice is not required under the opinion to former clients, "lawyers should recognize… data privacy laws, common law duties of care, or contractual arrangements with the former client relating to records retention, may mandate notice to former clients[.]"

3. "The opinion underscores the importance for lawyers to both plan beforehand for an electronic breach or cyberattack and to understand how model rules come into play when an incident is either detected or suspected."

iii. Wisconsin Formal Ethics Opinion EF-21-02 (Working Remotely)

1. "Basic technological competence includes, at a minimum, knowledge of the types of devices available for communication, software options for communication, preparation, transmission and storage of documents and other information, and the means to keep the devices and the information they transmit and store secure and private."
2. Lacking the knowledge to manage the technological aspects of the practice is not an excuse for failing to maintain technological competence.

IV. Best Practices and Practical Pointers

a. Pre-Breach

i. Be Prepared!

1. Written Information Security Plan (WISP)
2. Incident Response Plan

ii. Tabletop Exercises

iii. Engage data security and privacy counsel

iv. Data Minimization

1. If you don't need it, don't collect it

v. Limit Access

1. Only those with a need to know should have access

vi. Emphasize Awareness

1. Employee Training

vii. Use technological measures to reduce the attack surface and mitigate common risks

1. Multi-factor authentication
2. Encryption
3. Password managers like LastPass or strong passwords that vary across accounts
4. Email security
5. Endpoint Detection and Response

viii. Conduct vendor due diligence and use strong data security contractual provisions

1. Understand the measures a vendor uses to secure and keep private sensitive information
2. It is not sufficient to conduct due diligence at the outset, and never thereafter

3. Contractual provisions relating to reasonable security measures, data breach notification, reimbursement for notification expenses, and audit rights

b. Certain cybersecurity controls are critical to obtaining coverage:
    i. Multi-factor authentication
    ii. Segmented, frequent, and encrypted backups
    iii. Prompt implementation of security patches/updates
    iv. Endpoint Detection and Response Tools
    v. Have a strong cybersecurity program in place and be knowledgeable about the security in place.
    vi. Be thorough and truthful on your insurance application.
c. Post-Breach
    i. Follow Incident Response Plan
    ii. Take Action to Mitigate Harm if Possible
    iii. Contact Insurer
    iv. Contact Counsel
    v. Consider Attorney Client Protections when Working with Forensic Provider

Cybersecurity for Law Firms

What a Data Breach Means for Your Firm and Best Practices to Lower Risk and Mitigate Harm

Andrew J. Schlidt III | CIPP/US, CC

June 14, 2023

GODFREY & KAHN S.C.

MILWAUKEE | MADISON | GREEN BAY | APPLETON | WASHINGTON, D.C.

1

Today's Agenda

- The Current Threat Landscape
- Legal Obligations Post-Breach
- Ethical Obligations for Lawyers
- Best Practices and Practical Pointers

GODFREY & KAHN S.C.

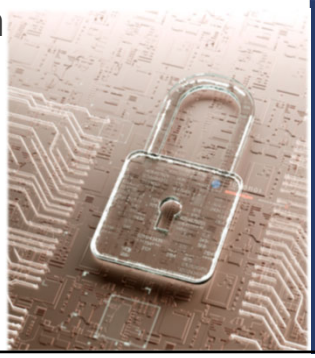
2

The Current Threat Landscape

3

Why Should Lawyers Care?

- Law firms are attractive targets
- Significant exposure and exponential losses
- Volumes of sensitive information
- Ethical and legal obligations



GODFREY & KAHN S.C.

4

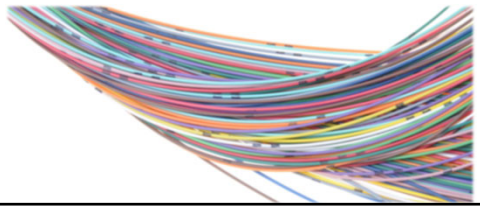
Law Firms are Vulnerable

Attack Vectors

- Physical Security
- Phishing
- Social Engineering
- Vendor Compromise

Attack Types

- Ransomware
- Email Compromise
- Wire Fraud
- Rogue employees



GODFREY KAHN S.C.

5

Ransomware

- Malicious software
- Locks down a system and files making them inaccessible unless a ransom payment is made
- Can be accomplished through security vulnerabilities or phishing schemes

GODFREY KAHN S.C.

6

Business Email Compromise

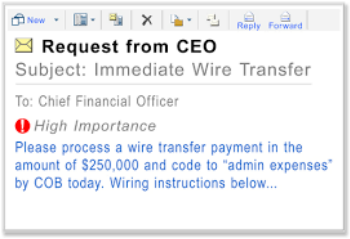
- Threat actor breaks into your email account
- Has access to entire inbox, can create rules to direct emails to folders so you have no idea
- Can send emails through your account without your knowledge
- Can be accomplished through security vulnerabilities or phishing schemes

GODFREY KAHN S.C.

7

Wire Fraud

- Fraudulent wire instructions are communicated to parties through a business email compromise or phishing scheme
- A party unknowingly sends money to a threat actor



GODFREY KAHN S.C.

8

Evolving Threat Landscape

- Law firms are especially susceptible to double and triple extortion models
- Emerging trends show law firms as top targets

GODFREY KAHN S.C.

9

Key Statistics (2016-2020)

- Average Incident Cost for Professional Services Companies: $211,000
- Most Frequent Claims (SMEs)
  1. Ransomware (~1500, $179,000 avg)
  2. Hacker (~450, $430,000 avg)
  3. BEC (~400, $123,000 avg)
  4. Phishing (~275, $13,000 avg)
  5. Human Error (~250, $72,000 avg)

Source: 2021 NetDiligence Cyber Claims Report

GODFREY KAHN S.C.

10

Legal Obligations for Lawyers

11

Breach Notification Laws

- Each state has its own data breach notification laws
- The definition of personal information may vary across states
- Each state will have its own standard for when notification is required
  - Unauthorized access to personal information
  - Unauthorized access to personal information PLUS risk of harm
- Timing and the necessity to also notify the state's Attorney General varies across state laws

GODFREY KAHN S.C.

12

Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98

- Personal Information means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:
  - The individual's social security number.
  - The individual's driver's license number or state identification number.
  - The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
  - The individual's DNA profile.
  - The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

GODFREY KAHN S.C.

13

Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98

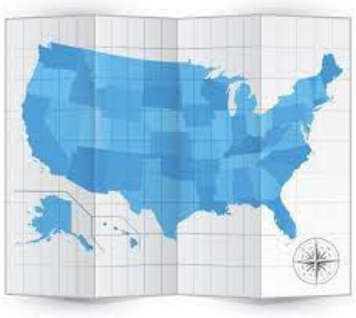
- Notice is not required if "the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."
- Notice to be provided within a reasonable time, not to exceed 45 days after learning of the incident.
- The Wisconsin Attorney General is not required to be notified.

GODFREY KAHN S.C.

14

Breach Notification Laws

- You will need to do an analysis of every state's law in which an affected individual resides



GODFREY KAHN S.C.

15

Other Required Notifications Common for Lawyers

HIPAA IF YOUR FIRM ACTS AS A BUSINESS ASSOCIATE

OUTSIDE COUNSEL GUIDELINES

GODFREY KAHN S.C.

16

Ethical Obligations for Lawyers

17

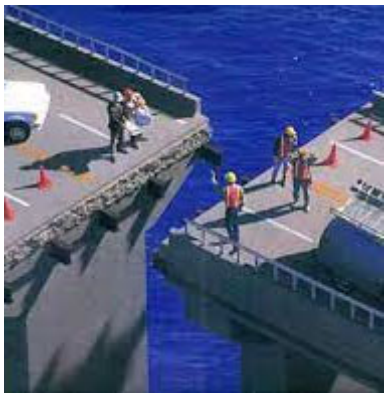
Ethical Rules

- SCR 20:1.1 Competence
  - Edits to Model Rules in 2012 – Rule 1.1 – Obligation to "keep abreast of knowledge of the benefits and risks associated with relevant technology"
- SCR 20:1.6 Confidentiality
  - Edits to Model Rules in 2012 – Rule 1.6 – "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."
- SCR 20:5.1 Responsibilities of Partners, Manager, and Supervisory Lawyers

GODFREY KAHN S.C.

18

SCR 20:1.1 Competence



- "The essence of this comment is that lawyers need to understand how they use different types of technology and different types of electronic devices to provide services to their clients and also understand the benefits and the risks of using these new technology advancements.

- As has been often stated, this comment does not mean that all lawyers must go back to school to obtain an electrical engineering or computer science degree, but it does mean that lawyers need to understand the different types of technology that they use to practice law."

  —Attorney Dean Dietrich, in *Wisconsin Lawyer* magazine, July 2017

GODFREY KAHN S.C.

19

ABA Guidance

- ABA Formal Opinion 477R (Securing Communications)
- ABA Formal Opinion 483 (Lawyer Obligations After a Cyber Breach or Attack)
- Wisconsin Formal Ethics Opinion EF-21-02 (Working Remotely)

GODFREY KAHN S.C.

20

ABA Formal Opinion 477R

- Lawyers have a duty to do the following related to email communications based on Model Rule 1.6(c) [which has not been adopted by Wisconsin]
  - Understand the Nature of the Threat
  - Understand How Client Confidential Information is Transmitted and Where It is Stored
  - Understand and Use Reasonable Electronic Security Measures
  - Determine How Electronic Communications About Client Matters Should be Protected
  - Train Lawyers and Non-lawyer Assistants in Technology and Information Security
  - Conduct Due Diligence on Vendors

GODFREY KAHN S.C.

21

ABA Formal Opinion 483

- Lawyers have a duty to notify current clients of a data breach under Model Rule 1.4 "in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'"
- While notice is not required under the opinion to former clients, "lawyers should recognize… data privacy laws, common law duties of care, or contractual arrangements with the former client relating to records retention, may mandate notice to former clients[.]"

GODFREY KAHN S.C.

22

ABA Formal Opinion 483

- "The opinion underscores the importance for lawyers to both plan beforehand for an electronic breach or cyberattack and to understand how model rules come into play when an incident is either detected or suspected."

—ABA Issues New Guidance on Lawyer Obligations After a Cyber Breach or Attack, ABA (Oct. 17, 2018), *available at* https://www.americanbar.org/news/abanews/aba-news-archives/2018/10/aba-issues-new-guidance-on-lawyer-obligations-after-a-cyber-brea/.

GODFREY KAHN S.C.

23

Wisconsin Formal Ethics Opinion EF-21-02

- "Basic technological competence includes, at a minimum, knowledge of the types of devices available for communication, software options for communication, preparation, transmission and storage of documents and other information, and the means to keep the devices and the information they transmit and store secure and private."

- Lacking the knowledge to manage the technological aspects of the practice is not an excuse for failing to maintain technological competence.

GODFREY KAHN S.C.

24

Best Practices and Practical Pointers

25

Best Practices Pre-Breach

- Be Prepared!
  - Written Information Security Plan (WISP)
  - Incident Response Plan
    - Tabletop Exercises
  - Engage data security and privacy counsel

GODFREY & KAHN S.C.

26

Best Practices Pre-Breach

- Data Minimization
  - If you don't need it, don't collect it
- Limit Access
  - Only those with a need to know should have access
- Emphasize Awareness
  - Employee Training

GODFREY KAHN S.C.

27

Best Practices Pre-Breach

- Use technological measures to reduce the attack surface and mitigate common risks
  - Multi-factor authentication
  - Encryption
  - Password managers like LastPass or strong passwords that vary across accounts
  - Email security
  - Endpoint Detection and Response

GODFREY KAHN S.C.

28

Best Practices Pre-Breach

- Conduct vendor due diligence and use strong data security contractual provisions
  - Understand the measures a vendor uses to secure and keep private sensitive information
  - It is not sufficient to conduct due diligence at the outset, and never thereafter
  - Contractual provisions relating to reasonable security measures, data breach notification, reimbursement for notification expenses, and audit rights

GODFREY KAHN S.C.

29

Cyberinsurance Tips

- Certain cybersecurity controls are critical to obtaining coverage:
  - Multi-factor authentication
  - Segmented, frequent, and encrypted backups
  - Prompt implementation of security patches/updates
  - Endpoint Detection and Response Tools
- Have a strong cybersecurity program in place and be knowledgeable about the security in place.
- Be thorough and truthful on your insurance application.

GODFREY KAHN S.C.

30

Best Practices Post-Breach

- Follow Incident Response Plan
- Take Action to Mitigate Harm if Possible
- Contact Insurer
- Contact Counsel
- Consider Attorney Client Protections when Working with Forensic Provider

GODFREY&KAHN S.C.

31

Thank You.

Andrew J. Schlidt III

414.287.9624

aschlidt@gklaw.com

G&K

32