What Estate Planning Professionals Need to Know About Cybersecurity in the Era of COVID-19

NAEPC Webinar
July 8, 2020

LEWIS THOMASON
KNOXVILLE | MEMPHIS | NASHVILLE

Justin Joy, CIPP/US, CIPT

JJoy@LewisThomason.com

- What are some of the cybersecurity threats confronting estate planning professionals?
- What are your legal obligations and risks in the context of data security?
- What are some growing cyber risk trends related to the COVID-19 pandemic?
- What are some (non-technical) strategies for reducing this legal risk?

LEWIS THOMASON

Cybersecurity threats vs. planning professionals

- Business email compromise
  - Fraudulent email apparently from a person of authority is sent to a targeted employee
  - Usually requests an immediate wire transfer or change in payment instructions
  - Exploits trusted relationships
  - FBI: “Losses are in the billions of dollars and climbing . . . the level of sophistication in this multifaceted global fraud is unprecedented.”

LEWIS THOMASON

Cybersecurity threats vs. planning professionals

- Ransomware attacks ("data hostage events")
  - Malicious software infects systems
  - Demands money paid in exchange for "returning" data
  - Data remains unusable (encrypted) or is destroyed if payment is not made
  - Increasingly, hackers are (also) stealing data from systems and threatening to disclose data if ransom not paid

LEWIS THOMASON

Some general data security legal obligations

- Data security incident
  - May or may not involve actual compromise of data
  - NIST: "is a violation ***or imminent threat of violation*** of computer security policies, acceptable use policies, or standard security practices"

LEWIS THOMASON

Cyber security threats and business exposure to data breaches

- Data breach
  - Defined by state law for most industries
  - In Tennessee:

  "the acquisition of [(i) unencrypted computerized data or (ii) encrypted computerized data and the encryption key] by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder"

Tenn. Code Ann. § 47-18-2107

LEWIS THOMASON

Reducing the risk

- Lack of data security procedures and training is a primary threat to businesses
- Who is the designated individual at your firm or company responsible for privacy and data security procedure development and training?

LEWIS THOMASON

Reducing the risk

- Vendor management
  - Determine the minimum level of access a vendor needs
  - Have agreements in place with any vendor with access to your firm's data
  - Consider what level of diligence needs to be completed before and during the vendor engagement
  - Understand what data your vendors has and how long they keep it

LEWIS THOMASON

Reducing the risk

- Vendors
  - Check current agreements
  - Review prospective agreements and negotiate when possible
  - Re-evaluate over time

LEWIS THOMASON

Reducing the risk

- Working from home
  - Help keep cybersecurity top-of-mind for employees working remotely
  - Provide alerts for known email-based threats
  - Re-visit payment request authentication procedures
  - Use multifactor authentication (MFA) where available

LEWIS THOMASON

Reducing the risk

- First party coverage
- Third party coverage
- What do you need covered?

LEWIS THOMASON

Reducing the risk

- Examples of first party coverages
  - Forensic investigation
  - Breach notification (mail vendor)
  - Call center
  - Credit monitoring
  - Extortion
  - Business interruption
  - Legal counsel

LEWIS THOMASON

Reducing the risk

- Examples of third party coverages
  - Claims made against your company
  - Litigation defense and settlement costs
  - Government investigation defense

LEWIS THOMASON

Reducing the risk

- What do you need covered?
  - How many workstations do you have?
  - How many servers do you have?
  - What devices are encrypted?
  - How many records containing PII do you have?
  - How long does it take you to restore from a backup?
  - Fraud coverage?
  - Network intrusion / hacking coverage?

LEWIS THOMASON

Reducing the risk

- Workforce awareness
  - Develop a written data security program and keep it updated
  - Familiarize employees on your policies and procedures
  - Conduct regular security awareness training based on those procedures

LEWIS THOMASON

Reducing the risk

- What is your firm/company legally required to do in the event of a data breach?
- What is your firm/company legally required to do in the event of a data security incident?
- Attorney-client privilege protection for investigation

LEWIS THOMASON

Reducing the risk

- How did hackers get in?
- What did they do (or get) when they get in?
- How long did the data breach last?

LEWIS THOMASON

Reducing the risk

- Notification obligations
  - Individuals
    - Current/former employees
    - Customers
    - Others?
  - Government agencies/AG offices
  - Media
- Other response considerations
  - Credit monitoring
  - Handling questions

LEWIS THOMASON

Reducing the risk

- BEC response plan
- Ransom payment considerations

LEWIS THOMASON

Reducing the risk

- Be breach ready
  - Know who to call in the event of a data security incident
  - Have a written breach response plan in place
  - Regularly review response plan and revise as needed
  - Check insurance coverage available for different types of cyber-related losses

LEWIS THOMASON