Cybersecurity: What Estate Planners Should Tell Clients

By: Brian Cluxton, Martin M. Shenkman, and Thomas A. Tietz

Some Webinar Pointers

- All programs hosted by Shenkman Law are free and we focus on providing colleagues with practical and actionable planning ideas. Our goal is to help you, our colleagues, with your practice.
- The PowerPoint is available for download from the web console during the program.
- A recording of this program and the materials will be posted to www.shenkmanlaw.com/webinars within about a week of the program. There is a growing library of 150+ webinar recordings there.
- There is a growing library of 200+ video planning clips on www.laweasy.com.
- There is no CLE or CPE for this program, but the webinar system will send you a certificate of attendance. We cannot control those certificates, so if there is an issue, we cannot assist.
- If you have questions, please email the panel. All emails are listed near the end of the slide deck.

General Disclaimer

- The information and/or the materials provided as part of this program are intended and provided solely for informational and educational purposes. None of the information and/or materials provided as part of this PowerPoint or ancillary materials are intended to be, nor should they be construed to be, the basis of any investment, legal, tax, or other professional advice. Under no circumstances should the audio, PowerPoint, or other materials be considered to be, or used as independent legal, tax, investment, or other professional advice. The discussions are general in nature and not person-specific. Laws vary by state and are subject to constant change. Economic developments could dramatically alter the illustrations or recommendations offered in the program or materials.

Introduction

Elder Financial Abuse Dwarfs Estate Tax

Elder Financial Abuse Dwarfs Estate Tax

- In one year ending June 2023, the Financial Crimes Enforcement Network (FinCEN) found that about $27 billion in reported suspicious activity was linked to elder financial exploitation.
- In 2022, approximately $22 billion was collected from the Federal Estate Tax.
- Consider the emphasis the profession places on saving estate tax vs. elder abuse, identity theft, and similar losses.

Evolving Emphasis of Planning

- Practitioners may consider evolving the emphasis of their practice as the world changes.
- Tech conversations at some point might be part of the conversation about security, asset protection and elder planning.

Practitioner's Cybersecurity

Assessing your own protections

Are Practitioners The Barefoot Shoemaker?

- An ABA report in 2023 found one in four lawyers reported that their firm had a cybersecurity breach in 2022.
- Practitioners may have state-of-the-art security at their firm, but wholly inadequate personal document and cyber security.

Adding Cybersecurity to the Discussion

Points to Consider When Meeting with Clients

Clients are Targets of Bad Actors

- FBI annual report on cyber crime found between 2019 and 2023 growth of nearly double the complaints, and more than triple the losses per year.
- Bad Actors look for weak links, such as older individuals.
- Elder abuse and identity theft can create a huge disruption in client's lives.

Firm Procedures to Consider Implementing

- Develop policies and practices to protect aging or infirm clients. **Example**: If a client sends confidential data unencrypted, have a policy for someone to follow up and email them about the risks.
- Train staff to recognize elder financial exploitation. Consider procurement concerns.
- Obtain information for a trusted contact and discuss when to contact.
- Report/respond to suspected elder financial abuse as permitted by law and ethical requirements.
- Educate clients as to steps they may consider to reduce the risk of financial exploitation.

Digitizing Physical Documents

- Many older clients store old bank and brokerage statements, tax returns and other sensitive paper documents.
- Are they secured against pilfering, such as by a health aide or repair person?
- Severe weather events, flooding, fire, etc. also pose a risk.
- Guide clients on going “paperless,” scanning, storing in a secure cloud-based portal, and then destroying physical originals of documents.
- This can also assist clients with downsizing as they age.

Choosing a Vendor for Digitization

- Clients may consider the following criteria when choosing a vendor to assist in scanning documents.
- The vendor should comply with relevant industry regulations and standards.
- Inquire about the security measures the vendor has in place.
- How does the vendor maintain a secure chain of custody for documents from retrieval, to scanning, to destruction?

Advise Clients of Risks with Electronic Communications

- Clients often transmit sensitive information to the practitioner via email.
- Even if a practitioner has state-of-the-art cyber-security, if the client has inadequate protections, the data could be compromised on the client's end.
- Highlighting some key issues might educate a client enough that they take appropriate measures.

Electronic Security Talking Points

- Secure Portal- for documents and communication.
- Using old email systems, i.e., Hotmail, AOL, etc. vs newer systems, such as gmail, outlook, etc.
- Free vs Paid email systems.
- Proactively encrypting emails.
- Using different business and personal emails.
- Lead by example- use your programs.

Clients Avoid Safeguards due to Complexity

- Even if the practitioner has secure options in place, clients may not use protections they are unfamiliar with.
- Consider offering “cheat sheets,” or instruction manuals.
- Short video clips and information could be posted to the firm website.
- Provide clients with a “quick facts” spreadsheet of statistics on cyber crime to help them understand the severity of the threat.

Software

Programs for Clients to Consider

General Points

- Practitioners should not and need not fill the role of IT consultant.
- However, many clients simply do not retain personal IT consultants and do not take adequate protective measures.
- Discussions that build general awareness can be seen as a value add by clients.
- Practitioners can use regular firm newsletters and other communications to educate clients about cybersecurity risks.

Anti-Virus Software

- Anti-virus software is essential.
- The free versions of anti-virus that typically come with new computers may not be sufficient.

Phishing Filtering

- What is Phishing?
- AI makes Phishing more advanced and dangerous.
- Examples of phishing might include- fake invoices, email from an attorney with documents for the recipient, etc.

Additional Scams to be Aware of

- QR-ishing.
- Smishing.
- Vishing.
- Social Engineering.

End-Point Detection Response Software

- This is next-generation anti-virus software.
- It monitors data flow and can shut down internet access if a potential issue is found.
- This helps prevent “Zero day” virus infections.
- Examples include: SentinelOne Singularity, CrowdStrike Falcon, Sophos Intercept X, Trend Vision One.

Password Managers

- A recent study found that 78% of people reuse the same password across multiple accounts.
- Having a system that remembers passwords lets you use stronger and more randomized passwords.
- Consider separate business and personal password managers.

Multi-Factor Authentication (MFA)

- Passwords, even strong complex ones generated by a password manager, are often not sufficient to rely on alone to secure an account.
- MFA provides an additional layer of security.
- MFA can be done through email, text message (“SMS”), or an authenticator app on the client’s cellphone.

Data Backup

Protecting Against Calamities

Protecting Physical Documents Still Needed

- While many documents may be able to be digitized, originals may still be needed of certain documents, such as wills, deeds, etc.
- With less physical documents, is a full-sized fireproof safe still needed?
- Consider fireproof envelopes to store originals that cannot be destroyed.

Need for Data Backup

- A survey in 2023 found that 11% of computer owners backed up their data daily, 8% weekly, and 15% monthly. 18% of computer owners said they've never backed up their data.
- Extreme weather events can destroy a laptop in addition to paper documents.

What Kind of Data Backup?

- Physical hard drive backups susceptible to extreme weather events same as other media.
- Cloud Back-up provides layers of protection but needs internet connection to access.
- Active cloud-based system vs. snapshot backups.
- Employ multiple kinds of backup systems.

Consistency

- Many individuals have numerous cloud backups: Apple for iPhone, OneDrive for Microsoft, Dropbox for personal, etc.
- What if client is incapacitated? Recommend clients document what systems they use and where data is stored.

Testing Backups

- Often someone finds out their backup failed when they need it.
- Occasionally someone, whether the clients, an IT consultant, or other professionals or family members, should test backups.
- Create documentation on how data can be restored so it is easy to follow in a stressful situation.

Routers and Firewalls

Protecting Networks

Weakest Link

- Firewalls are often used by businesses, but many clients neglect to implement them personally.
- If a business laptop is brought home, it could potentially be compromised by other computers on the network.
- Does the client's children's laptops have the same protections? Bad actors look for the weakest link.

Wardiving

- There have been bad actors that have hacked routers in residential neighborhoods. They can drive around the neighborhood and attempt to connect to the network from outside the client's home.
- Basic modem/router provided by an internet service provider may not be enough.

“Smart” Appliances

- Many Home appliances are connected to the internet through a home network.
- TVs, refrigerators, ring doorbells, even cat litter boxes!
- Change default passwords on devices.
- Update firmware.
- An aftermarket firewall may protect all of these devices.

Organizing Digital Information

More of Life is Online

Addressing Incapacity or Death

- Discuss with clients whether they have considered what will happen to their online assets when they pass.
- How will beneficiaries access the assets?
- Collect critical cyber information and include it with other emergency information in documents for fiduciaries or heirs.
- Password managers would assist with transmission of information.

Conclusion and Additional Information

Constant Evolution

Conclusion

- There is constant evolution in the technology used in home computer and other IT systems.
- Criminal methods are also consistently evolving, developing new methods of attack.
- Practitioners might recommend that clients have an IT professional complete a periodic assessment of their cybersecurity measures.

Additional information

- Brian Cluxton
  Brian@cluxtonIT.com
- Martin M. Shenkman
  Shenkman@shenkmanlaw.com
- Thomas A. Tietz
  Tietz@shenkmanlaw.com

A KEY ESTATE PLANNING GUIDE
Law Easy
ChronicIllnessPlanning.org