Tech Traps and Tips Every Practitioner Must Know Now that You've Tackled Remote Working

Handout materials are available for download or printing on the HANDOUT TAB on the gotowebinar console. If the tab is not open click on that tab to open it and view the materials.

PEAK TRUST COMPANY
Elevated Trust & Wealth Management Solutions

InterActive Legal

A KEY ESTATE PLANNING GUIDE

ChronicIllnessPlanning.org

Tech Traps and Tips Every Practitioner Must Know Now that You've Tackled Remote Working

By: Peter Fidler, Mary Vandenack, Jonathan G. Blattmachr and Martin M. Shenkman

PEAK TRUST COMPANY
Elevated Trust & Wealth Management Solutions

InterActive Legal

A KEY ESTATE PLANNING GUIDE

Law Easy

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 power point 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, power point 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.

Some Webinar Pointers

- 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. There is a growing library of 50+ webinar recordings there.
- There is a growing library of 150+ video planning clips on www.laweasy.com.
- There is no CLE or CPE for this program, but you will be sent a certificate of attendance from the webinar system. 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 on near the end of the slide deck.

Thank you to our sponsors

- InterActive Legal
  - Vanessa Kanaga
  - (321) 252-0100
  - sales@interactivelegal.com

InterActive Legal

Thank you to our sponsors

- Peak Trust Company
  - Brandon Cintula
  - (888) 544-6775
  - bcintula@peaktrust.com

PEAK TRUST COMPANY
Elevated Trust & Wealth Management Solutions

AANE helps people with Asperger's or similar autism spectrum and neurodiverse profiles build meaningful, connected lives. We provide individuals, families, and professionals with information, education, community, support, and advocacy — all in an inclusive atmosphere of validation and respect.

For more information, please visit us at **www.aane.org**.

Support Local Heroes

- Be Active In Your Community to Support responders, health care workers, or local businesses.
- Perhaps you represent an assisted living facility and can help provide health care directives to workers.

What happens when hundreds of thousands of workers return to their offices?

- Unsafe practices, adopted during remote work, are brought back to the office (Dropbox, email attachments, thumb drives, video/music streaming, etc.).
- Machines possibly infected off-site (laptops, etc.) are now connected directly to the corporate network.
- “Band-aid fixes” (P2P file sharing, etc.) used in place of secure solutions.
- Workers accustomed to solving own issues neglect to discuss their needs with IT Dept. or outside consultant.

Going Remote Changed The Security Equation

- In Person Offices typically have monitored keycard access, video surveillance, and logs of those coming and going.
- In Person Offices typically have network drives, network printers, and shredders.
- In Person offices have conference rooms for face to face meetings.
- Going remote changed the security equation and requires consideration whether remaining remote, going back into the office or some combination.

A New Strain on the IT Department

- Research indicates that as much as 50% of an organization's IT expenditure comes from teams, groups, and business units purchasing and using technology without the IT Department's knowledge.
- 63% of employees admit to sending work documents to their personal email account in order to access those documents when working from home.
- One-third of successful attacks experienced by businesses will be against their Shadow IT resources.
- 80% of workers admit to using SaaS (software-as-a-service) products of their own choosing on the corporate network.

Potential Impact On The Business

- Introduction of viruses/malware/intruders/ransomware/backdoors.
- Significant threat of downtime.
- Reduced worker efficiency/productivity/motivation.
- Significant risk of liability (threat to intellectual property, compliance issues, loss of trust).
- Potential Violations of Professional Ethical Rules.

Why Do Employees Use Shadow It?

- Employee finds a preferred file sharing application and starts using that.
- Employee finds a cloud-based application such as slack or dropbox.
- Employee finds it easier and more efficient to use home computer system than office laptop.
- It is sometimes easier to email documents to personal device.

Risks of Shadow IT

- If IT isn't aware of an application, they can't support it nor ensure security.
- Shadow IT creates security risks. (up to 1/3 of breaches)
- Redundant but different applications can increase costs.
- Theft.
- Common Shadow IT: Dropbox, Google Docs, Slack, Skype, Personal Laptop, Smartphones.
- Consider that Shadow IT can also be an opportunity to leverage by finding applications that will improve the organization.

How to prepare for a return to the physical office

- Interview returning workers (listen for habits acquired during remote work; “fixes” adopted by the user).
- Review internal IT security practices (password policy, prohibited activities, hiring/firing protocol).
- Solicit ideas for the IT Department from workers.
- Ensure regular, ongoing IT planning!

Managing Shadow IT Devices

- Organizations can learn a lot from examining the Shadow IT devices and applications that its workers are embracing.
- Identify areas where the needs of the worker are not being well met by management .
- The organization has an opportunity to provision IT tools that both meet the workers' needs and conform to proper business compliance standards.
- Communication – when the IT Department is made aware of everyone's needs, it can play the role it is meant to play within an organization: aligning the needs of the business with the safest, most secure technology available.

Use Lessons Learned to Plan Going Forward - What If you Go Remote Again?

- Should firm go to docking stations and laptops?
- Embrace Innovation
  - But control risks and prevent security breaches.
- Reconsider what firm should provide.
- Review policies.
- Educate to encourage safe, effective, connected use.
- Engage employees.
- Third party tools are available to provide monitoring of shadow IT risk areas.

Law Firm Breaches Have Been Growing

- Before the pandemic, a Legal Technology Report indicated that 26% of law firms reported breaches.
- Law firms should have written policies (and enforcement and accountability) regarding documents, computer use, remote access, social media, use of personal technology and employee privacy.
- Lawyers and staff must be trained on the policies annually.
- As we either return, or continue to work remotely, an opportunity is created to review policies and practices and adopt and implement improvements.
- 1/3 of breaches are from Shadow IT devices.

Basic Security

- All patches and updates should be installed as available.
- Endpoint protection (security software).
- Mobile Device Management.
- Know what you have in terms of equipment, applications, backup and keep updated.
- Policies and processes.
- Education and re-education.

Office 365 Security

- Require multi factor authentication for administrator accounts.
- Require multi factor authentication for user accounts.
- Conditional access should be implemented (can shut down access from certain countries).
- Turn on Auditing and Utilize and monitor those Logs.
- Enable alerts for possible unauthorized activity.
- Keep track of all devices on which 365 is downloaded.
- Turn of Office 365 features to alert users on email for the outside and addressing external contact.

Passwords

- Home wifi passwords should be lengthy. 8-character passwords can be cracked in 2.5 hours. Have a separate wifi password (SSID) for business.
- Firms should have policies with password requirements for firm employees to use home wifi.
- Password Managers (like LastPass or 1Password).

Two Factor Authentication

- Security breaches have increased during COVID. Hackers are not taking a break but rather taking advantage (Be careful on what you post to social media).
- Two Factor Authentication involves a second way to verify yourself.
- Two of: Something you know (password); something you have (hardware); something you are (fingerprint).

Physical Papers

- For offices with physical paper, most of such paper was typically kept in the office. In the remote environment, paper might be taken home or printed on a home printer.
- What strategies should law firms have in place to deal with paper printed and left at home? What happens if a remote employee quits?
- NOW IS THE TIME TO FINALLY GO PAPERLESS! If you are in the office, do it before you go remote again.

Hardware Inventory

- The remote work environment may have resulted in equipment being loaned by the law firm for home offices.
- Keep accurate records of all loaned equipment.
- Account for the equipment upon return.
- Remotely manage those devices (for updates and viruses).

High Speed Internet for the Remote Office

- With multiple people working at home at the same time, internet speeds may need to be adjusted.
- Segment your home network (if possible, get a separate internet line).
- Download and upload speeds may vary. (Often, download speed is faster than upload.).
- Issue arises when trying to be on a videoconference. Zoom requires 2mbps to share a screen.
- Satellite internet is problematic with videoconferencing. (Let someone else screen share.)

Considerations When Personal Computers Used For Work

- Encrypted Backup.
- Full Disk Encryption – guards against theft of laptop.
- Up to Date Virus Software – protect the integrity of personal computers.
- Best practice is that laptop should be used to log in to firm system on cloud or firm server (no personal work).

Firm Laptops

- Some firms have transitioned to docking stations and laptops. If a firm has returned to the office but again needs to go remote, law firm employees can take the firm laptop home.
- Sending a firm laptop, owned by the firm, allows the firm to dictate what happens with the laptop.
- Require passwords to unlock after a period of inactivity. Include remote access software.

Web Conferencing Software

- Keep software up to date.
- Use the web conferencing software security features such as waiting rooms and passwords.
- Use different links for every meeting.

Security Assessments

- Engage a cybersecurity firm. There are firms that fit all sizes of firms and budgets. Firm used should have true cybersecurity certifications.
- Goal of audit is to identify security vulnerabilities and develop protective policies.
- Cybersecurity firm perform 2nd audit after remediation of the vulnerabilities and security gaps.

Implementation of Policies Requires Training

- Phishing emails successfully target law firms.
- Perform phishing simulations.
- Training should be on a regular basis.
- Updates should be given on current scams and statistics on those who click on the link.

Ethical Duties To Consider
See Pennsylvania Bar Opinion 2020-300

- All communications, including telephone calls, text messages, email, and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information;
- Information transmitted through the Internet is done in a manner that ensures the confidentiality of client communications and other sensitive data;
- Their remote workspaces are designed to prevent the disclosure of confidential information in both paper and electronic form;
- Proper procedures are used to secure, and backup confidential data stored on electronic devices and in the cloud;
- Any remotely working staff are educated about and have the resources to make their work compliant with the Rules of Professional Conduct; and,
- Appropriate forms of data security are used.

Business Development At A Distance

- Stay In Touch With Current Clients – Keep Them Updated.
- Create a COVID-19 update page.
- Provide personalized updates to clients on issues that impact them.
- Provide regular updates on law firm status.
- Consider effective connection strategies that make sense for you.
- Clients are spending more time online. Be present.
- Online Communities.
- Host an Online Virtual Networking Event.
- Participate in Virtual Conferences.

Conclusion and Additional Information

Addressing Tech Security and other Issues is Vital

Conclusion

- Panel will give last thoughts

Additional information

- Peter Fidler WCA Technologies

pfidler@wcatech.com

- Mary Vandenack mvandenack@vwattys.com

Additional information

- Jonathan G. Blattmachr
  jblattmachr@hotmail.com
- Martin M. Shenkman
  shenkman@shenkmanlaw.com
- Interactive Legal sales@interactivelegal.com
- Peak Trust Company
  bcintula@peaktrust.com

CLE Credits

- For more information about earning CLE credit for this program or other Martin Shenkman programs please contact Simcha Dornbush at NACLE. 212-776-4943 Ext. 110 or email sdornbush@nacle.com