8 Defenses to Defuse the Ticking Time Bombs in Your Professional Practice

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

8 Defenses to Defuse the Ticking Time Bombs in Your Professional Practice

How to Protect Your Client Data from Hackers, Malware, Ransomware and Other Digital Threats

By: Tom Lambotte and Martin M. Shenkman

PEAK TRUST COMPANY
Elevated Trust & Wealth Management Solutions

InterActive Legal

A KEY ESTATE PLANNING GUIDE

Law Easy

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.

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.

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
  - Nichole King
  - Phone: 702.462.6677
  - Toll Free: 844.391.2789
  - NKing@peaktrust.com

PEAK TRUST COMPANY
Elevated Trust & Wealth Management Solutions

Tom Lambotte is the CEO & Founder of 2 companies serving the legal vertical:

A nationwide full-service managed service provider that helps high-growth law firms who exclusively use Mac-based technology.

GlobalMac IT
We Evaluate | We Help | We Maximize

A cybersecurity suite built specifically to meet the needs of solo lawyers and small to mid-size law firms, whether they use Macs or PCs.

BobaGuard
TURNKEY CYBERSECURITY SUITE

Some Ethics Background For Lawyers Lawyers on IT Considerations

Concepts Can be Applied to Other Disciplines as Well

PEAK TRUST COMPANY
Elevated Trust & Wealth Management Solutions

InterActive Legal

A KEY ESTATE PLANNING GUIDE

Law Easy

Communication – RPC 1.4

- A lawyer shall fully inform a prospective client of how, when and where the client may communicate with the lawyer.
- A lawyer shall keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information.
- Tech can provide a myriad of ways to meet these RPCs (all of which are just good practice and probably safer practice). Following is a listing, detailed examples are provided later:
  - Use your firm website to indicate how a client may communicate.
  - Use initial form letters to prospective clients to outline policies.
  - Include communication considerations in retainer agreement.
  - Use real time entries into billing system to communicate status to clients.
  - Use newsletters and other electronic communications to keep clients informed.
  - Add footers to bills with important info.

Ethics Opinion 477

- Ethics Opinion 477 updates Ethics Opinion 99-413 to reflect the now common use of tech such as tablet devices, smartphones, and cloud storage.
- Each device and each storage location offers an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties under Rule 1.1 of the ABA Model Rules concerning competency, confidentiality, and communication.
- Comment 8: Modified recently to include that lawyers should keep abreast of changes in the law and its practice "including the benefits and risks associated with relevant technology.
  - Simple solution: have your IT consultant prepare annually a summary of improvements made and steps to take. Use this letter to document that you are keeping current and addressing new threats and issues.
- Lawyers must take reasonable efforts to ensure that communications with clients are secure and not subject to inadvertent or unauthorized security breaches.

Ethics Opinion 477 (Cont'd)

- Lawyers must use "reasonable efforts" to ensure the security of client information. Citing the ABA Cybersecurity Handbook, the opinion explains that the reasonable efforts standard is a fact-specific inquiry that requires examining the sensitivity of the information, the risk of disclosure without additional precautions, the cost of additional measures, the difficulty of adding more safeguards, and whether additional safeguards adversely impact the lawyer's ability to represent the client.
  - What is "reasonable" is a gray area. As a result, practitioners should have their IT consultant prepare an annual letter, as suggested above, to review matters in the office and suggest improvements. Then be certain to follow up on the improvements recommended to assure implementation. A process of periodic review and follow up documented in this manner may provide corroboration that the practitioner has acted with "reasonable efforts."
- The opinion notes that generally lawyers may use unencrypted email when communicating routinely with clients.

Ethics Opinion 477 (Cont'd)

- Opinion 477 included several aspects to consider when sending unencrypted emails:
  - 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 clients should be protected.
  - Label client confidential information. This should include digital files.
  - Train lawyers and non-lawyer assistants in technology and information security.
  - Conduct due diligence on vendors providing communication technology.

IRS Publication 4557 Safeguarding Taxpayer Data: A Guide For Your Business

Tax Preparers and Others Should Consider

Introduction

- If you are ever sued over a data breach, you cannot claim you were not aware of the issue, or the steps discussed below as they are set forth in a publicly available IRS publication. This applies not only to CPA firms but to law firms that prepare gift and estate tax returns, trust companies that prepare trust income tax returns, and perhaps even many financial planning firms as the scope of their work expands.
- Data theft against tax professionals is on the rise.
- Addressing data security is an essential step for the largest firms and firms of all sizes including solo practitioners.
- The IRS recommends that tax preparers hire data security experts, buy cyber security insurance, and educate their staff.
- Tax preparers must create written information security plans to protect client data.

Basic Security Steps Recommended for Tax Preparers

- Learn to recognize phishing emails. Remember these scams are intended to entice you to open a link or to open an attachment containing malware.
- Create a written information security plan. See Small Business Information Security - The Fundamentals by the National Institute of Standards and Technology.
- Review internal controls.
- Install anti-malware/anti-virus security software on all devices (including laptops, routers, tablets and phones).
- Encrypt all sensitive files and emails.
- Backup sensitive data.
- Wipe clean or destroy old computer hard drives.
- Withdraw from any outstanding authorizations (e.g., power of attorney for tax information) for taxpayers who are no longer clients.
- Report suspected data theft or loss to the IRS immediately.

Use Security Software

- Anti-virus prevents malware from causing damage to a computer.
- Anti-spyware prevents unauthorized software from stealing information on your computer.
- A firewall blocks unauthorized access to your system.
- Drive encryption protects information from being read if a device is lost or stolen.
- Whatever you use must be updated regularly.

Other Steps

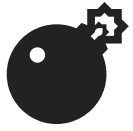
- Use strong passwords.
- Use multi-factor authentication.
- Secure your wireless network.
  - Use a strong unique password for the administrator.
  - Use a name for your router that is not identifiable (e.g., don't call it Tina Tax Saving Service, LLC).
- Protect stored client data.
  - Backup dated to secure cloud storage.
  - Use drive encryption.
  - Don't attach USB devices with client data to public computers.
- Be careful with and perhaps never use "free" software.
- Use separate personal and business email accounts. Do you consistently do this?

Report Data Breaches

- Report data breaches to:
  - IRS.
  - FBI.
  - Police (file a police report).
  - States in which you file returns see StateAlert@taxadmin.org
  - State attorney general for states in which you prepare returns.
- Retain a cyber security expert to assess the breach.
- Report to your insurance company.

Comply with FTC Rules

- Comply with the FTC's Safeguards Rule which requires financial institutions to protect consumer information they collect.
- Develop a written security plan that describes your program to protect customer information.
- The plan must be appropriate for the size of your company and the nature and scope of your activities and the sensitivity of customer information. If you engage in estate planning you may have tax returns, Social Security numbers, detailed family data, information on all assets including financial accounts, family data, etc. Could any data be more sensitive?
- Select service providers that can provide and maintain appropriate safeguards.

8 Defenses to Defuse the  Ticking Time Bombs  in Your Professional Practice

How to Protect Your Client Data from Hackers,
Hackers,
Malware, Ransomware and Other Digital Threats
Threats

BobaGuard

You Are Going to Discover:

The **most modern and effective** methods that solos & small professional firms MUST leverage to **stop cybercriminals** dead in their tracks.

You Are Going to Discover:

Discover:

8 Cybersecurity Solutions

I Recommend to Greatly Reduce

Your Risk of Getting **Hacked**

You Are Going to Discover:

The Easiest Way to **Add Massive Protection** in the **Least Amount of Time** Possible.

This is for you if...

You are a **solo, small firm attorney/CPA/professional** or **office administrator.**

This is for you if...

You believe you have an **ethical duty** to protect your client's data.

This is for you if...

You want to be **proactive** instead of reactive so you can **sleep well at night**.

This is for you if...

You want to do **everything you can** to protect your firm and client data, so you **never** have to tell your clients their data has fallen **into the hands** of cybercriminals.

Why This is Mission Critical

- Putin is knocking on our doors and making no attempt to hide it.
- More than 70% of attacks specifically target small businesses.

Why This is Mission Critical

Critical

- One out of every 3 lawyers has ***admitted*** to being hacked.
- Consider the **reputational** and **financial** carnage created by suffering a data breach. It is **devastating**.

Why This is Mission Critical

Critical

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Why This is Mission Critical

"Model Rule 1.6(c) includes nonexclusive nonexclusive factors to guide lawyers in in making a 'reasonable efforts' determination."

ABA Formal Opinion 483

Why This is Mission Critical

> The sensitivity of the information.
> information.
> - ABA Formal Opinion 483

The greater the sensitivity,
the bigger the steps you're expected to make.
make.

Why This is Mission Critical

> The likelihood of disclosure if additional safeguards are not employed.
>
> - ABA Formal Opinion 483

If a data breach has affected nearly one in three law law firms **despite** some of them using security safeguards,
then the ones **NOT** using additional safeguards must be must be running a sky-high risk of breach.

Why This is Mission Critical

> The cost of employing additional safeguards.
>
> The difficulty of implementing the safeguards.
> safeguards.
> - ABA Formal Opinion 483

The only way to lay hands on good protection has been from vendors exclusively focused on selling to medium and large law firms.

Why This is Mission Critical

> The extent to which the safeguards adversely affect the lawyer's lawyer's ability to represent clients (e.g., by making a device or device or important piece of software excessively difficult to difficult to use).
> - ABA Formal Opinion 483

The solutions we are going to discuss today have done-for-you implementation options, operate in the background, and protect you 24/7 without making it any more difficult to practice law.

Imagine…

- alert from your bank
- money has been transferred out of your IOLTA account to a foreign account in China

Imagine…

- the money is lost
- feeling of dread as you being to grasp the impact

Imagine…

- Open a claim with your cyber insurance provider
- Bring in forensic experts

Imagine…

- Operations are shut down

Imagine...

- Filing a notice of a data breach with the District Attorney's Office

Imagine…

- Letters to ***every*** single contact
- Current **and past** clients, opposing counsel, judges, etc.
- Provide mandatory credit monitoring
- Average cost of $225 per record!

Imagine...

- How quickly the cost of a data breach can rack up
- The importance of carrying a cybersecurity insurance policy

Fear mongering?

But First the Truth...

You will **never** be able to secure your practice from cyberthreats and the risks of a data breach **100%**.

But First the Truth...

You **can drastically reduce** your risk using **affordable solutions**.

Layered Security

8 Layers of Security You Need in Your Practice

Each works together to provide enhanced protection.

- Cyber-Security Training
- Phishing Simulations
- IT Security Policies
- Dark Web Monitoring

- Team-Based Password Vault
- Proactive Maintenance and Patching for Mac/PC with Antivirus + Web Protection
- Cloud-to-Cloud SAAS Backup for Microsoft 365 and Google Workspace
- Automated Phishing Defense Platform

Case Study: We were with a different IT provider, an hourly, hourly, pay as you go type, and **got badly hacked**. The
The funds in our **trust account were almost transferred to transferred to Hong Kong**.
That was the **aha moment:**
what we had been doing was not working, and we needed needed to **do something entirely different**.

You can't imagine the **carnage** that does to a small business business having to send out that kind of letter.

As a result, **the phone stopped ringing**.

David Eltringham
Managing Partner
Eltringham Law
Group
Boca Raton, FL

But what was **really freaky** for me was when I got the list of the stuff we didn't didn't have and had never heard of, that we *should* have been doing.

Our liability would have been off the charts for negligence. It would have been been potentially **gross negligence**, because of the exhaustive list of stuff we didn't we didn't have to adequately and reasonably protect ourselves.

At the end of the day, **you don't know what you don't know**.

And, for a law firm to say, well, gee, we had no idea.
I mean **how does that play in court**?

David Eltringham
Managing Partner
Eltringham Law
Group
Boca Raton, FL

Security Layer #1

Cybersecurity training

- If your employees are trained and knowledgeable about cybersecurity risks, they'll be better equipped to protect your data.
- **NOTE**: If your team doesn't retain the lessons, the training is worthless.

Security Layer #1

Cybersecurity training

- The best training use techniques, like storytelling, to educate your team members on what to look out for in a fun and engaging way.
- So they understand and retain the information.

Security Layer #2

Phishing Simulations

- What is phishing?
- What are phishing simulations?

Security Layer #2

Phishing Simulations

- 91% of successful data breaches started with a spear-phishing attack.
- You must be running phishing simulations to see how your employees are doing; who's struggling and who's leading the charge with security.

Security Layer #2

Phishing Simulations

- Without this solution, you have **no idea** who's putting your firm at risk without knowing it.
- **All it takes is one person**, one time, to grant access to your data.

Security Layer #3

IT Security Policies

Establish:

- Basic security practices and policies for employees, such as **requiring strong passwords**.
- Appropriate **Internet use guidelines** that detail penalties for violating company cybersecurity policies.
- **Rules of behavior** describing how to handle and protect customer information and other vital data.

Security Layer #3

IT Security Policies

- 25% of firms with 2-9 lawyers and 58% of solos **do not** have the security policies needed.

- All firms, regardless of size, should have at a minimum, these policies in place:
  - **acceptable use**
  - **business continuity**
  - **incident response**
  - **records management**
  - **mobile devices**
  - **passwords**

Security Layer #4

Dark Web Monitoring

- What is the Dark Web?
- The Amazon.com for cybercriminals.
- How long would **you** wait to change the locks?

Security Layer #4

Dark Web Monitoring

- 61% of breaches involved credential data*.
- Monitor 24/7/365 - You must **continuously monitor** the dark web for compromised account data on your primary company domain and personal emails.

Verizon 2021 Data Breach Investigations Report

Security Layer #4

Dark Web Monitoring

- **Those 3 slightly altered** passwords you use are most likely **already** on the dark web.
- For example:
  - password
  - password1234
  - pa$$w0rd1234

Shannon's Story

IMPORTANT: NOTICE OF DATA BREACH	
Name of Reporting Person: **Contact Information:**	Shannon [redacted] [redacted] Law Office, P.C. P.O. Box [redacted] [redacted] CA [redacted] Ph.: [redacted] Fax: [redacted]
What happened?	On or about May 5, 2018, we discovered evidence of unauthorized access to mycase.com by an unknown individual or group of individuals. It is unclear how this access was made since we have implemented all security measures offered by mycase.com. Client data was potentially accessed, client case information was deleted, and other administrative changes were made to the system. The extent of the information accessed will be thoroughly investigated by [redacted] Law Office, P.C. and mycase.com. You will be contacted if we discover any information specific to your case.
What Information Was Involved?	Generally, any information uploaded to mycase.com was potentially accessed, and information has been deleted. Information potentially accessed includes client names, social security numbers, driver's license numbers, phone numbers, email addresses, as well as legally privileged/protected information, including legal documents, case notes, disclosures, financial statements, evidence, photos, invoices, transcripts, trust balances, and attorney-client communications. Please note, our standard procedure is to remove identifiable account information from financial statements, tax returns, and disclosure documents *prior to uploading* them into mycase.com. We also do **not** store payment information, such as credit card information used for payments into your trust account. No payment information given to us was ever put into mycase.com whatsoever. We use bank approved software for all payment transactions, which is highly regulated and secure.

Shannon's Story

What she could have done to avoid this.

Date Found	Email	Password Hit	Source
03/16/18	shannon@[redacted] .com	9d2f75377ac0ab991d40c91fd27e52fd	id theft forum

Shannon's Story

What she could have done to avoid this.

Security Layer #5

Team-based Password Vault

- According to a google security study in 2019, as many as 65% of people **reuse the same password for multiple or all accounts.**
- Using a password management tool helps to:
  - stop insecure password sharing
  - create unique passwords
  - securely store all work-related passwords
  - access and share passwords with colleagues

Security Layer #6

Proactive Monitoring, Maintenance, and Patching for Mac/PC with Antivirus and Web Protection

- **Automated** operating system updates, 3rd party software updates, and security patches for both macOS and Windows computers.
- Monitoring notifies you of IT incidents such as your hard drive failing, battery issues and other potential issues - before they stop you dead in your tracks.
- Antivirus and Malware.
- DNS web protection blocks malicious URL domains.

Security Layer #7

Cloud-to-Cloud SAAS Backup
for Microsoft 365 or Google Workspace

- 77% of companies using cloud applications suffered a data loss incident over a 12-month period.
- Google and Microsoft are focused on fixing their own mistakes. But **they are NOT responsible when you make a mistake** — or when a malicious act stops your business cold, in events such as:

- Human error (64% of data loss incidents)
- Illegitimate deletion requests
- Sync errors

- Hackers
- Malicious Insiders
- Malware and viruses
- Ransomware

Security Layer #7

Cloud-to-Cloud SAAS Backup
for Microsoft 365 or Google Workspace

Most people assume everything in 365 or Google Workspace is automatically backed up.

It's not truly backed up, here's why:

- When an employee leaves, you must keep an active license, or else.
- If an employee intentionally tries to cover their tracks, you don't have a separate backup.
- Self-service eDiscovery function makes data requests a breeze.
- Backs up email, contacts, calendar and files (SharePoint, OneDrive or Google Drive).

Security Layer #8

Automated Phishing Defense Platform

- Spam filters don't work against phishing emails.
- AI-based proactive Phishing Protection that helps your 365 or Google Worskpace email filter out these threats before they hit your inbox and test your users.

Security Layer #8

Automated Phishing Defense Platform

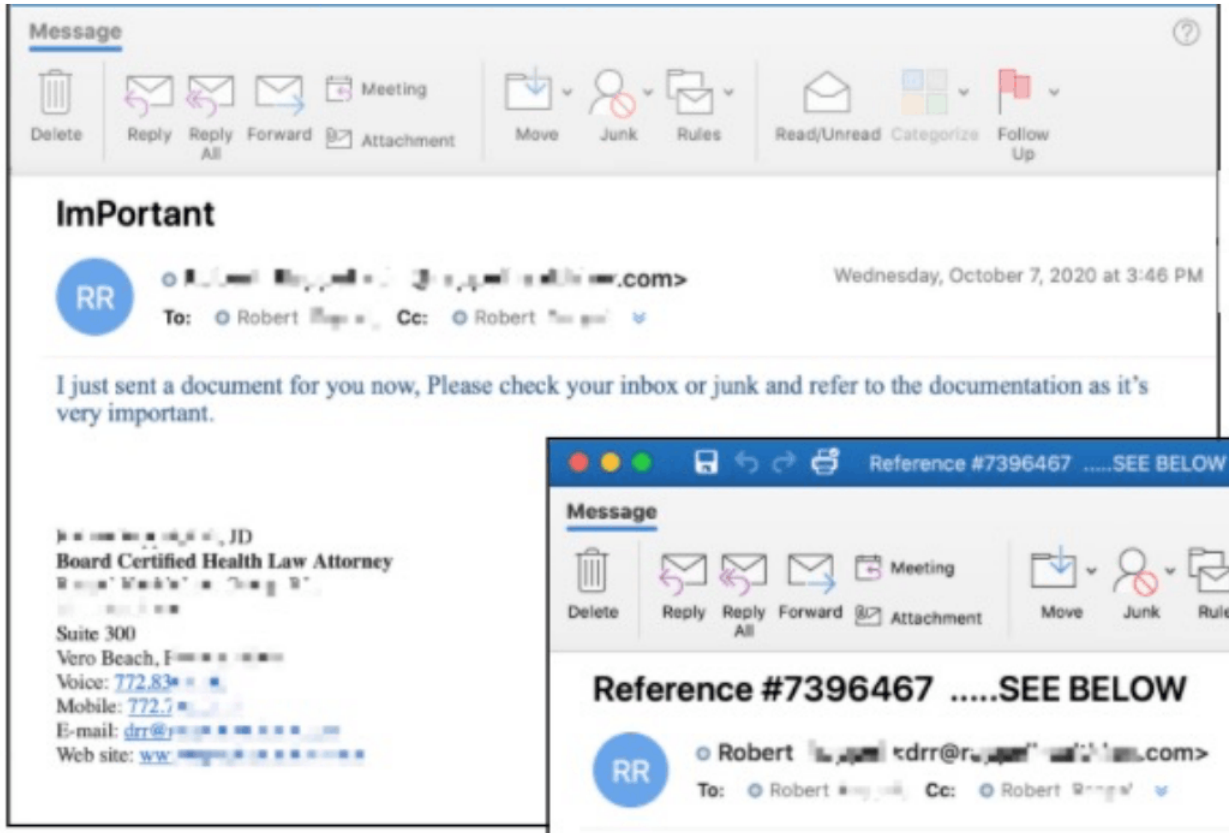
- Protects your entire team from cybercriminals posing as trusted contacts, providing substantial security against disasters like:
- Ransomware
- Business Email Compromise (BEC)
- Account Takeover (ATO)
- And other advanced threats
- **Able to detect and block 99.9% of sophisticated email attacks** before they ever reach employee inboxes.

Hi Tom,

I hope you are doing well and staying safe. We had an opposing counsel whose computer/email systems were recently hacked and it raised a number of questions for me that you may be able to help with. Please let me know if you have a few minutes to talk this afternoon or tomorrow. Thanks a lot.

Regards,

Jason [redacted]
Attorney at Law



From: Jason [redacted] attorneys.com>
Sent: Wednesday, October 7, 2020 4:03 PM
To: Robert [redacted] <drr@[redacted].com>
Cc: [redacted] attorneys.com>
Subject: Re: Email

Robert,

For some reason, the documents are not opening. Please try attaching the documents to this email or if for there is some reason you cannot, let's schedule a time to talk.

Regards,

Re: Email

RR

Robert [redacted] <drr@[redacted]com>

To: Jason [redacted]

Wednesday, October 7, 2020 at 4:04 PM

Thanks for your kind response, the requested email is legitimate and has been secured to your email. Kindly proceed to the document with this your email to gain access and let me know your thoughts immediately.

scan01.pdf
scan02.pdf

Robert [redacted] JD
Certified Health Law Attorney Florida Bar
[redacted] **Law Group, P.L.**
[redacted] Street
Suite 300
[redacted], Florida 32960
Voice: 772.[redacted]
Mobile: 77[redacted]
E-mail: drr[redacted]m
Web site: [redacted].com

8 Layers of Security You Need in Your Practice

Each works together to provide enhanced protection.

- Cyber-Security Training
- Unlimited Simulated Phishing Campaigns & Reporting
- IT Security Policy Templates
- Dark Web Monitoring
- Team-Based Password Vault
- Proactive Maintenance and Patching with Antivirus + Web Protection for Mac/PC
- Cloud-to-Cloud SAAS Backup for Microsoft 365 and Google Workspace
- Automated Phishing Defense Platform

Free Resources #1

#1

Security Checklist for Busy Busy Lawyers

Free Resources #2

Cybersecurity Strategy Call

- 45 minute meeting via Zoom

- Where we will:
  - Define your **biggest security risks and concerns**
  - Identify **the correct strategies** to protect your firm
  - Build **a custom plan** to meet your ethical duties and get peace of mind
  - Plus, we will answer all of the questions you have about **your unique situation**

Free Resources #3

Dark Web Scan Findings Report

A comprehensive Dark Web Scan performed for your firm's primary domain and your personal email, which means **you will know exactly which of your passwords are currently accessible to cybercriminals.**

Free Resources #4

Customized Cybersecurity Plan

A customized plan **built around your primary cybersecurity risks and concerns** along with a list of **recommended cybersecurity solutions** to protect your firm.

At the end of our time together

- You'll have a better understanding of the threats - **known and unknown** - that you need to protect your firm from.
- You'll learn the **most modern and effective solutions** out there that provide protection.
- You'll have a **customized plan**, with specifics, that gives you certainty in the actions needed to get **peace of mind**.

Everything You'll Receive

- Security Checklist for Busy Lawyers
- Cybersecurity Strategy Call
- Dark Web Scan Findings Report
- Customized Cybersecurity Plan

To claim your free resources, resources, **scan the QR code code** or **go to:**

www.bobaguard.com/strategy gy

Additional information

- Tom Lambotte tom@bobaguard.com
- Martin M. Shenkman shenkman@shenkmanlaw.com
- Interactive Legal sales@interactivelegal.com
- Peak Trust Company bcintula@peaktrust.com

www.bobaguard.com/strategy

gy

A KEY ESTATE PLANNING GUIDE

Law Easy

ChronicIllnessPlanning.org

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