ABOUT ME

Alex Rodriguez

- 15+ years working in-house IT for Big Law or providing Fractional IT Leadership for small law firms.
- Worked in Collin County for 8 years: Senior IT Director and IT Director for **Clark Hill <----- Strasburger & Price**. Moved Strasburger's office from Hall Office Park to their current location at the Frisco Sports Complex.
- Founder and CEO of **ABR Consulting, providing Fractional CIO** and Channel Sales to small businesses, including 2 law firms in DFW, one a 30 attorney firm, and the other a solo practice.
- CIO for **Lewis Roca**, HQ in Phoenix, before it combined with Womble Bond Dickinson
- IT Manager **Munsch Hardt Kopf & Harr** in Dallas for 4 years

What we will cover today

Shifting your Mindset around cyber security and technology spend

Identifying the Risks: Understanding the primary threats to your firm's data

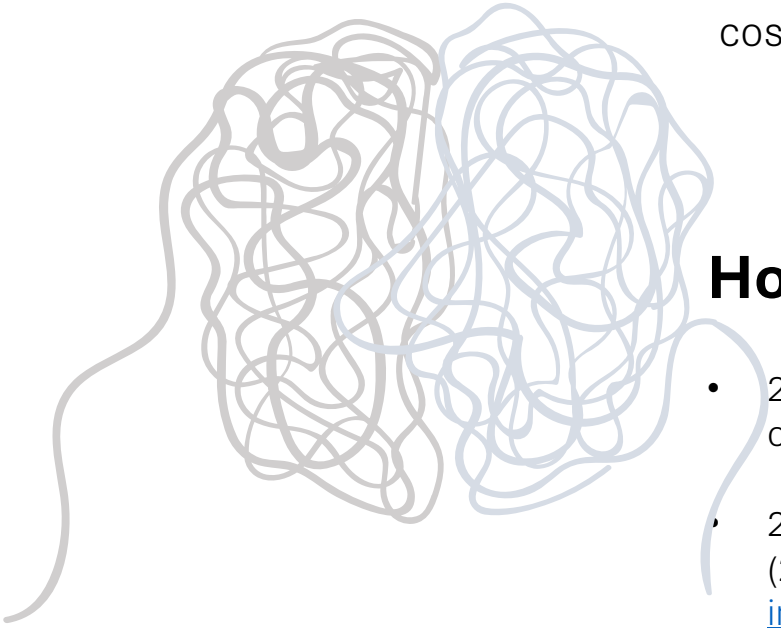
Building Your Strategic Defense: Best practices for people, processes, and technology

Building your Tactical Defense: Practical tools to secure your data and hardware

Technology Spend Mindset at Law Firms

Attorneys understand that technology spend is necessary:

- Internet, wireless, mobile, and legal apps are requirements to run a firm
- Keeping technology up to date satisfies client competence & confidentiality obligations and maintains competitive advantage vs other firms.



But attorneys tend to view Tech as strictly business cost, cost they work hard to minimize, focusing spend on products/services with high obvious ROI.

How much do law firms generally spend on technology?

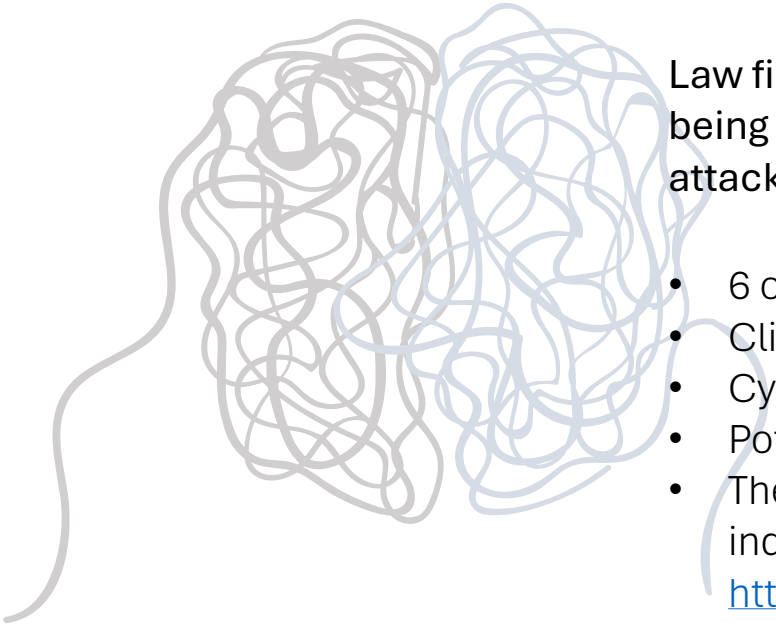
- 2024 article in the ABA Journal suggests Law Firms should be spending anywhere from 3% to 7% of their operating budget on technology https://www.abajournal.com/web/article/creating-a-legal-tech-budget
- 2025 article from Thompson Reuters shows that technology spend growth (7.6%) is far outpacing inflation (2.6%) https://www.thomsonreuters.com/en-us/posts/legal/legalweek-2025-increased-law-firm-tech-investment/

Shifting the Mindset

“Pennies on the Dollar”

The case for technology (cyber) spend should be viewed through an opportunity cost mindset & through a prism of Business Risk - leading to an understanding that cyber spend is a “pennies on the dollar” proposition.

Risk to firm finances – hard costs



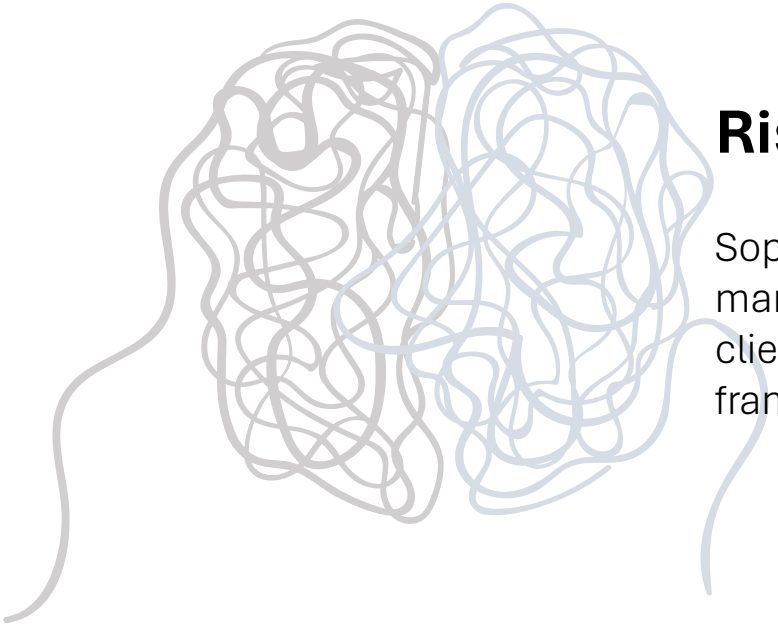
Law firms are prime targets for cybercriminals due to the sensitive nature of their data, explicitly being targeted during significant trials or merger negotiations. The financial impact of these attacks can include:

- 6 or 7 figure ransom payments
- Client notification costs, PR and media relations, and credit monitoring services
- Cyber Forensics teams, increased Cyber insurance rates
- Potential client lawsuits
- The software company Clio calculated in 2024 that the average cost of a data breach in the legal industry, both direct and indirect expenses, now exceeds $5.8 million. https://www.clio.com/blog/data-breach-lawyers/

Shifting the Mindset

Risk to firm finances – soft costs

Trust is the cornerstone of your firm. A single public breach has the potential to erase decades of built reputation, earned trust, and credibility. Firm clients not affected by a specific breach may decide to take their work elsewhere.



Risk to firm revenue – Client Acquisition & Retention

Sophisticated clients now routinely audit their law firms' cybersecurity measures as part of their risk management processes. Firms with strong cyber protocols are better positioned to retain existing clients and attract new ones. Many clients now expect their firms to show compliance with frameworks like ISO27001, NIST, SOC, HIPPA.

Identifying the Risks

Risk #1: The Human Element

Your Biggest Security Vulnerability is Often Sitting in Your Office

- **Desire for convenience**: Attorneys often choose ease and the path of least resistance. Storing data on unsecured file shares, thumb drives, local hard drives instead of the DMS. Transferring PII via unencrypted email or consumer file transfer sites.
- **Untrained staff**: Not being regularly trained and prepared to view all email, texts, or calls as potential attempts by a malicious actor to get you or your staff to reveal sensitive information (like passwords) or deploy malware.
- **Weak controls**: non-complex passwords, no Multi-factor Authentication, poor file security, admin rights given to non-admins, lack of clean desk adherence.
- **Insider Threats**: Whether malicious or accidental, employees can be a source of data loss through social media, file access, thumb drives, etc.

Identifying the Risks

Risk #2: Hardware & Systems Threats

Protecting your data from loss, theft, and failure

- **Data not backed up:** A crashed hard drive on a server or laptop can mean the permanent loss of client data if not properly backed up.
- **Data not encrypted**: Laptops, work phones, and even thumb drives containing unencrypted client data are easily lost or stolen.
- **Data not protected:** Insufficient endpoint management, file security, user security, network security. Lack of visibility and alerting to attacks in progress.

Identifying the Risks

Risk #3: Process Shortcomings

- **Patch Management:** Failing to govern a regular cadence of patch management for your operating systems, Microsoft Office tools, accounting, intake and case management systems leaves known vulnerabilities open for hackers to exploit.
- **Remote access:** Using consumer-grade routers without a proper firewall, not requiring VPN on unsecured public Wi-Fi, not requiring MFA for cloud or SaaS systems.
- **Third-Party Risk Management:** Not vetting where is your data stored and who you've given access to your data
    - Cloud Services (Dropbox, Google Drive, Clio)
    - E-discovery vendors
    - IT, Accounting Platform, and other Consultants

Strategic Defense

Cyber Policy

- **If its not written down, it doesn’t exist**

- **Creation, adoption and implementation of a comprehensive written policy set does several things:**
    - Facilitates the purchase of Cyber Liability Insurance at lower premiums
    - Forces exposure of firm leadership and staff to best practices
    - Creates a structure by which all your Cyber controls and tools can be governed
    - Can be incorporated into employee handbooks and acceptable use (AU) policy
    - These documents also become a client acquisition and retention tool

Strategic Defense

Foundational Cyber Policy Library

- **WISP – Written Information Systems Program** – a Library document covering a multitude of rules and best practices that don't need to each have a separate policy document: Acceptable use, passwords, internet, mobile, data, email rules etc.
- **IRP – Incident Response Plan** – Details how your firm will respond to a Cyber incident, structures your contacts, call tree, assignments and procedures
- **DRP – Disaster Recovery Plan** – Outlines multiple scenarios of recovering your firm in case of critical systems loss or a natural disaster, usually includes your data backup policy
- **TPRM – 3rd Party Vendor Risk Management** – Outlines policy on how your firm will vet your vendors for cyber risk, an external risk questionnaire for your vendors to fill out, and an internal due diligence questionnaire to ensure you properly rate the vendor's risk to your firm.
- **Change Management Policy** – Ensures that changes to technology systems are managed, approved, and tracked. Defines the Change Advisory Board (CAB).

Strategic Defense

Vulnerability Management

- **External Cyber Assessment (annual)** – bring in a 3rd party expert to assess and report on your posture and controls, ranking findings by priority
- **Table Top Exercise (annual)** – run through a simulated cyber attack with business stakeholders to understand and improve your Incident Response Plan
- **Penetration Testing (annual)** – bring in a human 3rd party ethical hacker to attempt to identify potential weaknesses in your technology stack
- **Regular Vulnerability Scans (monthly)** – scans, both external and internal, to report on open vulnerabilities on your network
- **Windows Update Program (monthly)** – identify and deploy updates to your Microsoft & 3rd party program to minimize outdated software risks

Strategic Defense

Security Awareness Training

- **Mandatory Quarterly Security Training:** Implement an inexpensive Learning Management system that pushes relevant curriculum and tracks completion. Courses on phishing, encryption, travel, and social engineering tactics.
- **Simulated Social Engineering Exercises:** Your LMS should be able to send simulated social engineering attacks, phishing, etc and track response. Assign additional training to those who do not pass the test.
- **Encourage a "See Something, Say Something" culture:** Encourage staff to immediately report anything suspicious to firm management or your IT provider without fear of blame.
- **Encourage a Clean Desk culture:** Lock your screen when you step away. Don't leave sensitive documents out in the open.
- **Train on visitor Management:** Be aware of who is physically in your office space.

Tactical (Operational) Defense

Good IT Operations – In-House and/or 3rd Party

- **Expertise to manage your technology operations:** Help organize, streamline and manage and support your day to day technology needs.
- **Either identify or implement cyber tools for your firm**: a strong operational staff or 3rd party Managed Service Provider (MSP) should be able to identify and implement some of the tools we will discuss below.
- **3rd party MSP providing Security Operations Center (SOC) services:** many now offer both the endpoint tools of an MSP with the 24/7 monitoring and alerting of a SOC.
- **In-house IT or 3rd Party MSP are not mutually exclusive:** You can have both an internal technology concierge 8X5 layered with the 24/7 coverage of a 3rd Party MSP

Tactical (Operational) Defense

Endpoint Security

- **EDR – Endpoint Detection and Response** – think of it as modern “anti-virus.” SentinelOne, Microsoft Defender
- **XDR – Extended Detection and Response** – threat detection, notification, and response. Huntress, Sophos, Red Canary
- **RMM – Remote Monitoring and Management** – Tools for secure support access, management of windows device policy and deployment of software patches. Superops.AI, NinjaOne
- **Encryption** – Bitlocker or similar to encrypt hard disks and thumb drives
- **MDM – Mobile Device Management -** like Intune to secure smart phones and tablets with firm data

Tactical (Operational) Defense

Network and File Security

- **Local and Cloud Backups** – Backups of local and server data to secure, immutable cloud backup providers. AFI.AI, Carbonite, etc.
- **MFA – Multi-Factor Authentication** – a second piece of login information to authenticate. Duo, Authenticator. Require “Number matching” over “Tap to Accept”
- **SSO – Single Sign on** – Access multiple applications with a single set of credentials, usually your Microsoft 365 credentials.
- **Password Managers** - create, store, and fill in complex passwords for every website for your enterprise. 1Password, Bitwarden, LastPass
- **IAM - Identify & Access Mgt –** Managing access to resources like file shares
- **Secure File Transfer** – Enterprise versions of Sharepoint, Box, Sharefile or iManage Share with MFA. Avoid free file transfer sites like Dropbox
- **Intrusion Prevention** – network devices that detect, report and stop traversal of your network by bad actors and can be integrated with a third party SOC
- **VPN with Zero trust frameworks for Remote Access**

Tactical (Operational) Defense

Web and Email Security

- **External Banner on inbound external email** – to help identify phishing attacks
- **DKIM and DMARC** – Prevent spoofing & phishing attacks using your email domain
- **Encrypted Email** – enablement of tools within M365 to give you and your staff options to send files securely by email
- **Office 365 Assessments by a 3rd party** - to ensure your Sharepoint and OneDrive settings and conditional access policies are set correctly
- **CNAME and DNS Cleanup** – to help prevent domain exploitation, email highjacking and maintain brand reputation
- **Dark Web Monitoring** – Services that actively search for and track your firm's potentially leaked information on the dark web.

Thank you!!!

ABR CONSULTING

Alex Rodriguez

- 15+ years working in-house IT for Big Law or providing Fractional IT Leadership for small law firms.
- Worked in Collin County for 8 years: Senior IT Director and IT Director for **Clark Hill <----- Strasburger & Price**. Moved Strasburger's office from Hall Office Park to their current location at the Frisco Sports Complex.
- Founder and CEO of **ABR Consulting, providing Fractional CIO** and Channel Sales to small businesses, including 2 law firms in DFW, one a 30 attorney firm, and the other a solo practice.
- CIO for **Lewis Roca**, HQ in Phoenix, before it combined with Womble Bond Dickinson
- IT Manager **Munsch Hardt Kopf & Harr** in Dallas for 4 years

LEWIS ROCA

Clark Hill

#simplysmarter clarkhill.com

Strasburger ATTORNEYS AT LAW

MUNSCH HARDT