The New-ish Billable Skill: CYBERSECURITY COMPETENCE

YOU DON'T HAVE TO BE A HACKER, BUT YOU DO HAVE TO UNDERSTAND ENOUGH ABOUT TECHNOLOGY TO PROTECT YOUR CLIENTS FROM ONE.

WRITTEN BY **MAJO CASTRO**

ONCE UPON A TIME, PROTECTING CLIENT CONFIDENCES MEANT LOCKING A FILE CABINET AND CLOSING YOUR OFFICE DOOR. Now it means updating your password and enabling multi-factor authentication (MFA).

Cybersecurity has quietly become the newest professional skill lawyers are expected to master, right alongside drafting, advocacy, and billing. The American Bar Association (ABA) has made it official: under Model Rule 1.6(c), lawyers must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." That sounds simple enough, until you realize that in 2025, "reasonable efforts" means knowing how to handle encryption keys, cloud storage, phishing emails, and maybe even a ransomware negotiation.[1]

From Locked Drawers to Digital Defense

The duty to protect client information isn't new—it's the foundation of trust in the attorney-client relationship. What's new is *how* that trust is tested. The profession's definition of competence expanded in 2012, when the ABA added the now famous Comment 8 to Rule 1.1, officially requiring technological competence. Translation: You don't have to be a hacker, but you do have to understand enough about technology to protect your clients from one.

The bar associations mean business. Texas and California have both issued opinions clarifying that lawyers are responsible for safeguarding electronic data and supervising the vendors who host it. New York City recently went further, requiring prompt client notification when a cyber incident compromises confidentiality. These opinions aren't theoretical—they're fast becoming the new standard of care.

And breaches aren't just a big-firm problem. According to ABA research, *70% of reported law firm breaches in 2022 involved firms with 50 lawyers or fewer.* The moral: The hackers don't care how big your practice is. Every inbox is an opportunity.[2] And this is nothing new.

Reasonable Efforts, in Plain English

So, what counts as "reasonable"? The ABA's Formal Opinion 477R[3] gives us a checklist, and no, "hoping for the best" isn't on it.

- *Encryption:* All client data (at rest and in transit) must be encrypted.
- *Access control:* Strong passwords, MFA, and device locks are non-negotiable.
- *Vendor diligence:* Vet cloud and AI providers carefully; know how they store and use your data.
- *Training:* Your people are your firewall. Phishing awareness and basic cyber hygiene must be ongoing.

The point isn't perfection, it's prevention. "Reasonable efforts" mean you've done enough to mitigate foreseeable harm. But "enough" in 2025 is a far higher bar than it was even five years ago.

The Zero-Trust Mindset

"Zero trust"[4] may sound pessimistic, but in cybersecurity it's a philosophy that keeps firms safe. The idea is simple: *never trust, always verify* as my mentor, Seth Nielson, founder of and chief scientist with cybersecurity engineering firm Crimson Vista, often emphasizes. Every device, every user, every login must prove itself every time.

Implementing a zero-trust approach doesn't require an IT army. It starts with a few key habits:

- *MFA:* Across all systems (yes, even billing).
- *Least-Privilege Access:* Each user gets *only what they need.*
- *Segmentation:* Keep your case-management system, HR records, and client-billing data on three separate network segments. Each "area" is walled off so users only access what they should, when they're supposed to, keeping client information safe by design.

Zero trust is the operational version of Rule 1.6(c): Preventing unauthorized access, but by design.

Data You Don't Have Can't Be Stolen

Another lesson from the trenches: data minimization. Collect only what you need, keep it only as long as

required, and securely delete it when you're done. Old client data is like expired medicine—it does more harm than good.

Most privacy and security regulations are headed in the same direction: data minimization—basically, keep only what you *actually* need. And honestly, even without the regulations, it's just good practice. Every extra file is one more thing that can leak. Keeping decades-old client data "just in case" is basically asking for trouble.

When Things Go Wrong (and They Will)

Even with the best safeguards, no system is bulletproof. That's why every firm needs a written incident response plan—your fire drill for data breaches.

A good written incident response plan should spell out exactly who to call, your IT team, your cyber insurance folks, your lawyer, your forensic experts, management, and even law enforcement if things get sticky. Basically, you want a "break glass in case of emergency" contact list so you're not scrambling to remember anyone's number at 2 a.m. It should also cover how to preserve evidence and how to talk to clients without creating more panic.

The golden rule: Don't wing your team's response after a cyberattack. A practiced plan turns chaos into control, and just like in our legal work, we have to practice what we preach when a cyberattack hits.

Privilege protection is another trap. A well-known practice to preserve confidentiality over forensic investigations is for outside counsel to retain the forensics firm, ensuring reports are created for legal advice and not for business remediation.

Finally, remember your notification duties. In many situations, clients must be informed if their data is compromised, and to make it more complicated, every state has its own breach-notification laws, some with very tight timelines. Your plan should spell out who's responsible for handling this so you're not drafting notices at midnight.

Why This Is the New Billable Skill

Regulators are no longer sympathetic to "we didn't know." In 2023, the New York attorney general fined a law firm $200,000 for poor data security that exposed approximately 114,000 client records.[5] Disciplinary bodies are citing lawyers for failing to train staff or supervise vendors.

Civil exposure is rising too. Plaintiffs' lawyers now use ABA opinions as evidence of what "reasonable care" looks like. A failure to follow them can open the door to malpractice or fiduciary-duty claims.

Cybersecurity is no longer an IT issue. Clients are now increasingly asking firms to disclose their data-security policies before engagement. Cyber insurers require regular audits. In short, protecting client data is now both an ethical duty and a business strategy necessity.

Meeting that standard comes down to three pillars:

1. *Administrative competence:* Train everyone, have policies, and review them.
2. *Technical competence:* Encrypt everything, enforce MFA, and adopt "zero trust."
3. *Governance competence:* Vet vendors, maintain an incident plan, and document compliance.

Lawyers have always carried the responsibility of trust. In the digital age, that trust is defined not only by our judgment and discretion, but also by the strength of the systems that protect the data behind them. **TBJ**

NOTES

1. Rules 1.1 & 1.6, and Comments, American Bar Association Model Rules of Professional Conduct (Am. Bar Ass'n 2020).
2. Texas Comm. on Prof'l Ethics, Op. 705 (2019); *see also* Cal. State Bar Formal Op. 2020-203; *see also* N.Y.C. Bar Formal Op. 2024-3; *See also* Corey Garver, *Three Things Midsized Law Firms Can Do Now to Mitigate Their Cyber Risk, American Bar Association Business Law Section* (January 12, 2024, https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-january/three-things-midsized-law-firms-can-do-now-to-mitigate-their-cyber-risk/.
3. Formal Opinion 477R, American Bar Association (May 11, 2017; rev. May 22, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-477.pdf.
4. The Law Firm Guide to Cybersecurity, Wash. State Bar Ass'n (2022); *see also* Sharon D. Nelson, Esq., *Zero Trust Architecture: An Imperative for Law Firms* ALPS Insurance Blog (Nov. 15, 2023); *see also* Data Minimization & Records Retention, Greenberg Traurig, LLP (2022), https://www.gtlaw.com/en/capabilities/data-privacy-cybersecurity/data-minimization-and-records-retention.
5. *Attorney General James Secures $200,000 from Law Firm for Failing to Protect New Yorkers' Personal Data,* Office of the New York Attorney General, Press Release (March 27, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-secures-200000-law-firm-failing-protect-new-yorkers.

MAJO CASTRO is the founder and managing attorney of CastroLand Legal, a Texas-based firm specializing in cybersecurity, privacy, and regulatory compliance. Castro advises startups, MSPs, and mid-sized companies on developing effective compliance programs that balance legal precision with business practicality.