STASH®

Not Better Data Protection. Bona fide Data Protection

LEGAL SERVICES

Law firms are facing increasing external cyber attack as well as insider threats. Criminals, nation state actors, and even interested commercial parties are attracted to the crown-jewel types of data with which firms are often entrusted. As law enforcement warns, law firms in general are more lax on security than the corporations they represent. As the Panama Papers shows, even sophisticated firms can be hacked with devastating impacts on their reputations as trusted advisors to large companies or high net worth individuals with closely held secrets. The consequences of breach can be firm-destroying with massive financial and even political consequences for clients. Firms who hold intellectual property, merger and acquisition, commodity investment, contract negotiations, market deals, and family and personally sensitive data are phenomenally attractive. The risk is as real for small firms as the largest firms.

"Nearly 50 law firms were targeted by a Russian cybercriminal who posted on a cybercriminal forum seeking a hacker to collaborate with him. He hoped to hire a black-hat hacker to handle the technical part of breaking into the law firms, offering to pay $100,000, plus another 45,000 rubles (about $564). He offered to split the proceeds of any insider trading 50-50 after the first $1 million. Sporting of him. The list of law firms reads like a "Who's Who Among Top Law Firms." … we believe most of them have been breached."

– Sharon D. Nelson, President & John W. Simek Vice President Sensei Enterprises Quoted in Law Practice Today, American Bar Association

"Law firms have always operated inside a bubble of their own making, in which information security will take care of itself because "we're all good people" and "we've been careful in hiring and training." A moment's reflection reveals the vacuity of those attitudes when put up against determined, full-time, state-supported hackers."

– Robert Owen, Partner in Charge Sutherland Asbill & Brennan's New York office quoted in Law Practice Today, American Bar Association

At a recent ABA seminar experts urged the creation a cyber-aware culture, the running of readiness assessments, obtaining cyber risk insurance, etc. But common to all the advice was the need for firms to encrypt data, test their backups, partition and limit data to only those who need access – "Rely on multiple layers of data protections that involves pervasive use of encryption and strong authentication". This is where STASH comes in.

AICPA | NIST | SOC 1 | SOC 2 | SOC 3 | ISO 27001 | Privacy Shield (Safe Harbor) | PCI- DSS | HIPAA

Digital Confetti® • Keys-on-the-Fly® • Data Integrity & Resilience for Decades • Cost Effective

+1 (844) 833-7373 Stash America LLC contact@stash.global

"I think that number is vastly understated based on what I experienced firsthand throughout my travels and conversations with firm leaders across the country. The fact that firms are typically not required to report unwanted network intrusions lulls other firms and the public into a blurred sense of reality in regards to what is really happening in the marketplace. When I'm in a group setting, I still don't see many people raise their hands to discuss a recent breach, but almost all of them have some type of incident to share that occurred at their firm when we are behind closed doors".

– Marco Maggio, U.S. Director, All Covered Legal Practice quoted in Law Practice Today, American Bar Association

"Law firms should understand the risk and have strong policies and procedures in place both for prevention/detection and mitigation of the information. If some client information is sensitive, measures should be taken to avoid storage where it is easy to obtain. Similar to the old practice of keeping paper files under lock and key, partitioning of especially sensitive data should be practiced. Law firms should have a data storage policy that only keeps documents on their main systems if necessary, then transferred to a more secure storage vehicle."

– Braden Perry, litigation, regulatory and government investigations attorney Kennyhertz Perry quoted in Law Practice Today, American Bar Association

Whether you want to keep things to yourself or share with others, STASH delivers DSECaaS™ (data-security-as-a-service) to meet your needs. In a world of Open Networks and Bring Your Own Device, we focus on the crown jewels. On the data. On what really matters to your business.

STASH Data Protection for everyday valuable data and STASH HIBERNATE® for very long term data protection with data integrity for decades are the most impactful encryption and privacy Solutions ever developed to protect the actual data bytes themselves. STASH doesn't analyze, predict, try to defend, or react to data compromise after the fact like 99.99% of all other security options. When data is protected with STASH, it has a statistical probability of nil to breach, manipulation, loss, harm, or ransomware.

Data, network, and infrastructure agnostic, STASH is completely automated and simple to deploy, without changing anything about how you do business. Activated via SAAS, Secure Backup, & API

AICPA | NIST | SOC 1 | SOC 2 | SOC 3 | ISO 27001 | Privacy Shield (Safe Harbor) | PCI- DSS | HIPAA

Digital Confetti® • Keys-on-the-Fly® • Data Integrity & Resilience for Decades • Cost Effective