LEGAL workspace
Your Law Office in the Cloud

Key findings from the Panama Papers

Learn more about how to protect your client's confidential data.

LEGAL workspace
Your Law Office in the Cloud

What the Panama Papers breach means for your law firm

11.5 million documents containing confidential data were stolen from Mossack Fonseca, the world's fourth largest offshore law firm, and published as The Panama Papers online. Hackers gained access to one of the firm's servers which allowed the hackers to steal valuable data and emails. All law firms collect and store a myriad of client and financial data making them attractive targets for cyber attackers.

High value data including trade secrets, acquisitions and mergers and personal health information (PHI) can be leaked to the public or used maliciously. For example, a large law firm handling a merger might be targeted by someone who wants insider information in order to buy or sell stock. Not all cyberattacks target complex data -- even basic client data can be targeted. For example, a small law firm might be handling a divorce and the other party works in IT and has the skills to discover what the representing attorney has planned.

While the hacking motives vary the consequences are consistently catastrophic for law firms. Data breaches erode the foundation of attorney-client privilege by exposing sensitive data solely entrusted to law firms. Therefore, securing and protecting privileged information is of the utmost importance.

How can you prevent a data breach?

1. Intrusion prevention and protection systems

   Your network should have an intrusion prevention and detection system in place to monitor unusual server traffic. This system helps to identify and shut down hackers, who constantly search IP addresses looking for weaknesses. Two-factor authentication provides an extra layer of intrusion protection by requiring users to enter two forms of identification during the log in process. This approach eliminates the chances that a hacker or computer program can log in to a system remotely and randomly create passwords.
2. Firewalls

Law firms should look for enterprise grade firewalls to protect against malicious software and hackers. Some law firms use multiple firewalls to ensure that if one firewall fails, a backup is already in place.

3. Email Encryption

   Hackers don't observe attorney-client privilege, and the highest value target is a law firm's email. Email is the easiest way for clients to send crucial documents and even medical records to attorneys. Email encryption protects data so only the sender and recipient can view email contents.

4. Internal and External Security Scans

   Hackers are constantly evolving their techniques to circumnavigate existing security protocols to find vulnerabilities. Routine security scans are required to ensure data is constantly protected. Law firms that require ultra-security, for HIPAA or governmental compliance, must conduct internal and external security scans on an annual basis.

5. Data Backups

   Off-site data storage is crucial in case all of the other security techniques fail or a natural disaster, theft or fire occurs. Data from ransomware attacks can be fully recovered using back up records, without paying a ransom fee to recover encrypted data.

Encryption, secure data centers, authentication protocols, intrusion monitoring: Complex IT considerations can make your head spin. Even if you have an IT department or person dedicated to managing those issues, it's tough to stay on top of the latest threats when you're focused on building your practice. Thankfully, you have options. Legal Workspace has extensive experience securing law firms from physical and cyber threats. We worry about security. You worry about practicing law.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more or arrange a free demo at legal-workspace.com.