U.S. Legal Support

10 Essential Cybersecurity Questions to Ask When Choosing a Litigation Support Services Partner

Cybersecurity threats are escalating, and the legal industry is no exception. According to the ABA's 2023 Legal Technology Survey Report, nearly **30% of law firms reported experiencing a security breach**—a worrying figure that highlights the vulnerabilities within the sector. Additionally, IBM's 2024 Cost of a Data Breach Report reveals that the **global average cost of a data breach has soared to $4.88 million**, the highest recorded to date and a 10% increase from 2023.

Professional services organizations, including law firms, face even greater risks, with **the average cost of a data breach reaching to $5.08 million**. High-profile incidents, including reported breaches at three Am Law 200 firms in 2023, further underscore the urgent need for robust cybersecurity practices.

Lawyers have an ethical obligation to safeguard client information under ABA Model Rule 1.6, which requires "reasonable efforts" to prevent unauthorized access or disclosure of client data. Failing to detect or mitigate breaches not only violates this ethical duty but can also lead to costly lawsuits, reputational damage, and erosion of client trust.

The rise of Artificial Intelligence (AI) in the legal industry introduces additional layers of complexity and risk. While AI tools offer efficiency and innovation, they also present unique cybersecurity challenges, including potential vulnerabilities in AI modeling, data integrity, and decision-making transparency. Legal professionals need to carefully evaluate how AI-driven tools and solution providers manage sensitive data to ensure their systems don't inadvertently expose their practices, and thus clients, to risk.

When selecting litigation support partners for services like court reporting, record retrieval, or trial services, it's imperative to thoroughly vet their cybersecurity measures, especially those involving AI technologies. Partners must not only have comprehensive prevention strategies but also quick-response plans to mitigate any threats that materialize. By proactively addressing vulnerabilities and staying informed about evolving risks, firms can uphold their ethical responsibilities, protect sensitive client data, and safeguard their reputation in an increasingly digital and high-stakes landscape.

U.S. Legal Support

10 Essential Cybersecurity Questions to Ask When Choosing a Litigation Support Services Partner

1. IS YOUR COMPANY HIPAA COMPLIANT?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 dictates how protected health information is stored, handled and disclosed. To ensure the confidentiality of your clients Protected Health Information (PHI), you need to work with a HIPAA compliant partner.

2. HAS A SOC 2 TYPE 2 EXAMINATION BEEN CONDUCTED?

SOC refers to "System and Organization Controls" and these are designed to measure how well an organization manages and protects client data. A successful SOC 2 Type 2 audit takes this an important step further, confirming that an independent third-party auditor has verified that best-in-class procedures, safeguards and technologies are employed across the five trust principles - security, availability, processing integrity, confidentiality and privacy. Equivalent examinations like the ISO 27001:2022 can also give you good insight into a firm's security posture.

3. HAS AN INDEPENDENT AUDITOR VERIFIED BOTH SOC 2 TYPE 2 AND HIPAA COMPLIANCE?

Without attestation from a reputable independent auditor, you cannot guarantee that systems and operational processes ensure HIPAA compliance and follow SOC 2 Type 2 guidelines. Without this third-party verification, a vendor will also be unable to corroborate its answers to the vital questions on this list, including the nature of system and operational controls employed within the company, what risks are being mitigated by these systems and the effectiveness of the controls.

4. DO YOU HAVE A SECURITY OPERATIONS CENTER (SOC)?

A Security Operations Center gathers input from the following sources to protect systems and data:

- Intrusion detection and prevention systems that continuously monitor a network for vulnerabilities
- Firewalls that are preventing malicious access to systems
- System events on servers and staff computers that could signal malicious activity
- Endpoint malware and malicious activity
- Internet protection systems reporting malicious activity

5. WHAT IS YOUR DISASTER RECOVERY PLAN AND WHAT REDUNDANCIES DO YOU HAVE IN PLACE?

As the saying goes, "if you fail to plan, you plan to fail." Disasters come in many forms. Whether hackers, electrical fires, floods or broken air conditioning units, It is imperative your partner of choice has a disaster recovery plan. Not only does this protect your data, but enables your business to continue operations in the event of an emergency or disaster.

6. HOW IS DATA PRIVACY ENFORCED AND MONITORED?

To safeguard your privacy, a partner should offer strict role-based access control, limiting who has access to your data within the organization. The enforcement of strict access control should be audited and tested in a company's SOC 2 Type 2 report.

7. WHAT IS THE INCIDENT RESPONSE PLAN?

In the event of a breach, having a complete incident response plan will reduce damage and help you recover as quickly as possible. When considering a potential partner, this is an important component that should not be overlooked. The incident response plan, and how incidents are handled within a company, will be audited and confirmed in the company's SOC 2 Type 2 report.

8. IS YOUR DATA BACKED UP AND IF SO, HOW OFTEN?

To prevent data loss, a provider should perform at minimum daily backups of all systems and data. A company should also replicate systems and data to a separate geographic location to assure that they are always available. Backup activities should be audited and confirmed in the company's SOC 2 Type 2 report.

9. ARE THIRD-PARTY PENETRATION TESTS CONDUCTED ON KEY SYSTEMS EXPOSED TO THE INTERNET TO ENSURE THEY ARE SECURE?

Penetration testing conducted by a reputable third-party firm helps ensure client data is safe when using systems exposed to the Internet. Confirmation of penetration testing should be included in a company's SOC 2 Type 2 report and a company should be able to produce a report that shows testing results.

10. FOR AI SOLUTIONS, HOW IS YOUR DATA MANAGED?

It's important to understand the scope of the data the solution has been trained on. For instance, has the AI solution been trained on data across the entire internet, or is it using a curated repository? Additionally, is your data being used for training and is it being stored? If so, for how long?

U.S. Legal Support

THE U.S. LEGAL SUPPORT DIFFERENCE:

Industry Leading Full-Spectrum Security

U.S. Legal Support offers **security and data protection** that no other litigation support company can provide. We follow the **NIST Cybersecurity Framework** regarding policies, procedures and controls, meeting and exceeding requirements. We work hard so you can rest easy.

- **HIPAA compliant**
- **SOC 2 Type 2 compliance**
- **Attestation from reputable independent auditor of all systems, processes and controls**
- **24/7 Network and Security Operations Center**
- **Intrusion detection and prevention systems**
- **Third-party penetration testing**
- **Incident Response Plan vetted by independent cybersecurity incident response experts**
- **Frequent backups and replication across multiple datacenters in separate geographic locations**
- **Disaster recovery plan**

To learn more about U.S. Legal Support's robust security and full-service litigation support services, please contact your local U.S. Legal Support Representative.