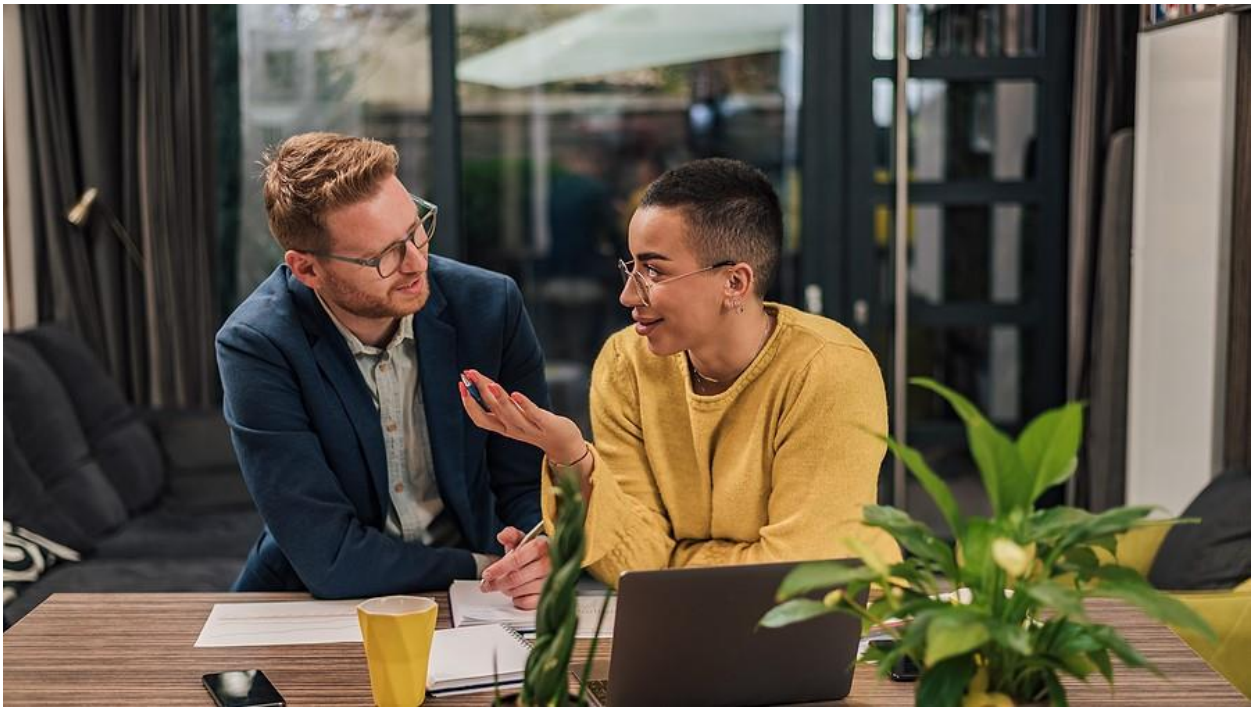
Law Firm Cybersecurity Questions to Ask Your Attorney



In 2020, the law firm Grubman Shire Meiselas and Sacks suffered a ransomware attack. When the firm refused to pay the ransom, hackers threatened the firm's superstar clients, including Lada Gaga, directly. The attack highlights the importance of evaluating your attorney's security stance by asking key law firm cybersecurity questions.

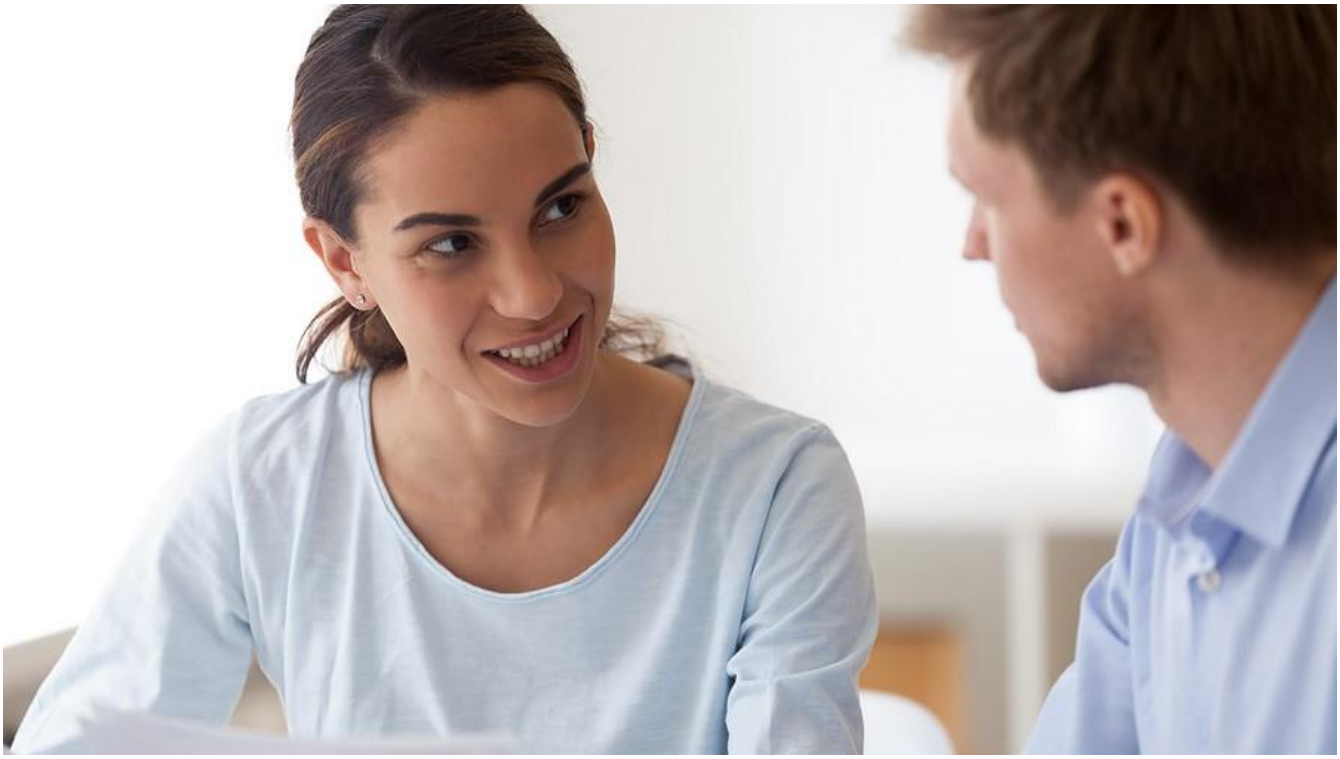
As you approach a potential legal team, think about the amount of personal and business data they hold. This treasure trove includes financial information, business contracts, highly personal data of executives and employees and data relating to any active or prior litigation.

Fifty years ago, a thief would have to physically break into the law offices to access that data. Now, a sophisticated hacker can potentially steal the data from thousands of miles away, with little risk of prosecution.

Consequently, businesses need to thoroughly vet potential legal teams. The following questions will help executives determine the security posture of firms with responsibility for protecting both business data and reputation.

What Legal and Ethical Responsibilities Do You Have Regarding My Data?

According to ethics standards and various privacy laws, attorneys must take reasonable steps to protect client data. However, the specifics of those regulations vary from state to state and continually evolve. Make sure that your legal team has procedures in place for keeping up to date with regulations and demonstrating compliance.



How Will You Protect My Sensitive Data?

Your attorney will store some of your most sensitive data. You need to know what policies and procedures they have in place to protect that data. A competent legal firm will have a comprehensive cybersecurity strategy in place that includes at least the following measures:

- Data encryption – Your attorney should ensure encryption of your data both in transit and at rest. This should include both files and emails, whether they live on a server, in the cloud, on a PC or on a mobile device.
- Multi-factor authentication (MFA) – Traditional passwords prove inadequate against sophisticated cyber criminals. MFA provides a critical extra layer of protection by requiring three factors to verify identity when accessing sensitive data.
- Robust email security – Email remains the go to attack vector for hackers. A multi-layer approach to email security includes high-quality email filters, regular cybersecurity training for employees and advanced threat detection.
- Risk assessments and monitoring – Organizations should conduct regular risk assessments to highlight and fix security vulnerabilities. In addition, automated 24x7 monitoring solutions discover and address anomalies before a breach occurs.
- Remote access management – Attorneys conduct much of their business from mobile devices and laptops. Consequently, a solid cybersecurity strategy must address those endpoints with comprehensive endpoint protection and mobile device management.

- Regular backups – Verify that the firm has automated a system of regular backups, with testing and off-site storage.

Does Your Firm Have an Incident Response Plan?

Even with strong cybersecurity, incidents will occur. Your attorneys should have a detailed incident response plan in place. That plan will include procedures for incident detection and containment, as well as data recovery.

Your attorneys' cyber-attack protocol should also address policies and procedures around breach notification. They should be able to clearly explain how and when you and the public will be notified in the event of a breach.

Build Law Firm Cybersecurity Questions into Attorney Engagement

Because law firms store valuable data, they present an attractive target for cyber criminals. Unfortunately, many firms have not implemented adequate cybersecurity to counter that threat. In fact, a recent American Bar Association study found that less than half of respondents used basic security measures such as encryption and MFA.

Therefore, when engaging an attorney, organizations should carefully prepare law firm cybersecurity questions to learn about their cybersecurity strategy. Additionally, ensure that your contract with your attorney includes language guaranteeing key cybersecurity practices.

The legal cybersecurity experts at eMazzanti know both the risks you face and the challenges unique to the legal sector. They can help you evaluate your key business partners from a security perspective and ensure that your critical business data remains safe.