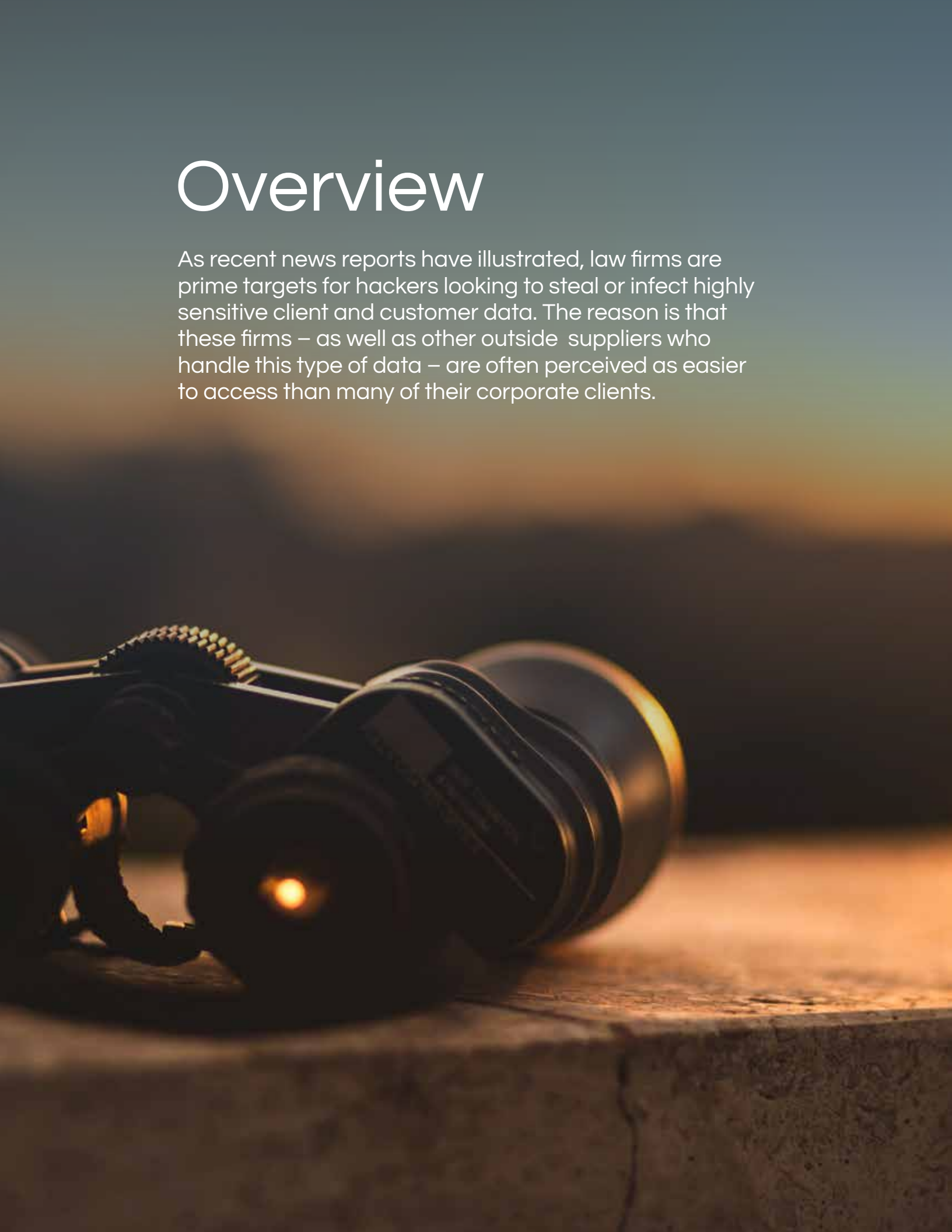
epiq precision

Seven Questions to Ask Your eDiscovery Vendor About Data Security

People. Partnership. Performance.

Overview

As recent news reports have illustrated, law firms are prime targets for hackers looking to steal or infect highly sensitive client and customer data. The reason is that these firms – as well as other outside suppliers who handle this type of data – are often perceived as easier to access than many of their corporate clients.



It is essential for companies sharing sensitive information outside their control to ensure that each supplier who receives that data meets or exceeds all regulatory security requirements for the classification of data you trust.

Epiq is considered one of the security leaders in eDiscovery, protecting highly sensitive data for law firms and corporate legal departments throughout the world. What follows in this white paper is a suggested vendor security screening and evaluation process to vet each vendor before they are allowed to access secure information. This may be helpful as you evaluate your own approach and process. For this white paper, we are assuming your internal security meets or exceeds the standards for your industry.

Vendor Data Security: Considerations

A common misconception is that vendor security is primarily a technology and security issue. It is actually far more involved, encompassing a much broader scope of vendor activities and procedures not directly related to technology, such as personnel screening and documentation.

You should have an established, documented (and regularly updated) process framework to govern and guide your vendor screening and management process. The scope and intensity of your screening and management efforts will likely vary by vendor, based on the services that vendor is providing and the risk associated with both the specific vendor and data. Defining and assigning these risk classifications are both initial steps in the process outlined here.

Some prescreening questions to consider: Have you documented all touch points for the data accessed by the vendor candidate? Do you have clear, written security requirements and restrictions established? These are essential steps prior to screening. Each instance of your data moving beyond your vendor network (such as when information related to litigation and regulatory matters is shared with outside counsel, experts and opposing parties) must also be included.

Vendor screening and management is a complex process, requiring specialized expertise and an ongoing, potentially substantial commitment of time and resources: first, to prepare for each screening and then conduct the review, analysis and remediation, and finally, to manage vendor relationships and service components throughout the vendor life cycle. There is no doubt these steps are essential to ensuring data security, but, understandably, not every company or organization can – or wants – to take it on. For those who do not want to shoulder the burden, outsourcing is the preferred option.

“The most common misconception we see is that vendor security is primarily a technology and security issue. It’s actually far more involved, encompassing a much broader scope of vendor activities and procedures.”

Prior to Vendor Screening: Data Risk Clarification

If your organization has an established classification framework, use it to classify the categories of data you share with outside vendors. Is it sensitive or secret? Does it contain protected data, such as health, personal or financial information? What's the risk of unauthorized disclosure, theft, corruption or loss? This helps you assess the depth of screening and monitoring required for each vendor and the different risk layers of data they may be handling.

Some of the factors to take into account during vendor risk classification:

- **Regulatory requirements:** You should have a clear understanding of all regulatory and compliance requirements applicable to your industry, organization and vendors.
- **Security requirements:** Which of your policies and procedures concerning data transfers and information sharing and technology apply to this vendor?
- **Privacy requirements:** Does the data contain multi-jurisdictional privacy data? Do you need a DPA addendum and special security measure?
- **Risk appetite:** How much risk are you willing to accept for this vendor, based on the data they have access to? Your risk appetite decision should consider the full range of services this vendor is contracted to provide for you.
- **Organizational policies:** What other internal policies and requirements may apply to this vendor?

Prior to Vendor Screening: Vendor Risk Classification

Similar classification must then be applied to each of your vendors. Is this vendor core to your revenue stream? Do they access or process data with critical classification levels? What is your risk/liability/publicity if the information you supply to this vendor is disclosed, stolen, corrupted or lost? A vendor classified as critically important (due to revenue impact, etc.) that is handling highly sensitive personally identifiable information (PII) will likely require your most thorough/frequent level of screening.

Vendor Screening

Once the data and vendor risk assessments have been completed and the requirements and classifications defined, the vendor screening process can begin. This process should follow an established cycle, with defined review points, as well as defined triggers for the escalation of concerns.

This vetting process can often take two to three months or more, depending on the vendor's size and structure and their ability and willingness to respond to remediation requirements that may arise.

1. Develop and distribute vendor questionnaires

Your questionnaire(s) should cover all relevant topics determined by your data/vendor risk classifications and defined requirements (developed prior to screening). The appropriate questionnaire is sent to each vendor, so you can begin assessing their ability to successfully safeguard your data.

Some companies use the Standardized Information Gathering Questionnaire (SIG) by Shared Assessments (www.sharedassessments.org), a series of questions on how a vendor manages information technology and data-security risks across 16 risk-control areas.
It may meet your needs or serve as a starting point for your own customized questionnaire(s). Submit the questionnaire with the requested completion date.

2. Establish expectations and scope of services

In addition to completing your questionnaire, the vendor should provide sufficient evidence (screenshots, policies/procedures, narratives, etc.) that their controls are operating as stated. We recommend an initial call to establish expectations and discuss the scope of services covered in the questionnaire. Information deemed confidential by the vendor should be gathered in person or via a secure online connection.

3. Analyze, verify and evaluate completed questionnaire and supporting documentation

via a secure online connection.
You now need to thoroughly evaluate and research the responses to determine if the vendor is operating in a way that meets the data-protection level you require for the data they are handling. Your internal auditor(s) must be satisfied that the information provided is sufficient proof that the controls are operating as required. This is an iterative and potentially time-consuming step, as it often requires considerable communication between the organization and vendor until the evidence is deemed satisfactory. Your auditor(s) may also need to spend time at the vendor's site to request, view and verify evidence that specific processes are operating as stated in the questionnaire.
At this point, there may be items that do not have sufficient evidence or that are simply not operating properly. These items should be compiled and documented for the subsequent report that will be used to track issues which call for vendor remedial activity – in other words, what the vendor needs to do to fix the problems identified that fail to meet your security requirements.

4. Meet with vendor to review findings and next steps

At this meeting, the findings report is reviewed in depth and hopefully agreed to by both parties. This can be a challenging meeting, in that you may be requiring the vendor to modify or replace long-standing processes, buy new equipment and/or software or undertake some other significant improvement to meet your requirements for working together. There could easily be push-back. Rather than make this an adversarial situation, we suggest you encourage their feedback – they may have a sensible explanation for why one of your requests is not necessary or can be approached in a different way. If the vendor cannot (or will not) remediate the concerns identified in your review, you will need to address this internally and decide if a compromise will fit your company's risk-acceptance profile for this vendor and data. If they are willing to proceed, however, the vendor should then be asked to prepare a remediation plan and timeline. Remediation may last two to three months, depending on the vendor's ability to successfully accomplish the changes.

5. Track and verify vendor remediation

Once the vendor agrees to your remediation requests and provides a timeline, you essentially assume the role of project manager: tracking progress and timeline completion dates, examining the results and potentially requesting and evaluating new evidence, as required.

6. Submit final vendor report

Prepared once all remediation has been completed, this report documents the risk the vendor posed to your company at the start of the process and where they are now. If they meet your security and contractual requirements, they receive your authority to operate. If the risk is still too high, based on your internal classification and risk tolerance, and further remediation is not an option, you must decide whether to accept the risk or look for a new vendor.

7. Ongoing vendor management / repeat screenings

Screening is usually not a one-time event and often must be repeated. In many cases, an annual reassessment is appropriate, while in others your data and vendor risk classification may require more frequent audits to ensure that no security lapses have occurred.

The Outsourcing Option

Outsourcing eDiscovery to a company such as Epiq can mean substantial cost-savings and convenience over internal screening and management, but it doesn't alter your need for rigorous vendor security. The company you choose must meet or exceed the industry's strictest security standards for protecting your data, which Epiq does.

When you host your data, you have to continuously monitor your internal security – and that of your vendors – to ensure that hackers cannot gain access to it. Epiq's data security is the best in the industry and has passed exhaustive auditing by Fortune 500 companies and Am Law 100 law firms. With Epiq eDiscovery data hosting, managed services or document review, your most sensitive data is as safe as it possibly can be, rigorously protected by multi-layered security, anywhere in the world. Epiq also provides unmatched expertise and response in the event of a data breach incident.

Conclusion

Whatever path you choose for your discovery-related data, it is imperative to ensure that the proper security is in place at every stage of your data lifecycle. Data security is more about the team you have driving it than it is about technology, though advanced technology is obviously a critical component. And it is all about protecting your company's revenue and reputation, today and in the future.