

Managing E-discovery Risks

Electronic data, also known as electronically stored information, or ESI, has been subject to discovery, which means it can be requested as evidence in court cases. Consequently companies must now consider electronic discovery early and often, in fact it is necessary to formulate electronic discovery (e-discovery) plans within 100 days of the beginning of a lawsuit.

While most corporate legal departments understand the gravity of discovery, many management teams and departments that create and manage ESI are not fully aware of their exposure. Lack of a proactive e-discovery process can lead to fines, unfavorable judgments and increased operating costs while also eroding corporate resources and damaging reputation.

What is ESI and E-Discovery?

Electronically stored information is a category of discoverable information separate from print documents, which includes both structured and unstructured data such as e-mails, instant message logs, Word documents, PowerPoint presentations, scanned documents and more. With the diffusion of social media, the amount of data created continues to increase exponentially, heightening e-discovery risks.

In financial investigations or litigation, e-discovery is the process of identifying, collecting, preserving, reviewing and producing relevant electronic data or documents as evidence. Determining what ESI is relevant is not simple due to the lack of precedence and established standards; however, it is undoubtedly critical to be able to quickly access the right ESI. While failing to produce all required ESI can be considered negligence, handing over too much

data could mean disclosing privileged competitive information and jeopardizing corporate strategy or product plans.

It is essential for organizations not only to recognize the risks associated with e-discovery, but also to proactively create appropriate procedures and plans for effective risk mitigation. The decision to handle the legal e-discovery process on a case-by-case basis results in costly, frantic overtime operations when a company finds itself involved in litigation, since demonstrating due diligence to the court means gathering and presenting all electronic evidence as soon as possible. Furthermore, lack of preparedness for e-discovery could be motivation for external parties to bring litigation in hopes of a settlement in place of the cost of e-discovery.

Many management teams and departments creating and managing ESI are not fully aware of their exposure should they be involved in litigation.

Evaluating Your Exposure

As with all risk management, it is important to establish the right balance between ample preparedness and excessive risk mitigation. E-discovery risks impact each organization to different degrees; a comprehensive gap

Provided by Brier Grieves Agency

Managing E-Discovery Risks

analysis can help you understand how much it affects yours. In assessing risk, focus on three main points:

- Identify the most likely e-discovery requests the company could receive.
- Quantify the cost of fines, judgments or compliance with e-discovery requests.
- Determine what steps are necessary to mitigate risk.

Internal Cooperation

A successful e-discovery strategy requires close cooperation between two generally disparate corporate functions, legal and IT. While communication between these groups is sometimes problematic – whether your legal counsel is in-house or external – both play an integral role in ensuring the organization can quickly produce the right ESI in the event of litigation. Other departments that create electronic data, including compliance, sales and marketing and corporate audit, should be involved in assessing risk and creating:

- An ESI request process that defines procedures for swift response
- An ESI information life cycle, examining data from its creation to its destruction
- An ESI preservation process
- A production process that identifies procedures and technologies used to satisfy requests for production.

Mitigating Risk

There are several steps organizations can take to minimize e-discovery exposures:

- Minimize the amount of unnecessary data created. A recklessly written piece of ESI could jeopardize your defense in court. As a general rule, the more data you create, the more exposures you face.
- Maintain and enforce a corporate policy regarding

style of communications.

- Limit the lifetime of all but essential data.

Insurance Coverage

All reasonable and necessary costs associated with an investigation, settlement and defense of a claim are generally covered as part of “loss” in a General Liability policy. In most cases, this has generally included the costs of discovery.

At the same time, many insurance policies require these costs to be previously approved in writing by the insurance carrier, which can be complicated or even impossible in the case of e-discovery. Carefully review your policy to determine its exact limits.

The insurance professionals at Brier Grieves Agency are here to work with you on all your risk management needs. Contact us today at (813) 876-4166 to discuss your strategy for managing your business risks.