SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Compliance Scorecard: New Rules for Your Electronically Stored Information – FRCP's eDiscovery Rules

William Plante

Originally Published in Security InfoWatch

October 2008

Compliance Scorecard: New Rules for Your Electronically Stored Information – FRCP's eDiscovery Rules

In 1996 I was involved in a lawsuit between my then-employer and another company. My employer had engaged outside counsel for the litigation, and I needed to send some documents their way. I thought e-mail would be the best method, so I called the outside counsel to ask for an appropriate e-mail address. To my bemusement, he replied, "We don't have e-mail here," and went on to explain that his office applications were a couple of versions behind. Hiding my surprise, I pointed out that perhaps his firm was a little behind the times and at some disadvantage. The lawyer's reply: "We lawyers are a bit slow to catch up, but we always manage to."

Indeed, the legal system has caught up with the information age with the amendments to the Federal Rules of Civil Procedure (FRCP) that became effective December 1, 2006. The new rules, often referred to as eDiscovery, address corporate electronically stored information (ESI) that may be subpoenaed under a civil action. The rules intend to redress both real and perceived problems involving ESI.

Security's Role Regarding ESI

While it is the primary domain of lawyers to take charge of legal matters, security executives should understand the principle points of the new rules and help lead necessary ESI change management within their corporations. Failing to abide by the new rules could lead to litigation sanctions that include fines, evidentiary exclusions, adverse jury instructions, increases in settlement/risk value of cases and potential obstruction of justice and criminal liability charges.

EDiscovery rules significantly affect the way in which counsel approaches the timing and scope of discovery—the process of locating and searching data for use in legal action. The rules also place new requirements on corporate IT resources to identify, describe, preserve, and produce corporate information. Companies should reexamine their information retention program and develop a defensible strategy that includes abiding

by the rules. Security leaders must become cognizant of the company's IT infrastructure and data archiving policy and programs, for data stored outside as well as within the United States.

While the FRCP was amended to address seven principle areas. let's briefly examine two of the more problematic and significant changes: Early Attention (Rule 26f) and Forms of Production (Rule 34).

Rules for Dealing with Data

The amendments require parties to meet early in the discovery process and address ESI issues that can include preservation, scope of discovery, costs and burdens, forms of production, privilege concerns, privacy/security/confidentiality, and accessibility. For the first time, parties are *required* to discuss ESI preservation and develop a discovery plan.

For example, many companies use third-party software to record and manage security incidents and investigation files. Upon request for discovery, how will that ESI be produced? In hard copy? Fine, but how will requests for the original source data be handled? True, the data is often in an open-architecture file format and may be accessed in a non-proprietary application. But then, how will redacted data be managed? If the data needs to be presented in court in the application in which it was originally created, does your company need to establish and maintain a legacy application library?

Data is becoming more prevalent across the enterprise in an increasing variety of forms: in e-mail, voice mail, instant message, on PDAs, local drives, shared drives and Web sites. Preparing for litigation implies that all of these new data repositories must be included in a data and records retention policy and program. Security executives involved in litigation could be called upon to describe their company's records retention policy and be knowledgeable of the systems used to manage their department's data. Lacking a credible program or failing to adhere to the policy is indefensible in court and may expose the company to legal risk.

There is good news for security executives. At times it may simply be too onerous and burdensome for a company to track down every instance of discoverable data. The rules recognize this and permit a process to request a limit to ESI discovery. However, the respondent must identify what information it is not able to provide, explain to both the court and the plaintiff why it cannot comply, and provide sufficient detail for the court to evaluate costs and the likelihood of finding responsive data.

For example, how would a company that had purchased the intellectual assets of another company handle un-catalogued ESI archived data now stored in a third-party facility? This situation is not uncommon. The costs to discover that information may be transferred from the respondent to the plaintiff in some cases. So in their own litigation planning process, plaintiffs will need to be prepared to pay for a respondent's production. Note that while the data may not be responsive, it must still be preserved.

How to Take Action

You can help your organization comply with these new rules by taking the following steps:

- Know where your ESI is on a global basis including data mapping, formats, local and off-site locations, media, archiving rules and retention policies.
- Be prepared to preserve all relevant information when a civil action is reasonably foreseeable.
- Know what is data is reasonably accessible, what is not and why.
- Know the cost to produce all data regardless of accessibility.
- Consider whether presenting legacy data will require legacy applications.
- The ability to argue information inaccessibility is related to costs and burden, so know your numbers.
- Know how you will redact privileged ESI data beforehand.

Despite all of our best efforts, discoverable and responsive data can be innocently lost. To avoid an accusation of evidence spoliation, ensure that your department adheres to the company's legal hold policy and keep your legal department informed of electronic discovery problems in a timely manner.

And it wouldn't hurt to discuss ESI with your general counsel over a coffee.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com