Seven Elements of Bulletproof Internal Investigations

Do it right, or suffer the legal consequences.

Most companies have a good deal of latitude in how they perform internal investigations of electronic information, but the driving question should always be: Will this investigation pass muster under the questioning of a judge and jury?

After recently testifying on the quality of an internal electronic investigation in an employment case, it struck me that IT, legal, and HR professionals needed a clear and practical course of action for their internal investigations of electronic data.

Poorly designed and inadequately executed internal investigations today will have significant costs down the road. It is crucial to think with the end in mind. So how can IT, legal, and HR professionals consistently work together on internal investigations that stand up to scrutiny later on, even years later? The acronym **PROTECT** highlights the most critical elements of any internal investigation of electronic information, including email, loose files, and databases.

Preservation—Preserve electronically stored information.
Range—What is the scope of the investigation?
Organization—Form and outline a plan in writing.
Team—Engage stakeholders.
Execution—Implement the plan.
Chain of Custody & Logs—Document the process.
Tools—What tools are needed to execute the plan?

Preservation is often considered a litigation task, but it is regularly mentioned in reference to internal investigations. The fact is, if electronic information is not properly preserved during the investigation, it will be hard for the investigation to be legitimate and to stand up under legal scrutiny. It must be a priority.

Issuing a hold and preserving electronic information do not have to prove difficult or expensive. Using the proper tools and organization (discussed later), a company can preserve information in a way that enables transparency into the process and validates the story they tell to the Court.

Range. The range or scope of an investigation involves the content to be searched and the method used to find it. The content includes the custodians, both human and computer, that will be searched. The Proportionality Triangle model (discussed here: www.quantumediscovery.com) elaborates on the scope of discovery negotiation in litigation, forming a rigorous approach in terms of weighing costs and time within the scope of an investigation.

Organization should be one of the earliest concerns in an internal investigation. Don't take this for granted. This is where the plan is established and is outlined. It is crucial for the stakeholders to accept the plan, and it is best to do this in writing.

Team. Who are the stakeholders, the team? Stakeholders are responsible for forming and executing the investigation. They must work as a team in order to successfully execute the investigation plan. Organizational silos can often preclude collaborative efforts and the result is an inefficient and ineffective investigation.

Each stakeholder's perspective and insight can raise the overall plausibility of the investigative plan. Judges and juries deeply appreciate common sense and the fruit of a collaborative approach.

Execution. It's one thing to plan, organize, and staff an investigation, but quite another to execute the plan. Internal investigations with great intentions can fail at the execution stage due to poor follow through. The stakeholders must appoint a project manager to keep everyone communicating and on task, all the way to the finish line.

Chain of Custody & Logs. Documenting the execution of the plan is probably one of the most overlooked, yet vital, elements of any investigation. Simultaneous documentation with the investigative acts is the best evidence that an organization has done its job well.

While formal chain of custody may not be required in every investigation, teams should be aware of proper procedures so that the documentation meets the needs of the specific investigation.

Often, logs are automatically generated by the system that is exporting the data. Almost every enterprise mail archiving system automatically generates logs that state the date, time and data that were exported from the system.

Tools. The investigation team needs to have the right tools for the task and they need to know how to use them. If the team is reviewing e-mail, it will need to demonstrate its thoroughness and its process. Not all search technologies are created equal. In some cases, a forensic-level search may be required; in others, simply using the internal capabilities of a tool such as Microsoft Outlook may be perfectly acceptable.

Bullet-Proof Your Investigations. In a world flooded with technology, internal investigations of electronically stored information are increasingly inevitable. Bulletproof your organization by utilizing PROTECT. It will reduce litigation costs and raise your team's confidence as they face the growing challenge of internal investigation. I

Jeff Johnson is a principal consultant for the Leawood office of Quantum Services.
P | 913.544.7408
E | jjohnson@quantumediscovery.com