APRIL 21, 2016

Legaltech® news

ONLINE

An ALM Publication

The E-Discovery Compliance 'Playbook' for In-House Counsel

Experts at the ACEDS 2016 E-Discovery provide the 7 elements of an effective e-discovery compliance program.

BY ERIN E. HARRISON

E-discovery and compliance experts assembled during a panel at the Association of Certified E-Discovery Specialists (ACEDS) Conference in midtown Manhattan to outline their collective, "foolproof" e-discovery compliance program for large organizations.

An effective program not only helps insulate a company and its officers and employees from criminal and civil fines, it can also protect its board of directors from personal liability and create a culture of a "good citizen corporation," explained Carole Basri, adjunct professor at Fordham Law, who co-authored the first e-discovery treatise for in-house counsel.

"If you don't have a good compliance program you are overseeing, you are liable or else it is a breach of fiduciary duty of care and loyalty … to protect the board members from personal liability," Basri explained.

A poorly constructed program can serve as a roadmap for prosecutors, damage morale and encourage fraud and unethical conduct to continue, she added.

Aldo Crusher for Legaltech News

The panel outlined ways an e-discovery corporate compliance department should be rolled out—based on a Part C risk assessment and seven additional elements, founded on the U.S. Sentencing Guidelines that were first introduced in November 1991 and were subsequently revised in November 2010.

"That is your shield," Basri said.

In other words: the difference between being proactive versus reactive.

"At the end of the day good e-discovery compliance is good information management compliance. That's really the essence of e-discovery, so the assessment is really the best place to start," explained Ken Rashbaum, a partner at Barton who advises multinational corporations and healthcare organizations in the areas of privacy, cyber-security and e-discovery. "The part you need to be thinking about is who is going to see this assessment later on. … hat you don't want is a regulator

or an adversary seeing your vulnerabilities."

Rashbaum said one of the mistakes organizations make is they bring in their assessments through another office other than the general counsel's, which isn't held to the same level of confidentiality.

"Retain counsel first, then have counsel retain the technical consultants," he said. "Because good e-discovery compliance is good information management compliance, you have to have an interdisciplinary group … it takes a village. It's not just IT's issue, it's everybody's issue."

Element 1: Establish Policies and Controls

First, it's important to keep policies up to date, to have a records retention policy and schedule, as well as policies for BYOD, mobile device use, social media, and litigation hold, noted Ignatius Grande, senior discovery attorney and director of practice support at Hughes Hubbard and Reed.

He gave one example companies will use to limit records retention, such as capping email storage at 2 gigabytes—which can have negative results.

"You have to think about whether it's really effective or not," he said. "Employees will always find a way around a policy if it's not something reasonable they can comply with."

Element 2: Exercise Effective Compliance and Ethics Oversight

Referring to the gap between the GC's office and the CIO, Basri said, "The energy and the process may be in technology, but the talent isn't there," which is why these policies need to lie in the compliance function, she said.

This is where reporting lines and compliance structure from the chief information officer to the chief compliance officer and general counsel need to be formally established. "The CIO should be at the C-suite level," Basri said.

Element 3: Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals

Legal departments also need to ensure that background checks happen for key e-discovery/information systems personnel, including criminal background checks, drug testing, credit reports and fingerprinting.

Element 4: Communicate and Educate/Element 5: Monitor and Audit Compliance and Ethics Programs

But what good is all of the above if policies and practices are not taught, and done so on a continuing basis?

"Training is not a set it and forget it, leave it alone," Rashbaum said.

After initial training, compliance training needs to include regular updates. "There are new threats every day, the laws are changing rapidly. This area is changing dramatically," Rashbaum said.

The panel also said a good e-discovery compliance program should be scalable; think about who the audience is, keep it simple, encourage questions, document attendance (as it provides defensibility), and record training for new employee orientation.

Element 6: Ensure Consistent Promotion of the Program

Auditing, monitoring, testing, surveillance and reporting in partnership with consultants and in-house/outside counsel also need to be established.

"Are you acting on them, are you continuously improving?" said Phil Cohen, shareholder and co-chair of the e-discovery practice at Greenberg Traurig.

Compliance needs to be encouraged from the top down to ensure policies are practiced, Basri added.

Element 7: Respond Appropriately to Incidents

Finally, in-house legal departments need to update their internal investigation protocols in order to appropriately respond to compliance incidents.

"The CIO should update the compliance program by reviewing the Part C risk assessment and each of the seven steps for effectiveness on a continual basis when a crisis occurs," Basri said. "Do an executive summary, the information should be condensed so you aren't exposing all data and making the company vulnerable."

Always report the results you get on a regular basis to board members and/or the audit committee on a quarterly, if not a monthly basis, she added.