AGENDA

A Financial Times Service

An E-Discovery Expert Gives Tips to Directors

By Tony Chapelle March 23, 2017

Jake Frazier leads the information governance and compliance department at FTI Technology, a part of the legal and IT firm, **FTI Consulting**. Frazier is an expert in electronic, or e-, discovery. He's also an attorney.

He recently spoke to *Agenda* about the board's role in mitigating lawsuits involving electronic records.

AGENDA: What is the law in this country on e-discovery or on electronic records management?

FRAZIER: Well, I can't give legal advice. Even though I'm an attorney, you should definitely seek counsel. But, in general, I think it's safe to say the law in e-discovery is that you have a proactive obligation to preserve information once you reasonably anticipate it may be relevant to future litigation. That means, if there's an incident where you think there's going to be a lawsuit, that's when that duty kicks in.

Conversely, the regulatory information management regulations are proactive and apply to types of information. So, for example, a regulator may say this type of customer communication must be kept for six years, or this type of communication for three years. And so forth.

AGENDA: Can you cite an example about a company at which e-discovery prevented a problem from escalating to involve regulators?

FRAZIER: So, we were working with a large global investment bank that was multi-national and had information strewn across several different continents. We were able to deploy technology that typically was used for e-discovery, called Stored IQ, in which we indexed the network, found all the unstructured information, and located pockets of information that had really high risk materials in it—compensation statements, material, non-public information, personal health information, the information that, if a hacker gets, it can really become very difficult for the firm.

We then used Ringtail, which is a visual analytic software, to drill down and determine really which information has the highest risk. From the combination of those tools, we were able to remediate tens of terabytes of information, either deleting it if there was no need to keep it anymore, or putting it in a proper repository that had more security.

AGENDA: Briefly describe the fortress versus the crown-jewels cyber security approaches to protecting corporate data, and which might be best for companies to use.

FRAZIER: so the question is how can we compare the fortress approach with the crown jewels approach? The fortress approach really is set up to say let's protect our network at the boundary, at the perimeter. Let's make sure nobody gets in, and then we don't have to worry about really what's inside our network.

The crown jewels approach, conversely, says people are going to get in and there also may be internal bad actors, as well, so let's make sure we find the most critical information with the highest risk and put that under lock and key, even within the network.

I would argue that the crown jewels approach is really the more realistic way. However, both can work together pretty well.

Copyright 2016, Money-Media Inc. All rights reserved. Redistributed with permission. Unauthorized copying or redistribution prohibited by law.