Legaltech news

Are E-Discovery, Cybersecurity, Two Sides of the Same Coin? BIA Says Yes

A new data breach security service from BIA demonstrates how e-discovery techniques and tools are being used to advance the cause of cybersecurity and make recovery after a breach more manageable.

by **Frank Ready** | January 14, 2019

BIA, an e-discovery and digital forensics software and services provider, has announced it has launched a new data breach discovery service applying e-discovery technology and practices towards the purpose of identifying information that may have been compromised during a system intrusion.

continued next page

The new initiative is a partnership between BIA and Reckoning Consulting Partners founder Ryan Bilbrey, and it will focus primarily on email and file servers that become exposed.

Beyond the business implications of opening up a new line of business, the latest venture from BIA also illustrates how e-discovery methodology has slowly started to creep into key gaps in cybersecurity and breach response. According to Lowndes shareholder Drew Sorrell, the two disciplines are linked by a fundamental paradox shared under the auspices of data governance.

"The correction between the two… is you need [data] to be easy to produce when you want it to be easy to produce, and then hard to be produced when you don't want it to be produced," said Sorrell.

In other words, you don't bury a treasure chest in the middle of a tropical island without making a map. A log that lists the names of people who have seen or had access to the map would also probably come in handy too.

The aftermath of a data breach is a little like that, only instead of gold doubloons, there tends to be significantly more personal identifying information and a patchwork of conflicting state regulations involved.

"If you know where your data is and what it is and what the definitions of the data are, when you have a data breach that helps you understand if that data that was taken, stolen, [or] lost triggers regulatory filing requirement and what the communications need to be to stakeholders," Sorrell said.

According to Bilbrey, there was a time when post-breach inventory reviews were typically comprised of a "blunt force" review of documents that eventually became more refined with the use of keyword searches. That approach also had its drawbacks, with a tendency to return data pools that were either too small or too wide for the task at hand.

"When we're looking at this pile of data we have to say, 'OK, what are we looking for?' It's defined by 50-plus different jurisdictions. Also are we talking about PII [personally identifiable information], are we talking about PHI (personal health information) which is governed by HIPAA?" Bilbrey said.

continued next page

The data breach discovery service at BIA will make use of some of the advanced analytics capabilities in the company's e-discovery tool kit with the goal of quickly singling out data that was compromised during a breach.

BIA's senior vice president of sales Mark MacDonald called the encroachment into cybersecurity territory a natural progression for e-discovery, which isn't to say that they're planning on relocating there permanently any time soon. This is more of an extension than a complete reinvention of purpose.

"We have the technology, we have tools, we have know-how and to be able to adapt that to what is really kind of a new evolution to how we can leverage our expertise to solve this big new problem that is really kind of bubbling under the surface," MacDonald said.

BIA isn't the only e-discovery company to be stretching its wings. Mary Mack, executive director of the Association of Certified E-Discovery Specialists (ACEDS), has noticed spillover between the marketing and sales of e-discovery and cybersecurity products.

"I think it's been percolating for a while. Our forensics community, many of them have moved into not only like fixed machine forensics or hard drives or things like that, [but] now they've moved into the cloud for forensics on cloud applications and network forensics, like the movement of data," Mack said.

If e-discovery professionals are looking to change pace with a security job, they are definitely out there. According to Mack, banks and retail businesses carry a heavy security profile and employ a lot of forensic personnel who will occasionally oversee e-discovery responses as well.

A downed website in the aftermath of a breach can translate into missed sales and other lost dollars, which means that cyber-evidence runs the risk of being trampled upon in the haste to get things up and running again. Professionals who can have a background in collecting and protecting evidence can be useful in those scenarios.

"I think our e-discovery companies and communities are now becoming more cyber-aware. They've got a seat the table," Mack said.

continued next page

Attorneys, meanwhile, can use an e-discovery background to help bolster their own value to clients when it comes time to advise on compliance proceedings.

"I understand how the usual corporation sets up their information system and I can help advise them based on my experience with e-discovery how to deal with some of the cybersecurity aspects too and vice versa," Sorrell said.

Frank Ready

Frank Ready is a reporter on the tech desk at ALM Media.
He can be reached at fready@alm.com.