METROPOLITAN
CORPORATE
COUNSEL®

JULY / AUGUST 2017 WWW.METROCORPCOUNSEL.COM

For Internal Investigations, Technology Is Playing Catch-Up With Technology

Companies focus on hackers and data, and sometimes overlook inside threats

***Scott Lefton** is a senior sales engineer at **AccessData**. Though he is not directly involved in conducting or supervising investigations, he spends a lot of time talking to the people who do, including chief security officers, people in HR and, of course, in-house lawyers. He listens to their "woes," he said, and suggests software designed to help them. His remarks have been edited for length and style.*

How does your product assist individuals and companies that need to do internal investigations or any investigations?

Scott Lefton: AccessData is focused on delivering solutions that investigative teams need to find critical data and evidence for their case. Our solutions help quickly identify, collect and analyze data in any type of investigation, from compliance to internal investigations and e-discovery. We're not focused on preventing a company from being hacked or preventing a data breach. Rather, if they want to know, for example, "Is this person doing something they shouldn't be on a company computer?" we are the go-to tool they use.

What are the top investigations regularly conducted by corporations today?

Lefton: We're seeing a lot of investigations for fraud, theft, IP theft, abuse of property, compliance and security. We conducted a survey last December that found organizations are conducting multiple investigations, almost daily, with the top investigation types being focused primarily on compliance and data security.

You've got hundreds of ways people can try to covertly chat, and you've got hundreds of ways people can try to covertly hide data.

How have investigations changed over the last few years?

Lefton: The volume of data has increased so much, so you've got more places to look. People have more intellectual property than they've ever had before. It's out on the cloud, mobile devices, tablets, and there's just so much of it. It's become much more difficult, and the need for these types of investigations has risen as a result. One of the concerns that we hear about now is intellectual property theft. It is people taking stuff when they leave. Because that is such valuable information to the company – trade secret information, client contacts and things like that. And when people leave, a good portion of that goes out the door. A lot of that is what's driving this change in how companies are performing investigations. And we're seeing a lot more investigations conducted proactively to ensure companies are compliant in protecting their data and their customers' data.

Any other big factors driving this change?

Lefton: Regulations – especially in finance and health care. As regulatory agencies put more guidelines in place and penalties for noncompliance, organizations are increasing efforts to ensure that their systems, processes, and data privacy and protection measures are in order. Also the increased attention on data privacy and security is impacting investigations in a big way. You don't want your name in the news as the next company to have their data compromised. High-profile breaches or incidents like ABB, Inc., come to mind. There are some employee theft cases where $100 million goes missing, and that really affects the entire life of the company, and it can affect your annual report. Especially for smaller companies. Sixty percent of small companies that suffer a breach go out of business within six months. It's hard to come back from the financial and brand impact an incident can have on a company. So that's why so many are doing more to proactively ensure they know where their data is located, and they have the tools in place to quickly investigate and remediate a potential threat.

What are some of the challenges corporations face in managing investigations across the entire enterprise?

Lefton: There are three challenges we're hearing. It's a lack of collaboration. Not having the tools to get to the data that they need. And then just the proliferation of data sources. There's so much out there now: Dropbox, OneDrive, there's stuff in the cloud. There are new chatting applications, and those

Scott Lefton *is the principal sales engineer and customer engagement representative at AccessData. In this role, he consults daily with prospects and customers to understand the current trends and challenges they face in the areas of digital forensics, investigations and e-discovery, and he educates clients on how to effectively leverage software solutions to better manage their investigative workflows. Prior to joining AccessData in 2010, Lefton held roles as an in-house IT administrator and litigation support specialist for Epstein Turner and Song. He can be reached at slefton@accessdata.com.*

ACCESSDATA®

are definitely some of the top challenges.

The collaboration piece is a disjointed process. In any investigation, imagine how critical time is. And if you have a manual investigation process, HR has to call the general counsel, get approval, write out an approval request and go take that request to IT. And then *they* have to get the proper people in line to get to that data. Maybe they don't even have tools to get to that data, and it's even more of a manual process to go out and have to collect everything out of that site and then try to make sense of it. In the interim, you've lost the data.

What they need is a platform where HR, legal, compliance, audit – all of these people – can work together. "Here's my request: I need these assets searched; I need them done today." You really need to have better visibility into your network, and we do that by, for example, providing connectors into these various repositories. Technology changes so fast. You have new software being installed and it's highly structured data that's on the endpoints, and technology moves a lot faster than our ability to learn how to collect it in a way that easily can be viewed by an attorney or that can be in accordance with the Federal Rules of Civil Procedure (FRCP). It's really hard to subpoena a highly structured data repository. It's not a file cabinet with a file in it anymore.

It's funny because for years I've been hearing about the law playing catch-up with technology. But now you're saying that technology is playing catch-up with technology.

Lefton: You can look at it that way. Our job gets exponentially harder every day. Think about just this fact: There's well over a million apps in both the Google and iTunes stores. You've got hundreds of ways people can try to covertly chat, and you've got hundreds of ways people can try to covertly hide data. And you've got mobile device makers that come out with a new operating system every other month.

You mentioned data breaches. We hear a lot about them. We hear about hackers sitting on the couch, we hear about North Korea, Russia, China, and how capable they are of hacking into corporations, government agencies, etc. Do you think these are the biggest threats facing companies today?

Lefton: It is a massive threat, but one of the bigger threats that I think is overlooked, and where we all are putting our heads in the sand, is really the internal threat. I've been calling it "the Snowden effect." In corporate America, it's your IP theft or it's just people being careless, and that is another big problem. We email stuff without it being encrypted. We have data on a laptop that we shouldn't have, and it gets stolen. A lot of times people will be careless in the sense that they might install an unapproved application that's vulnerable.

What I like to tell customers is that by putting these tools in place, you are arming yourself in the event an investigation arises and you will be able to respond quickly. When I started, people were pretty confident in their ability to keep bad actors out. And now everybody realizes it's an inevitability. There's actually an assumption that you're already breached. We see more organizations taking steps to try to protect those assets from both internal and external threats.

You talked about corporate espionage. How much of that is going on? Are companies routinely spying on each other?

Lefton: Finding the proof of it is the hard part, but definitely it is out there. There is no doubt about it. One thing that comes to mind is going to seem a little silly, but you have a recent incident with a scout for a Major League Baseball team who pleaded guilty to two and half years worth of corporate espionage; his employer was fined $2 million dollars, and he was sentenced to four years in federal prison. This case involved a somewhat careless password policy regarding a database. Obviously, you have a bad actor. But then you also have IT people negligent in not following what in hindsight should have been a better password policy for that database. IT should always consider changing passwords regularly and making sure remote system access is disabled when employees depart.

What role or roles should in-house lawyers be playing in terms of protecting the company? And what role should they play when internal investigations are called for?

Lefton: They need to be ahead of issues and on top of them when they arrive. You don't want to be reacting. That's going to be where you've got a problem. You need to be, obviously, setting the right policy and having a clear process that you adhere to consistently when these things arise. You can't shrug off what might be a low-level alert. You really have to be vigilant on all matters. That would be my advice for the general counsel.

What advice would you give the company as a whole to help ensure that they're conducting more thorough, efficient internal investigations?

Lefton: Ensure that you have visibility into where your data sits across the enterprise, and the ability to quickly collaborate with necessary teams to help simplify the process of managing complex investigations. You have to record and document everything and have a repeatable process, so if you do get questioned, you have an audit trail of what was searched, when was it searched, what was located, what was not located. Also, look for integrated tools that help to connect the phases of the investigative workflow and minimize data movement to reduce cost and risk. Every time data gets passed between tools, you're risking possible data corruption or spoliation that could undermine your investigation and end up having evidence dismissed in court.