LAW.COM
An ALM Website
May 31, 2016

Preparing For the Breach: A Look Into Essential Cyber IG Practices

By Ricci Dipshan

It's a situation every attorney dreads: You are sitting at your computer on what seems like a normal day, when suddenly the screen goes blank, replaced by a notice that your files are being held ransom or your most valuable data has been stolen out of your system.

In the immediate aftershock, myriad questions can run through your mind. But none is perhaps more important, more pressing, than—what's next?

The answer, explains Jake Frazier, senior managing director at FTI Consulting, depends largely on what has come before.

"Pretty much what I see is that the work you do before the breach is most everything you can rely on once the breach happens. Once the breach happens, it's really difficult to maneuver," explains Frazier.

Preparing for the question of "what's next?" ahead of time can at first seem like common sense, but it is too easy to underestimate the complexities and handicaps posed by an actual breach.

"We do these what we call table-top exercises, where basically we'll come in and it's like a war game simulation," Frazier says. "And we'll say we just learned the system has been comprised or this ransomware is happening, trying to encrypt things, so what do we do?"

Often when we work with clients who maybe have underestimated the difficultly of what would happen. They might say, 'OK, first I'm going to email so and so,' and we say 'No, you can't email, email's offline—now what?' And then we just get blank stares and people immediately say, 'OK, we don't know what to do."

The problem, Frazier explains, is that as cyberthreats have evolved, information governance programs have stayed the same.

"What information security historically has done was focus on the fortress approach—how do we put walls up to keep people out. So that would be proxies, firewalls,

encryption security event information management systems, etc.," he says. "But as we've seen for the most part, that is not sufficient, people will get in one way or another, so the problem is once they get in through a backdoor or over the fortress wall, then they can just run amok."

Triage and Mirage

But this can only happen if data is out in the open for cyberattacks to exploit. Paramount to any data breach preparation is the golden rule of any information governance program: knowing where sensitive data resides. Yet this, of course, is much easier said than done.

"The key to a good IG policy," explains Farid Vij, lead information governance specialist at ZL Technologies, "is having a complete understanding of your data at all times so that you can be in a proactive position during a data breach, which is the biggest challenge for enterprises today. There's simply too much data."

Thankfully, however, data breach preparedness doesn't require an all-or-nothing approach.

"This isn't about creating a basic data map; today, we have to get down to the content level of the document to identify things like personally identifiable information, personal health information, and payment card information."

What this comes down to is extracting the most sensitive information among the daily network traffic and regularly created or obtained files, and placing them in repositories with security provisions and data backup options.

"That's definitely one of our most popular engagements right now," Frazier says. He adds that in previous client engagements, "we were looking at the transactional data that had to do with account setup, and account numbers, things like that," in which to create "a tiered approach where critical, private data goes off to other repositories that are much more secure, and your transactional data stays behind."

While these repositories can have the usual layers of security such as "requiring stronger passwords and dual factor authentication," Frazier notes that they can also provide "data masking."

This entails scrambling data to create invalid credit card or Social Security numbers. These work as decoys to cyberattackers, while allowing developers to build and test apps using the information as well.

Careful Sharing

Equally as important and valuable in data breach preparedness is controlling user access rights to these repositories.

"The key challenge with these breaches is often figuring out what data has actually been compromised and ironically, most organizations don't know where to start," says Vij. "Take Sony, for example. The majority of the risk and cost associated with the cyberattack was not the data that was directly hacked, but all the data that the hackers got access to as a result of securing passwords and confidential information."

But as Terrence Coan, senior director in the Law Firm Advisory practice at HBR Consulting explains, when it comes to delegating file access, the legal industry is ahead of the game.

"Law firms are obviously very organized around client and matter, so there's an implied hierarchy; if I know who is authorized to access a client matter, then when I file documents into the system by that client and matter, the system applies the appropriate security to the matter team or to those who have reason or right to know.

Yet like any company in 21st century, law firms are also at the mercy of file shares, which while increasing employee efficiency and collaboration, potentially leave valuable data unsecured and accessible to all.

Frazier calls file shares "one of the least secure areas in a network, because it doesn't have really rigid permissions. There are a lot of permission profiles on file shares that we see called 'everyone,' which means anyone who is in the network can just navigate to the file shares and have access."

He adds that such areas have been used as "dumping grounds," where in a recent engagement with a client, Frazier and his team found "a few petabytes of data." Such fileshares, he notes, can include "HR records, compensation statements, customer records, and permission forms to set

up direct deposits with routing numbers and account numbers, and all kinds of really risky data."

But like a potentially unsecure database, Coan says, file shares can be an easy fix. "We may lock those down and prevent people from filing to those locations going forward. While we may not delete the materials currently filed there immediately, we tell users that these locations are not an appropriate place to file materials, and if they do file materials on a network file share, we are going to purge them automatically within a defined period of time."

Of Man or Machine?

While breach preparedness seems simple in theory, execution may be a whole other story.

"On almost every engagement, I'm asked by the clients, do you believe in a human approach where users are going to classify the data and put it in the right spot, or do you believe in a more automated scanning approach? And my answer is always yes — both," Frazier says. "So it's always a belt and suspenders approach that works best."

Using scanning and AI technology even on computers not connected to the network, he adds, can allow companies to find, move or lock down critical files.

"But in the end," says Coan, "it often comes down to users having to interact with the data to have context to what the data is saying. If they have personal experience with it, they can then make an informed decision where it goes."

Admittedly, it can be difficult to trust employees — after all, the rise of shadow IT, fileshares, and poor digital hygiene have made insider threats more probable than external breaches.

But employees will always remain central to breach preparedness and must be kept up to speed through constant training, Coan advises.

"It's always more going to be a situation that they don't train enough. And that's because they can't or don't get the budget to do the necessary training and education. … There has to be ongoing and routine training, there needs to be training for new employees who are brought into the organization, and there has to be refresher training of the entire employee population on some periodic basis. For example, every year or every couple of years, just to remind people about why this is important, why we are doing it and what we are expecting people to do."

And more important, Fraizer notes, training works: "We find ultimately that through education and awareness, people do get better about how or when they use shadow IT such as cloud storage, or that they are more rigorous around defining who can access it and making sure that there are controls to minimize unrestricted access by somebody who shouldn't have it."

When developing a data breach preparedness plan, he adds, companies must also be careful not to set employees up for failure by encouraging them towards shadow IT or other risky tech behavior.

"In a breach, when systems start getting shut down, knowledge workers have pressure to get their jobs done. If all of a sudden emails are not working because there's a breach, it's not unlikely that you'll see users using Yahoo, Gmail, Dropbox, Google Drive and really anything they can get their hands on to continue to do their job."

Companies, Frazier says, need to let "users know if there's a breach, don't go using other systems, and your manager will take into account any lost time due to this breach —an escape valve, so that the day-to-day pressure is alleviated a little bit while the breach remediation is happening."