Dial M for Malicious

Companies face new vulnerabilities as hackers push the envelope

MCC interviews ***Brookes Taney****, vice president of* ***Data Breach Solutions*** *at* ***Epiq Systems****. He can be reached at* ***btaney@epiqsystems.com.***

MCC: Please start with your perspective on the cyber-breach landscape. We understand there's been a recent shift, particularly after the Sony breach.

Taney: Over the last 5-10 years, companies have been breached on a fairly consistent basis, with hackers interested in data for the sake of profit: Typical targets were names, addresses and Social Security numbers (SSNs), as well as credit card and healthcare information. With this information they could commit healthcare fraud or sell the medical information and Social Security numbers online.

The recent Sony Pictures breach changed the game. The attack targeted atypical information, like employee salaries, personal emails between executives and celebrities, and creative themes and other details about upcoming films – in other words, data that was not of much benefit except for the purpose of malicious exploitation.

Today, the thought among hackers is that there is a hierarchy, really a contest of sorts, with the highest classification level based on the "how-far-can-you-go" concept. In order to make the A-list, hackers now must exceed their past accomplishments; this current dynamic of malicious intent creates new vulnerabilities for corporations.

MCC: Please talk through the components of an effective breach response plan. What differentiates the services of Epiq Systems?

Taney: In the past, a breach response lifecycle began with the discovery of an incident, meaning some form of intrusion, though its extent and any specifics as to what information was taken remain unknown. The next calls are often to the insurance company, if a policy is in place, and to outside counsel. After that, a good response plan will call for entering into a contract with an investigation company, which will find out what type of information was compromised, when it was taken and how quickly the leak can be stopped. At this point, a determination can be made as to whether the incident meets a breach requirement by state law, which will trigger the need for notification services.

The breach landscape is, however, changing rapidly, and savvy legal and IT teams are looking for more than just one-off breach responses. Where Epiq is truly different is in that we are the only company that handles a breach from detection through to any resulting litigation – and even offers adjacent services, such as proactive information governance, to help both reduce the risk of a data breach, and minimize the damage if one does occur. And, after a data breach, we provide services to efficiently and effectively handle any litigation that arises from the breach, such as a class action litigation – including electronic discovery services, class action notification and administration, forensics and collections, document review and processing and production.

Epiq manages all aspects of the security breach process under one roof, including data handling, data research, forms, noticing and contact center setup and support. This gives you a single point of contact during the entire process, and enables us to drive effective data breach response by eliminating the inefficiencies introduced by cross-vendor coordination.

To make the A-list, hackers must exceed their past malevolence.

—Brookes Taney

In terms of data breach notification services, Epiq will enter the process five to 10 days before notifications must be sent, and we handle multiple notice types, depending on state regulations (Massachusetts requires a letter, New York doesn't, and so forth) and any additional considerations for recipients who are minors or deceased. We take in and process data in multiple steps, including deduplication and running it against the national change of address database, which updates addresses as needed, minimizing returned mail. Where allowed, our email capabilities can be a huge cost saver versus paper notification.

Taking a step back to answer your second question, the breach response process is very similar to class action administration, which Epiq has been handling for 20 years. We came into the cyber world with a fully operational infrastructure, which gave us a competitive advantage out of the gate and continues to give clients a welcome leg up as our systems and call centers are always up and running. From a capacity and process standpoint, we have long been in the business of processing data – intake and deduplication, among other functions – therefore, unlike many competitors, we're not scrambling to develop capabilities to meet a more recent demand for breach response services.

So throughout the breach response process and depending on the size of the engagement, we can seamlessly ramp up call centers from various locations – Portland, New York, Washington, D.C., Phoenix and Dallas – and train agents to provide professional responses to the specific 30-40 questions we anticipate. We have built a standard service level agreement (SLA) with respect to our response time: 90 percent of calls are answered within three minutes. Again, the big advantage for Epiq is our existing infrastructure: we have enough agents trained in multiple matters (breaches, class actions and bankruptcy settlements) and can allocate each day's work depending on which engagement is busier that day – so we can meet those SLAs.

Many of our competitors don't have SLAs, but we know that response time and quality are critical. One of the best ways to eliminate class action lawsuits after a data breach is to make sure that all forms of notification are promptly mailed and provide as detailed an explanation as they legally can. When recipients have all their questions answered in a timely fashion, and clearly understand what steps are being taken to mitigate and remediate the problem, they are less likely to open up the yellow pages and find a plaintiff's attorney to file a lawsuit.

So we take a lot of pride in our SLAs: swift and accurate notifications, prompt phone service and creating a good experience for everyone in the wake of an unfortunate incident that affects both a company and its consumers.

MCC: In the event of subsequent litigation, what additional support is needed?

Taney: As the breach runs through its life cycle, litigation may arise – depending on factors such as the size of the breach, the company and consumers involved, the nature and scope of what was taken or compromised – and that's when our class action and eDiscovery groups can seamlessly come into play.

As an example, our eDiscovery group has helped many large retail companies collect, process and review electronic documents and communications during litigations. As part of the discovery process, we perform automated searches on collected data to determine relevance to the case at hand, as well as to showcase compliance with federal and local statutory requirements for protecting data. We will look for proof that the company had systems in place to avoid a breach in the first instance, such as systems that meet standards for financial data protections as set forth by the PCI Data Security Standard (PCI DSS). We bolster the company's defense by finding stated corporate policies as to data loss prevention and any associated auditing procedures. We look for evidence that the company had no advance knowledge of potential threats and, post-breach, responded with timely and adequate notice.

Document review in data breach litigations can be very exhaustive, with large bodies of documents needing to be reviewed by trained experts for relevance in very short periods of time. To that end, Epiq offers a complete outsourced solution for document review – with secure facilities, tested training methodologies and review workflows and the ability to staff up for very large projects extremely quickly.

If and when the breach turns into a class action lawsuit, our class action administration group in Portland, Oregon handles the notifications, reviewing the claim information and distributing funds to the members. Taking as an example the recent Target consumer class action settlement for $10 million, we would leverage all possible methods to notify class members by mail, substitute notice (magazines, newspapers, websites, etc.) – and then mail out claim forms, which class members complete and submit within a certain timeframe. We then intake the claim forms, determine the eligible payout to each authorized class member and make the actual payments.

We have handled class actions for breach matters that involved T.J.Maxx, Countrywide Financial, Certegy Check Services, Heartland Payment Systems and the Veterans Administration, processing millions upon millions of security breach notices and paying out commensurate millions for settlements.

MCC: There is certainly plenty of press about the blockbuster data breaches. What about small-scale matters? Does outsourcing still make sense?

Taney: From a response standpoint, there is no breach too small for services like ours. If you're facing a 3,000-member breach, for, say, a dentist's office, we offer very low setup fees. In all events, there is something to be said for not placing the burdens of a breach response on employees who otherwise would be carrying on with daily activities. Handling mass mailings and breach-related phone calls are not only a business distraction, they are bad for morale. While we can handle very large capacities, most breaches involve 30,000 or fewer members, and some have gone as low as 50 members.