Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

'Tis The Season ... For Data Breaches And Data Analytics

Law360, New York (November 24, 2014, 10:45 AM ET) --

Mike Kheyfets

As the calendar turns toward Thanksgiving and on to Christmas, the holiday season officially begins. The familiar signs of the season abound — caroling, Christmas trees and Hanukah menorahs, Black Friday mall runs, eggnog and countless family gatherings to name a few. Unfortunately, recent holidays have also been marked by a less happy occurrence, particularly for retail establishments — holiday season data breaches.

Last holiday season saw some of the biggest and costliest data breaches in the retail industry's history,[1] including credit card or personal information from more than 100 million Target Corp. customers,[2] over 1.1 million credit and debit cards from Neiman Marcus Group[3] and 3 million payment cards from Michaels Stores Inc.[4] With optimistic forecasts for spending during the coming holiday season,[5] retailers will no doubt once again be in hackers' crosshairs in the coming month.

When a data breach occurs, most firms employ a multifaceted approach, relying on both internal and external resources to manage the incident. For example risk professionals, attorneys, information technology personnel, forensic computing experts, and sometimes law enforcement may all become involved. At the time of a breach, there are a number of competing concerns and interests, all of which must be addressed, often in relatively short time frames.

The International Association of Privacy Professionals provides guidance as to four fundamentals to incident management in the event of a breach — (1) determination of whether a breach has occurred, (2) containment and analysis of the incident, (3) notification of affected parties, and (4) implementation of effective follow-up methods.[6]

Implementation of data analytics — an important but sometimes underutilized tool — can assist in all phases of incident management. Broadly speaking, data analytics involves the compilation, preparation, synthesis and analysis of complex (and often voluminous) data sets to provide rigorous answers or contextual information to a range of business problems. Useful data analytics rely on a combination of careful framing of the relevant questions at issue, sound data management techniques and robust statistical analyses.

What Can Data Analytics Offer in the Context of a Large-Scale Corporate Data Breach?

In fact, there are a number of ways in which both a firm's breached and unbreached data systems, as well as data from external sources can be used in the course of the incident management lifecycle laid out by the IAPP.

Data analytics experts — working together with computer forensic professionals who have identified potential sources of threats — can use data sets kept in the ordinary course of the firm's operations to identify unique patterns and investigate the key questions relating to the timing, scope, and magnitude of a breach.

Think of it like a crime scene investigation: On the scene, investigators identify and collect relevant evidence, but analysts at the "crime lab" help piece together what happened and determine what the evidence suggests. For example, login entries (both successful and failed) contained in security logs may be analyzed for anomalies in order to identify when and how the intrusion occurred. Likewise, large volumes of data contained in system and application logs may hold the answers to questions regarding the breach.

Once a breach has been contained and mapped out, data analytics can be further utilized to ultimately frame the full extent of the breach. Data management techniques can be used to link information across tables within an affected data system, and even across multiple — disparate but potentially affected — systems. For example, analysis of affected system components can identify what personally identifiable information — if any — was compromised, or whether only certain portions (e.g., credit cards but not debit cards) were. Based on these linkages, reports can then be run to both identify the universe of the affected data and to develop documentation of the incident for future reference.

Additionally, data analytics can meaningfully inform the notification phase of the incident management process. Because both the notification process itself — as well as any ancillary costs, such as providing credit monitoring for affected customers — can be very costly, it is important that the appropriate and accurate set of affected individuals be identified. Here, the breached data sets can be cross-referenced against other internal and external data sources to determine, for example, which accounts are inactive/expired or contain outdated information.

Because legal requirements relating to notification may vary by industry and state, data analytics, under the guidance of legal counsel, can also be used to construct notification lists that reflect the relevant notification statutes. However, this process is not as straight forward as it might seem, particularly given the immediacy required in the post-breach timeframe. Because transactional data (such as that containing records about individual sales) is rarely audited for quality and completeness after it is recorded in a database, developing comprehensive notification lists — together with the information that needs to be conveyed to customers — under tight deadlines may require retention of data analytics professionals. The notification lists compiled during this stage may also become valuable as a tool for valuing risk and legal exposure in instances where a lawsuit is brought against the breached firm.

Given the Potential Usefulness of Data Breach Analytics, Why Aren't Such Tools Used More Widely?

The reality is that while firms increasingly have data breach response plans and teams in place (73 percent of firms in 2014, compared to 61 percent in 2013)[7] and many have privacy and data protection awareness programs (54 percent of firms in 2014, compared to 44 percent in 2013),[8] the majority of executives do not believe that their organization understands what needs to be done following a material data breach.[9] Accordingly, there are a number of reasons why data analytics has not yet become a commonplace tool in data breach response.

- First, at the time of a breach, the isolation of key data sets, and even the extent to which data sets are kept in the ordinary course of business can vary widely across systems and firms. Certain system generated data sets may only be kept for short windows — potentially limiting their use for post-breach analyses.[10]

- Second, many data sets are not ready for data analytics. They must be cleaned and prepared for use quickly if they can be effectively implemented in a post-breach analysis.

- Third, given the rapid timetable for a response and urgency of the various facets of compliance occurring at the time of a breach, the value of data analytics is sometimes ignored in favor of expediency.

- Finally, given the heightened concerns about security, specifically at the time of — and immediately following — a breach, data analytics must be done in a secure location, most often on-site.

As the prevalence of data breaches — and the associated cost to firms — continues to grow, the ability to conduct rapid and effective response will remain of paramount importance to chief risk officers, legal teams, compliance officers, and IT professionals. Given the critical nature of the task, stakeholders must utilize all of the tools at their disposal to deal with the consequences and subsequent prevention of data breaches. Data analytics can be a useful addition to this tool box, requiring critical thinking and appreciation of the comprehensive analysis at hand.

—By Mike Kheyfets, Matt Milner and John Johnson, Edgeworth Economics LLC

Mike Kheyfets, Matt Milner and John Johnson are partners in Edgeworth Economics' Washington, D.C., office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Some of the largest retail breaches in prior years — such as the 2007 theft of over 45 million credit and debit card numbers from TJX — also took place during the holiday season. (See e.g., http://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html)

[2] Harris, Elizabeth A., and Nicole Perlroth. “For Target, the Breach Numbers Grow.” The New York Times, 10 Jan. 2014. (available at http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html)

[3] Harris, Elizabeth A., Nicole Perlroth, and Nathaniel Popper. “Neiman Marcus Data Breach Worse Than First Said.” The New York Times, 23 Jan. 2014. (available at http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html)

[4] Harris, Elizabeth A. “Michaels Stores’ Breach Involved 3 Million Customers.” The New York Times, 18 Apr. 2014. (available at http://www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html)

[5] “Optimism Shines as National Retail Federation Forecasts Holiday Sales to Increase 4.1%.” National Retail Federation. 7 Oct. 2014. (available at https://nrf.com/media/press-releases/optimism-shines-national-retail-federation-forecasts-holiday-sales-increase-41)

[6] Swire, Peter P., and Kenesa Ahmad., U.S. Private Sector Privacy, Law and Practice for Information Privacy Professionals, 2012. pp. 118-119.

[7] Ponemon Institute LLC, Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach, September 2014, p. 1. (Available at http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf)

[8] Ibid.

[9] Id., p. 3.

[10] Hackers can also affect the ability to perform certain forensic analyses after the breach. For example, during the recent breach at J.P. Morgan Chase, hackers deleted many of the log files that tracked their movements through the bank’s network. (See http://www.nasdaq.com/article/jp-morgan-found-hackers-after-finding-breach-of-race-website--update-20141031-00640)