ALSTON&BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

JULY 7, 2016

Six Myths of Breach Response

***by** Jim Harvey*

Data breach has, unfortunately, become a fact of life. Practically every corporation has experienced some sort of security incident, although most have avoided (to their knowledge) significant network intrusions and loss or destruction of data on the scale of Sony, Target and the Office of Personnel Management. While the number of major security events has exploded and the space has experienced growth in the professional ranks, there remain a number of myths and common challenges in breach response.

"If We Have to Notify Customers, It Will Be the End of Us"

In so many instances, the issue of whether to notify customers drives significant portions of the conversation in breach response. Companies are rightfully concerned about notifying customers of a breach; however, millions of individuals in the United States have received notifications of multiple breaches, and many of those individuals have had one or more payment cards replaced by their issuer in recent memory.

Notwithstanding the near ubiquity of consumers having already received multiple breach notifications, executives are often myopically focused on the issue of whether to notify individuals after a breach. In some cases, this concern is well placed due to the company's relationships with its customers, its regulatory posture or other valid reasons, but often these concerns arise out of unfounded fears that their company will be unfairly or disproportionately criticized or penalized for providing notification.

Perhaps one of the worst mistakes a company can make in response to a breach would be to delay notification or, worse yet, stretch the analysis in order to avoid notifying their customers of a breach. While the decision to notify customers should not be undertaken lightly or assumed to be a non-event, notification should not be artificially avoided at the expense of the integrity of the investigation and response.

"Notifying Consumers Is No Big Deal – It Happens All the Time"

While some may have an irrational fear of notifying customers of breaches, others suffer from a bias in the opposite direction. The other end of the spectrum holds the view that breach notification has no negative consequences because consumer notifications are so commonly encountered. This similarly extreme view fails to consider the full

range of legal consequences of notifying third parties of a security incident; companies should bear in mind that any public notice of a breach runs the risk of attracting the attention of state authorities (from the attorney general to various departments of consumer affairs), plaintiffs' lawyers, federal regulators and more (depending on the company and the industry).

Of course, there are many disclosure nuances on both sides of the equation that have to be taken into account; however, succumbing to the myth that either notification is the end of the world or that notification does not matter whatsoever can lead to unnatural and surprisingly negative results. An experienced, evenhanded and knowing analysis of the facts and the law should make the decision of whether, when and how to notify relatively easy. That decision may be uncomfortable for any number of reasons, but it should not be undertaken with a particular bias in one direction or the other.

"We Only Need an Email Header to Protect Everything Under the Attorney-Client Privilege"

The prevailing paradigm in breach response is to have a forensic investigator hired either by internal or external counsel and have the investigation conducted under the attorney-client privilege. This is absolutely appropriate as it is a legal investigation conducted with the assistance of an expert in order to render legal advice. The results of that investigation allow counsel to better assess the incident and the resulting legal and business obligations. That said, some involved in these investigations often mistakenly labor under the impression that anything they do within shouting distance of a lawyer constitutes legal advice to which the privilege will attach. Perhaps the most common mistake is the belief that anything labeled "Attorney-Client Privileged" will be protected by the privilege and therefore immune to production to adversaries, which is an overly simplistic view and quite possibly completely wrong.

Successfully maintaining the privilege can be very difficult to do in a dynamic, crisis-driven breach response, and it should not be left to amateurs. Counsel and their clients are well advised to understand and implement the fundamentals of the attorney-client privilege as they embark on a complex breach response; failure to do so may subject the client to allegations that wide swaths of communications that should have been protected by the privilege are nonprivileged and discoverable. Adversaries that seem to pop out of the woodwork after a significant breach are increasingly arguing that the results of an investigation (even one undertaken at the direction of counsel) are facts that are not privileged. Moreover, those same adversaries are arguing that efforts were remedial in nature, rather than investigative, and therefore not subject to the privilege. It is important to remember that there is much more to the attorney-client privilege than a simple email header; failure to bear this in mind may land the company in the middle of an unintended and perhaps avoidable fight over what should have been privileged.

"I Will Just Use My Existing Counsel/PR Firm for This Breach"

Many professional firms are trying to enter the incident response space because of the significant and sizable market opportunity that it represents. In-house counsel should familiarize themselves with the true experience of those they seek to hire. Lawyers who are solely focused on consumer notification obligations operate at the risk of tunnel vision that could cause them to miss many other legitimate issues arising in a breach, including law enforcement, securities disclosure obligations, insurance coverage, litigation preparedness and the entire panoply of legal issues that result from a security incident. Of course, pure specialists in any one of these subject-matter areas may be helpful when circumstances dictate, but primary counsel for the matter should have appropriate familiarity with each of these areas in the context of a breach. This allows them to spot the issues in advance and further allows them to consult subject-matter specialists when appropriate. Similarly, outside counsel who have a longstanding relationship with a

client, but who have never responded to a large breach, have the advantage of knowing the client's business but are unable to respond with the legal breadth and depth that is required in the live-fire exercise that ensues in a major network intrusion. Indeed, the Department of Justice has recognized the issue and recommends hiring lawyers with experience in breach matters: *Best Practices for Victim Response and Reporting of Cyber Incidents, v. 1, April 2015*.

Many companies also have established relationships with public relations / crisis management firms. Public relations plays a critical role in breach response, assisting companies in monitoring and managing the 24-hour news cycle across all forms of media after a breach. If the company's public relations or crisis management firm does not have significant experience in security breach response, they run the risk of performing activities that have (for those experienced in the space) become almost passé. Knowing the powerful influencers in the security- and privacy-oriented social media world, how to deal with them and their typical tactics is an absolutely critical role. As is the case with outside counsel, companies run a significant risk of relying on a solid, historical PR relationship that unfortunately lacks appropriate expertise and experience in the breach response context, perhaps diminishing the effectiveness of their overall response.

"We Should Just Use Our Existing Security Firm – They Know Our Systems"

As is the case with counsel and public relations firms, incident responders and forensic investigators who are experienced in these matters can be the difference between a fast and effective breach response and a slow, ineffective response. Just because a company has a relationship with a particular security firm does not mean that that security firm is best situated to handle some or all of an incident response. A company should consider whether its security firm has true investigative response experience or whether its experience is better suited to creating and implementing security solutions. In fact, those security solutions and a particular firm's prior role at the company may create a conflict of interest—real, potential or perceived—that might hinder its ability to investigate what led to the breach and what is required to appropriately address the security vulnerability.

It should also be noted that not all forensic incident responders bring the same set of skills and tactics to the table. Some responders may be better at quickly identifying whether and what malware is in the environment, but the methodologies they deploy may not facilitate documentation of facts necessary for the defense that the investigation is intended to support. Additionally, if a security firm is overly reliant on technology that misses a particular piece of malware, then its client will have missed a prime opportunity to mitigate its exposure in the incident (and the "digital shoe leather" required to find the malware will simply be missing from the equation). At the same time, if a particular technology or investigative methodology yields results that are not repeatable, the client may benefit from rapid information regarding the intrusion and the malware, but lack the appropriate foundation on which to base its defense of third-party claims.

Therefore, it is important to know the exact capabilities and methodologies of the security firms a company is hiring. Their ability to quickly develop the facts should not frustrate sound forensic, investigative and evidentiary methodologies. It should not be assumed that just because a company spent hundreds of thousands (or millions) of dollars on technology or services from a particular firm that the firm is also the right technical incident responder in a large network intrusion. As is the case with so much in a complex breach, experience and nuanced judgment in selecting the right firm will help avoid issues later in the investigation.

"We Need to Tell the Public Everything as Quickly as Possible"

Knowing when to notify the public and third parties and what to say to them is an essential component of risk mitigation in incident response. Public communications are one of the few things that a company can control (at least to some extent) in a complex incident response and one of the most important factors in limiting and mitigating exposure. Even though the importance of public communications in response to a cyber-incident cannot be overstated, companies often make the mistake of saying too much too fast (based on insufficiently developed or nonexistent facts) or saying so little that they are accused of hiding the ball and correspondingly pummeled in the court of public opinion.

Companies and the executives involved in a security incident response are, almost without exception, doing it for the first time and laser focused on "doing the right thing for their customers." While the motivation to do the right thing as quickly as possible is laudable, that zeal should not be allowed to cloud sound business and legal judgment, leading to rash and unfounded public communications. It is extremely difficult to deal with the volume of incoming information while at the same time developing third-party communications in the face of executives, customers, the press, regulators and adversaries pounding on the table for more information, more quickly. This need to communicate quickly has to be balanced with the threat of after-discovered facts and legal/business downside associated with overly enthusiastic communications. The best means of juggling these competing interests is by practicing the incident response plan and building a team that is experienced in high pressure, high stakes security incident response.

Our clients and prospective clients are rightfully concerned that breach communications will be "lawyered up" or sound "too legalistic." Experienced counsel and PR advisors should, however, be able to use both legal judgment and solid writing skills to produce communications that tell the story in a customer-friendly way, without at the same time creating problems with ill-timed, unfounded, vague or overly optimistic communications. This is by no means an easy balance to strike, but experienced and skilled practitioners should be able to simultaneously sort through hypertechnical facts of a security incident, identify the resulting business and legal issues, and develop well-crafted public statements that advance your business interests in a customer-friendly manner – all without "sounding like a lawyer."

If you would like to receive future *Privacy & Data Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Jon Filipek
+32 2 550 3754
jon.filipek@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Dominique R. Shelton
213.576.1170
dominique.shelton@alston.com

Paula M. Stannard
202.239.3626
paula.stannard@alston.com

David M. Stein
213.576.1063
david.stein@alston.com

Brian Stimson
404.881.4972
brian.stimson@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Jeffrey E. Tsai
650.838.2095
213.576.2608
jeff.tsai@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Michael Zweiback
213.576.1186
michael.zweiback@alston.com

ALSTON&BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333