MITIGATING THE CONSEQUENCES OF A DATA BREACH

BY ANDREW GOODMAN & DAVID OLENER

A data breach is like a bad car wreck. It can occur due to an unforeseeable event like being hit by a drunk driver, or it can be a completely preventable injury like falling asleep at the wheel. Either way, the harm has been done and Hippocrates cannot help. What to do next? If you are able to ask that question, it likely means you have stopped the bleeding. Now it is time to notify the family and start your recovery.

Recovering from a data breach is a multifaceted endeavor. There are compulsory measures pursuant to the laws and regulations of relevant local, state, federal and international jurisdictions. Then there are steps that, while not legally required, you ignore at your organization's peril. Among the most time-consuming activities after identifying the full corpus of potentially compromised data is determining who the individual data subjects are and who among them, if any, are legally entitled to a notification that a breach occurred. Further considerations include ascertaining whether data belonging to any commercial partners might have been exposed and which ones you might want to notify as a demonstration of transparency and goodwill. This can go a long way in ensuring your business relationships remain intact. Lastly, it is not hyperbole to say any proprietary information extruded could be extremely valuable to competitors. Giving them the benefit of the doubt that they would never actively try to steal your company's confidential material and hoping they will ignore anything now available is probably not an effective mitigation plan.

Once you have identified the data that has presumably been exposed, it is the unfortunate reality that you will need to review it. How quickly and how thoroughly depends on the requirements of the regulations that apply and an examination of the probability and scope of risks associated with any delay. If multiple jurisdictional rules cover the data breach, it may be fair to say that your process should follow the ones that are most arduous. In the United States, the California Consumer Privacy Act (CCPA), as one of the strictest privacy laws in the country, may be an appropriate framework absent confirmation that the breach is limited to data subjects in another state. Internationally, the European Union's General Data Protection Regulation (GDPR) has with good reason triggered significant concerns for most transnational corporations over potential fines for noncompliance with its complex rules and strict notification requirements. A recent example in a nonbreach context is the nearly $900 billion fine levied by Luxembourg's data protection authority against Amazon, which it accused of improperly using the vast amount of individual information it has amassed. While Amazon argues that the fine is improper because, according to its public statement, "There has been no data breach, and no customer data has been exposed to any third party,"[1] the implication is that companies would expect hefty fines in the event of a regulatory violation that does involve a data breach. While the fines associated with data breaches have not reached the level imposed on Amazon and other major corporations in other contexts, they should be no less concerning. A Swedish conglomerate that owns the H&M retail chain was penalized for inadvertently providing companywide access to all of its sensitive human resources data about individual employees. This breach lasted only a few hours and was not an external one; however, the Hamburg Commissioner for Data Protection and Freedom of Information chose to impose a $41 million fine on H&M.[2] Appropriate mitigation procedures can potentially lead to reduced fines, whereas failure to properly adhere to notification requirements could be disastrous.

With these and other incidents shedding light on the financial ramifications of a data breach, it is critical that your team take immediate action in such an event, and it is

essential to either develop an internal data breach mitigation process or hire an outside vendor that can provide customized processes and has the expertise and resources to effectuate them. If you choose to include review and notification procedures for third-party businesses and a review to identify internal confidential data, it is important to determine whether you will conduct them concurrently or in succession, and, if concurrently, whether you will have a single team review the documents for all three categories simultaneously. To help make this decision, first evaluate the scope of each individually. If the relevant statute or regulation imposes an aggressive and strict timeline within which individual data subjects must be notified, you may not have the flexibility to implement a contemporaneous workflow. First steps in determining the size and timing of the required effort can include running the data through an appropriate screen that is targeted to capture names, addresses, birthdates, Social Security numbers and other personal identifiers like eye color, height, weight and, of course, olfactory information. Olfactory information? Yes, you read that correctly. The CCPA includes "olfactory information" as a category of personal information. What this means exactly is unclear, but presumably it is something that would come up in the context of someone smelling really good or really bad (or, perhaps something more specific, as in the case of Charlie McKenzie's ex-girlfriend Pam from the movie So I Married an Axe Murder – he broke up with her because "she smelled like soup").

Think of your screening and review for data breach remediation as discovery for an internal investigation with external ramifications. You want your search terms to be broad enough to identify a vast majority of personally identifiable information, but narrow enough that the resources required to complete the review do not go beyond the bounds of reasonableness. For example, it is probably not a reasonable expectation that your vendor review 100 million documents out of an original set of 110 million. At the same time, it is probably not reasonable to merely do a spot check. Also, as in a discovery review, using a standard review platform and setting up a coding panel to tag PII types and capture text will be invaluable for fulfilling your reporting requirements later and providing further documentation of your process. In addition, you can distinguish between documents that have sensitive or nonsensitive personal information, a step that will be extremely helpful in identifying which individuals require notification.

"Think of your screening and review for data breach remediation as discovery for an internal investigation with external ramifications."

If you decide that it is wise to notify commercial entities such as vendors, business partners and corporate clients, you may choose to run a data breach screen that will target documents containing account numbers, personnel cell phone numbers, confidential/proprietary information and a list of known entities. Some of this will overlap with personally identifiable information, and some of it will be unique to a "business terms" screen. Again, there is value in using a discovery review tool so that you can code documents based on the type of information they contain. Because these documents may contain PII as well, there can be a significant time and cost-savings to a single review team reviewing them for both purposes concurrently. Reviewers skilled in data breach reviews should be able to manage identifying both personal and business information.

Finally, depending on the scale of the breach, it is likely prudent to review the compromised documents for your organization's own confidential, proprietary or otherwise commercially sensitive information or anything that would cause a reputational risk to the company if made public. There are different ways this can be accomplished. One method is to run a single confidential information screen based on the types of documents in the breached servers or in the possession of breached custodians. Another is to run a separate screen for each server based on department or for each custodian based on

role in the organization. This can be done with separate coding panels for each set, limiting the number of tags needed for the review of each document. In the event leadership wants to more fully understand the magnitude of the breach, separating the confidential information review into distinct content areas can simplify the output for an effective and easily distilled executive summary. This approach does have its own challenges, however. Documents that are shared across departmental servers or among custodians could hit on screens for more than one review, increasing the total document count and potentially duplicating effort. To mitigate this, it is important to thoroughly examine the breadth of the content that can be found in each set by reviewing samples before finalizing the search terms and coding panels. When this is done correctly, documents reviewed in a given set can be eliminated from subsequent sets. In this case, reviewing one set at a time may be the logical approach to take, given this is being done on an internal schedule as opposed to a statutory one.

There exists a plethora of skilled consultants with their own toolboxes that can be utilized to develop and implement a data breach remediation plan. The one that you choose for your organization should have significant experience doing this type of work and the flexibility to develop a process that fits the unique characteristics of the company and the breach itself. If, or more likely when, a data breach occurs at your organization, you may not always see it coming. Like the example of being hit by a drunk driver, there are some events that you know are possible but are still difficult to prevent and near impossible to predict. In order to protect yourself, you need to acquire as effective an insurance policy as possible. **ILTA**

***Andrew Goodman**, AVP of litigation services at QuisLex, has over 20 years of experience actively managing and supervising large-scale, complex document reviews in numerous industries and practice areas. He has trained multiple large teams on document review and creating privilege logs and is currently responsible for spearheading QuisLex's litigation training programs. He also manages key aspects of QuisLex's client and vendor relationships. Goodman frequently speaks on topics related to e-discovery and legal project management. He received his J.D. and MBA from Washington University in St. Louis and earned a B.A. with honors from the University of Michigan.*

***David Olener** is the associate director of legal solutions at QuisLex. Olener has over 15 years of experience as a litigation and e-discovery attorney, providing discovery and review oversight for some of the nation's largest lawsuits and investigations. He began his legal career at Proskauer Rose where he first became involved with highly sensitive discovery matters. Subsequently, Olener advised clients regarding the selection and use of analytical and review technologies and developed data loss prevention policies for international organizations, utilizing proprietary enterprise software. Olener joined QuisLex in 2019 and is heavily involved with data breach and incident response matters. He received his B.A. from Franklin & Marshall College and his J.D. from Benjamin N. Cardozo School of Law, where he was articles editor of the Cardozo Law Review.*

---

1. *Bodoni, F. (2021, July 30). Amazon Gets Record $888 Million EU Fine Over Data Violations. Bloomberg. https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach*

2. *Germany fines H&M 35 million euros for data protection breaches. (2020, October 1). Reuters. https://www.reuters.com/article/us-h-m-dataprotection/germany-fines-hm-35-million-euros-for-data-protection-breaches-idUSKBN26M5WM*