Legal Holds in Response to Data Breaches

Perhaps there is no better way to begin an article related to cyber risk than with the admittedly clichéd attention grabber:

“There are only two types of companies: those that have been hacked, and those that will be.” Since spoken by then-FBI Director Robert Mueller in March 2012, this refrain has evolved. As noted in a March 2015 opinion by District Judge John E. Jones III of the Middle District of Pennsylvania, the only two types of companies are “those that have been hacked and those that don’t know they’ve been hacked.”

For those in the latter category, ignorance is bliss, at least in the short-term. Sooner or later those companies will find themselves facing a host of difficult decisions, including whether there exists a litigation-related duty to preserve potentially relevant evidence, including electronically stored information (“ESI”).

In the immediate wake of a confirmed security incident, an organization’s efforts must be focused on containment, remediation, notification obligations, reputational damage, and other long-term repercussions. Subsequent efforts may require some documentation of the incident in connection with a potential investigation. Although preservation for this purpose may be narrow in scope, broad preservation efforts may be appropriate in certain instances. For that reason, an organization’s data breach response efforts may, depending on the circumstances, involve the issuance of a broad legal hold in connection with the duty to preserve and for defending against a possible spoliation claim in the event of litigation.

The vast majority of data breaches do not result in litigation. See Romanosky, S., Hoffman, D. A., & Acquisti, A, Empirical Analysis of Data Breach Litigation, 11 Journal of Empirical Legal Studies (2014). Then how, as an organization proceeds through the lifecycle of a security incident, can an organization determine whether it must comply with the litigation-related duty to preserve potentially relevant evidence? Regardless of whether a litigation-related duty to preserve evidence arises, an organization should take immediate steps to preserve electronic evidence to avoid the loss of key information, such as file creation dates, security logs, or other information that would enable the organization to narrow down the scope of the event. While there may be practical reasons to preserve this type of information, the duty to do so in anticipation of litigation is not quite as clear.

Automatically issuing a broad legal hold simply because a security incident occurred could unnecessarily burden organizations and their IT departments, which are properly focused on responding to the incident. Fortunately, the mere fact that a data security incident occurred, standing alone, does not automatically trigger the litigation-related duty to preserve. Rather, this duty is triggered only when there is also reasonable anticipation of litigation or an investigation as a result of the breach.

This determination is highly fact-sensitive. In the context of a data security incident, organizations should consider the nature of the breach, number of records at issue, relevant jurisdictions, underlying laws, whether the duty to notify impacted individuals has been triggered, plus numerous other factors. The legal hold decision is straightforward as to certain large-scale and highly publicized incidents. But what about smaller-scale breaches? While no single factor is dispositive, a close review of certain factors in the immediate aftermath of a breach will guide organizations and their counsel as to whether there is a reasonable anticipation of litigation or investigation such that a legal hold should be issued.
Anatomy of a Breach Response
Security incidents present in a variety of forms, including physical theft or loss of equipment that stores data, attacks to obtain access to IT systems, acts of malicious insiders, and even the mere failure to properly safeguard information. Regardless of an incident’s nature, the risk to an entity is the disclosure of personally identifiable information (PII) belonging to customers, employees, business partners, students or patients, or other confidential data such as trade secrets, intellectual property, or other sensitive corporate information.

When faced with a security incident, an entity must move swiftly. In short order, an entity responding to such an incident must:
• Trigger its incident response team, including identifying the appropriate members of the team depending on the scale of the suspected event;
• Conduct an investigation to identify how the security incident occurred and determine if it does in fact constitute a data breach;
• Contain the breach and conduct remedial activities to minimize the possibility of subsequent incidents;
• Identify the type of information exposed;
• Determine and comply with internal and external notification and reporting requirements, such as those related to regulatory agencies, consumers, patients, business partners, vendors, or employees and board members.

A growing trend among regulators is to inquire as to the steps and procedures used by entities in determining the scope of a breach and specifically the number of affected individuals.

The Duty to Preserve
More than a decade has passed since a series of opinions in Zubulake v. UBS Warburg LLC, et al., 02-cv-01243 (S.D.N.Y)

A growing trend among regulators is to inquire as to the steps and procedures used by entities in determining the scope of a breach and specifically the number of affected individuals.

• Triggering the incident response team, including identifying the appropriate members of the team depending on the scale of the suspected event;
• Conducting an investigation to identify how the security incident occurred and determine if it does in fact constitute a data breach;
• Containing the breach and conducting remedial activities to minimize the possibility of subsequent incidents;
• Identifying the type of information exposed;
• Determining and complying with internal and external notification and reporting requirements, such as those related to regulatory agencies, consumers, patients, business partners, vendors, or employees and board members.

A growing trend among regulators is to inquire as to the steps and procedures used by entities in determining the scope of a breach and specifically the number of affected individuals. Besides merely following an incident response plan, entities should, in appropriate circumstances, document their breach response efforts and preserve such documentation with regard to post-incident actions and the results of the ensuing investigation. But where litigation or an investigation can be reasonably anticipated, entities may be obligated to preserve much more.

Determining Whether There Exists a Reasonable Anticipation of Litigation
Anthem, Home Depot, and Sony. Rattle off the names of these companies to the average person on the street and the term “data breach” may very well come to mind. But determining whether or not there is a reasonable anticipation of litigation is not as simple as playing word-association
games. Highly publicized security incidents involving tens of millions of records will almost certainly result in at least some litigation. The sheer volume and scope of such incidents renders it nearly impossible to defensively avoid issuing a broad legal hold and embarking upon document preservation efforts. Fortunately, the typical data breach does not fit this description.

While most data breaches do not result in litigation, determining whether litigation can be anticipated requires a fact-sensitive analysis. In its simplest terms, is the breach at issue more akin to a routine fender bender or a four-car pile up resulting in multiple fatalities and life-altering injuries? A wide range of factors specific to the nature of data breaches must be considered, in addition to the type of exposed information, notification requirements, and potential statutory damages, among numerous other factors.

Scope and Breadth of Breach
The most obvious factor in determining whether litigation can be reasonably anticipated is the scope and breadth of the breach. Incidents involving millions of records will almost certainly result in at least some litigation or regulatory investigation. However, this analysis is not as easy where a breach is minimal in scope. As a result, this narrow factor is far from determinative.

Notification Requirement
The scope of a breach may have little bearing on a company’s obligation to notify impacted individuals and offer identity theft protection. A breach of the Health Insurance Portability and Accountability Act (HIPAA) through disclosure of protected health information (PHI) triggers a reporting duty to the Office for Civil Rights (OCR) under the U.S. Department of Health and Human Services (HHS) pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act regardless of the number of affected individuals. For breaches impacting 500 or more individuals, not only is notification required, but the entity will most likely find itself listed on OCR’s “Wall of Shame.”

Where a breach must be reported to regulators, there may exist a duty to preserve at least basic response documentation in instances where it is foreseeable that the regulator may seek information on the steps taken to contain the breach, remedial measures taken, the types and number of records affected, and so on. When notification is required, but the entity will most likely find itself listed on OCR’s “Wall of Shame.”

Litigants are expected to take certain affirmative steps to preserve evidence, including ESI, once litigation or an investigation can be reasonably anticipated.

Nature of Breach
The manner in which data is exposed may also provide a suggestion as to whether litigation or a significant investigation is likely to ensue. Security incidents deriving from the accidental temporary publication of sensitive data to a website stand in stark contrast to a deliberate attack and infiltration of a network. As to the latter, the use of criminal means and the presumed existence of a criminal motive suggest that exposed data may be used for a nefarious purpose, potentially increasing the likelihood of litigation.

The determination of whether there is a reasonable anticipation of litigation is highly fact-sensitive and should turn on consideration of the above factors along with the nature of potential litigation and the past experience of the organization and the industry as a whole. Regardless of an entity’s initial determination as to whether the litigation-related preservation obligation has been triggered, the entity should continue to monitor the situation. A preservation analysis two months following a security incident, after additional information has been obtained, may indicate that a radically different approach to preservation is required. But even where litigation appears unlikely, an entity should follow the procedures outlined in its incident response plan for documenting its response to an event. Such documentation may be relevant to any potential ensuing investigation regardless of whether litigation actually follows. Additionally, in the event of a subsequent breach, regulators may seek information about how an entity responded to a prior incident.

Scope of Preservation
Once a determination is made that litigation can be reasonably anticipated, what’s next? As a starting point, a formal, written legal hold must be issued. After that, there is no clear path to follow. Pursuant to preservation best practices, counsel should conduct interviews with document custodians and IT personnel to identify ESI locations and confirm that routine deletion practices have been suspended. But this will not nec-
Because entities are increasingly outsourcing management of their IT systems, it is important to take into account information held by third-party vendors that is relevant to the entity’s information security.

As decisions and steps taken by an entity may be questioned later on. These include board of director meeting minutes and correspondence, privacy officer correspondence and materials, post-breach correspondence and documentation, and correspondence and materials for IT, HR, and management.

The mere fact that a data breach has occurred does not automatically create a reasonable anticipation of litigation because the majority of data breaches do not result in litigation. However, the duty to preserve potentially relevant evidence cannot be dismissed. Following a security incident, organizations must consider the nature of the breach and the type of exposed information, among other factors, to determine whether, and to what extent, the duty to preserve has been triggered. Only then can an organization make a timely and informed decision as to issuing a legal hold and implementing a plan to appropriately preserve potentially relevant evidence.

For companies making the difficult transition from “those that don’t know they’ve been hacked” to “those that have been hacked,” internal resources will be spread thin. Immediate efforts upon becoming aware of a breach should focus on containing and responding to the security incident. At the same time companies cannot lose sight of potential long-term repercussions, including those related to litigation. While it is impossible to prevent a litigation adversary from second-guessing preservation efforts, early consideration of preservation and the implementation of a measured and reasonable approach to this duty serve to greatly enhance defensibility of process and reduce the potential for claims of spoliation in the event of litigation.