Articles + Publications | October 2, 2024

# Navigating the Complexities of Cyber Incident Reporting

**WRITTEN BY**

Sadia Mirza | Ronald Raether, Jr. | Karla Ballesteros | Kaitlin J. Clemens

*Published in Law360 on October 2, 2024.* 

Lawsuits and regulatory investigations have always been a possibility following a cybersecurity incident.

For years, the issue was whether plaintiffs' claims could even get past the threshold jurisdictional requirement of concrete harm. With courts opening the floodgate, we are experiencing an increase in both the number and nature of the companies and issues resulting in lawsuits and regulatory investigations.

When this occurs, companies are forced to reflect on the activities and decisions made during their incident response efforts, which are frequently executed under pressure and without a complete understanding of the incident's scope or effect — sometimes taking months or even years to fully reveal itself.

This uptick in the number and targets of legal and regulatory actions requires a more thoughtful incident response plan beyond what has become a check-the-box process. This additional focus emphasizes the necessity for businesses to document the facts underlying the assumptions, complexities and obstacles of their decisions during the incident response.

The objective is to demonstrate that the company conducted a reasonable investigation, including to determine the potential number of individuals affected and the type of information involved, and managed the notification process appropriately.

Regarding the latter notification issue, state and federal breach notification laws generally dictate who must provide notice after a security incident. However, these laws have not kept pace with technological advancements, increased data collection and the growing use of third-party vendors. The large volume of data managed by businesses and vendors adds new complexities to incident response, which regulators are starting to recognize.

Of course, we also should not forget that criminals are behind this cat-and-mouse game of testing security and hiding their illegal acts, further complicating the investigation.

For example, after the February Change Healthcare cybersecurity incident, the U.S. Department of Health and Human Services issued the "Change Healthcare Cybersecurity Incident FAQs" at the end of July[1] to clarify

certain Health Insurance Portability and Accountability Act notification obligations for covered entities. These FAQs were released “given the unprecedented magnitude of [the] cyberattack” and its “widespread impact,” acknowledging the complexities of the incident and the need for flexibility in regulatory compliance.

While the flexibilities granted to covered entities affected by the Change Healthcare incident are welcome news, businesses have long faced similar challenges. Often, what is practically achievable and feasible for a business may not align with the expectations of regulators or plaintiffs counsel. In such cases, it is crucial for the business to document any assumptions, complexities or obstacles that affected their incident response strategy and to rigorously test these assumptions to ensure they can withstand scrutiny.

It is important to remember that courts and regulators will evaluate whether the conclusions drawn during the incident response favor the business or the affected consumers. If it appears that consumers are disadvantaged, the business may face greater challenges in defending its response.

Historically, when businesses faced a cybersecurity incident, they determined whose information was involved in one of two ways: either by conducting the review internally or by hiring a third party to analyze the data, a process known as data mining.

Data mining typically involves two steps. The first step, the “programmatic review,” uses broad search terms to scan the dataset for any potential protected or sensitive information.

After this, the organization reviews the results to eliminate false positives. This helps reduce the cost and time of the second step, the “manual review,” where each document is manually checked for protected or sensitive data. The final report, usually an Excel file, lists individuals, their addresses — if available — and any potentially protected personal information found.

In the past, this process was straightforward with small datasets. However, with technological advancements, evolving threat tactics, and the storage of unstructured data — i.e. free-form data that is not easily readable by a machine, such as multimedia files or the body of an e-mail — the process has become more complex.

Now, when determining the effect of a security incident and the appropriate notification strategy, businesses must consider several key factors, including the following.

**Did the forensic investigation present any challenges?**

One of the primary goals during an incident is to rely on forensic evidence to determine the scope and confirm what files/folders were involved. However, businesses often encounter significant challenges in this process, particularly due to the lack of a comprehensive suite of logs that provide a complete picture of the incident.

Certain logging may not have been enabled for the relevant time periods, or logs may have rolled over before the investigation began for legitimate business reasons, e.g., storage and cost limitations. Furthermore, sophisticated threat actors may take steps to delete traces of their activity in the environment, further complicating efforts to piece together the sequence of events. These gaps can lead to uncertainties in the forensic investigation, making it difficult to ascertain the full extent of the incident.

When faced with uncertainties, businesses may need to rely on alternative information or sources to better understand the incident or make decisions based on assumptions rather than facts.

These sources might address factors such as the duration of the threat actor's access to the environment; the encryption of data and the accessibility of encryption keys; intelligence about the threat actor's tactics or techniques; a threat actor's file path listing obtained during negotiations; or results from dark web monitoring.

By compiling and analyzing these alternative facts, businesses may be able to form a defensible narrative around the scope of the incident, even if the forensic evidence is incomplete.

When businesses rely on sources other than direct forensic evidence, it is essential to document what those sources are and why it is reasonable to rely on them to determine the scope of the compromise. By doing so, a business can argue that this method of piecing together the story was reasonable and led to a more accurate assessment of notification obligations.

Without such an approach, the business might be compelled to over-notify due to the lack of direct evidence, which could cause unnecessary consumer panic and distress. Additionally, if all businesses adopted this approach, it could dilute the effectiveness of breach notifications, as consumers are likely to experience "notice fatigue."

Regardless, this process and the conclusions should reflect the lack of certainty if assumptions are made as to whether any consumer or element of protected data was in fact affected by the data incident.

**Is data mining needed or practical?**

Even when an organization can accurately identify the files or folders involved in an incident, the dataset slated for review may still be unwieldy. Beyond the question of size, the types of files in the dataset significantly affect the time, cost and complexity of data mining.

In addition to straightforward Word files or PDFs, datasets can include other unstructured data such as free text fields, audio files, poorly scanned images or handwritten documents. Reviewing these types of files to determine if they contain protected information is a time-consuming and costly process, often requiring separate protocols from those used for structured data.

In its 2020 guidance,[2] the Vermont Attorney General's Office specifically addressed breaches involving unstructured data and encouraged data collectors to "deploy any technologies available to assist in searching for PII, within reason relative to the size and sophistication of the business, and the nature of the data involved."

The office further stated that "where a business takes a long time to report an unstructured data breach because they did not take advantage of available technology, it may have violated the Act."

This guidance suggests two key points:

***1. Data Mining as a Necessary Step***

While the guidance does not define “available technology,” organizations should consider data mining — using programmatic reviews to identify protected data — as an essential part of a diligent investigation.

However, data mining is not a perfect solution and has not perfected the data review process. Careful consideration must still be given to how the data mining should be conducted, what the review protocol entails, and the final deliverable that will be presented at the end of the review.

Businesses should also be prepared to find that, even after data mining, additional levels of review may still be necessary to determine who ultimately requires notice of the incident and with respect to what data.

***2. Reasonableness and Proportionality***

The use of data mining technologies should be reasonable and proportionate to the “size and sophistication of the business.” For instance, if the cost of a data mining exercise is exorbitant, it may not be considered reasonable.

Similarly, if a data mining exercise could technically be completed but would take months or years or involve extensive resources to complete, it may not be the best approach. Organizations need to evaluate what it would take to perform data mining and, if practical, include it as part of their response.

If not practical, it is crucial to document the challenges posed by data mining and explain why avoiding that step was in the best interest of both the business and affected consumers or customers.

It’s important to note that businesses are not required to engage a third-party vendor to mine affected files in response to an incident. If a business can reasonably determine the data involved using internal resources, documenting that process and providing notification based on those findings may be sufficient.

That said, if an incident is likely to receive the attention of plaintiffs counsel or regulators, there are key advantages to using an outside vendor, including one that has not been part of the company’s cybersecurity program.

**Has the issue of data ownership complicated the notification strategy?**

Under state and federal breach notification laws, entities that “own” data are typically required to notify affected individuals of a data breach. In contrast, entities that merely process or maintain data on behalf of another organization — i.e., the data owner — are generally only required to notify the owner of the data.

The issue of data ownership has further complicated notification strategies in recent years. Service providers, who do not have an obligation to notify affected individuals directly, are increasingly assuming this responsibility. This shift is often due to contractual obligations or, more frequently, to protect their reputation and business relationships.

However, before a service provider can take this step, several questions must be considered.

- Does the service provider have the right to review the affected data at the granular level needed to effectuate

notice?

- Does the service provider have an understanding of the data such that it could determine what protected or sensitive data elements are involved?
- Is it administratively practical or feasible to identify the affected individuals and determine which data owners they are associated with?
- Has the data owner agreed to the service provider providing notice on its behalf, and what does the opt-in, or sometimes, opt-out, process look like?
- What information should the service provider include in the breach notice to explain why they have the affected individuals' data?
- How will the service provider notifying affected individuals affect the regulatory notification strategy or litigation defenses?

These are examples of the questions service providers should consider when developing a data review and notification strategy.

If businesses choose not to have a service provider send notifications on their behalf, they should also consider whether this approach will result in an individual receiving multiple notices from various data owners about the same incident. This could create the impression that the individual's information has been repeatedly breached, even though all the notifications pertain to a single incident.

As seen in the Change Healthcare incident, regulators are increasingly recognizing the complexities of data owner notification in large breaches.

Another example is the CDK Global incident from June, where there are reports suggesting that CDK obtained permission from the Federal Trade Commission to file a consolidated notice on behalf of all its affected dealer clients.

This reported agreement — applicable if CDK determines that the reporting requirement under the FTC Safeguards Rule has been triggered — means that individual dealers will not need to file separate notices with the FTC regarding CDK's June 19 incident.

**Above all, document the notification strategy and prioritize consumer and customer protection.**

Determining the scope of an incident and identifying who needs to be notified and how is not always a straightforward task. In areas where there is a lot of gray, it is crucial to document the clear, factual basis that informed the notification strategy.

Likewise, any assumptions made about the affected dataset should be pressure-tested and reviewed from the perspective of affected consumers and customers.

As courts and regulators are beginning to recognize, responding to an incident is not a one-size-fits-all exercise. Businesses should feel empowered to think outside the box when determining the scope of an incident and crafting a notification strategy.

With careful consideration, a consumer-friendly approach can align with the goals and expectations of the business, ultimately resulting in not only a defensible response but also a positive narrative to share.

---

[1] Change Healthcare Cybersecurity Incident Frequently Asked Questions, July 30, 2024, U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html.

[2] Vermont Security Breach Notice Act Guidance, June 2020, Office of the Vermont Attorney General, https://ago.vermont.gov/sites/ago/files/wp-content/uploads/2020/07/2020-07-14-Security-Breach-Guidance.pdf.

**RELATED INDUSTRIES + PRACTICES**

- Incidents + Investigations
- Privacy + Cyber