Articles + Publications | August 24, 2023

Data Protection: One of These Incidents Is Not Like the Other

WRITTEN BY

Stephen C. Piepgrass | Samuel E. "Gene" Fishel | Sadia Mirza

This article was originally published on August 24, 2023 in Reuters and is republished here with permission.

In the burgeoning realm of data incidents, it is a truism that such incidents are not created equal. Indeed, a data incident is not necessarily a data breach.

An incident is any “occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system,” or an event that constitutes a violation of an organization’s computer security or acceptable use policies. National Institute of Standards and Technology, Minimum Security Requirements for Federal Information and Information Systems, FIPS 200, at 7 (Mar. 9, 2006) (nist.gov). A breach is an incident that imposes statutory and regulatory obligations on an affected organization when it holds or controls certain consumer information.

Data incidents and associated breaches can engender state and/or federal investigations, shareholder suits, and consumer-driven private litigation, including class actions. Organizations therefore must quickly assess the nature and scope of a data incident and undertake a course that not only resolves the incident itself but also addresses all legal obligations while simultaneously limiting liability exposure.

In part one of this four-part series, we identify the different types of incidents and what regulators look for when evaluating them.

A. Three categories of incidents

No two sets of facts are identical among data incidents, although many retain similar characteristics. Recognizing this, we can organize them into three broad categories: (1) those that are quickly assessed and contained, (2) those where the scope is uncertain and further investigation is necessary, and (3) those of such a large scale or sensitive nature, whether readily apparent or not, that a regulatory investigation is all but inevitable. Certainly, these categories are not mutually exclusive, as an incident can shift between them or encompass more than one.

Notably, the specter of government investigation hovers over each of these categorical baskets, particularly if the incident is, or potentially could be, a breach. Organizations must therefore be vigilant in the wake of any incident. Legal obligations, such as data breach notification statutes and agency regulations, are generally invoked when certain “personal identifying information,” or an equivalent label, is compromised, thus transforming it into a breach.

Confusingly, each state and regulatory body has its own definition of personal identifying information. Social Security numbers, financial account information, and driver's license or state identification numbers generally trigger laws across the board. Information like date of birth, medical information, passport numbers, and biometric data, however, receive varied treatment. Given this, organizations should be aware that, depending on its size, an incident may enkindle federal regulations and/or 50+ state and territorial laws, and so should consult with legal counsel as appropriate.

1. Quickly assessed and contained incidents

These incidents typically involve an event that is smaller in scale and affects an easily identifiable data set. For example, a company employee accidentally emails a spreadsheet containing the names and credit card numbers of 100 of the company's customers to the wrong individual. The email provides clear evidence of what was sent and to whom.

Presumably, the risk of harm to the customers is relatively low particularly if the recipient is familiar and it can be confirmed the recipient quickly deleted the email. Yet this scenario may still be a breach in some states. If the company quickly addresses the incident and provides notice in a timely fashion, governmental entities are unlikely to initiate an investigation, presuming there are no other aggravating factors.

2. Incidents of uncertain scope

These are incidents requiring in-depth investigation to determine what data was affected, if any. In this hypothetical, an employee for a tax preparation service company inadvertently mails flash drives to 50 clients containing tax information pertaining to the company's employees. The company is unsure specifically what employee information is contained on each flash drive.

There is a chance, however, that any one drive contains an employee's Social Security number and the tax withheld from that employee's income. Importantly, if indeed present, these data elements qualify the incident as a breach under many states' breach notification statutes. It will be a challenge to track down all 50 flash drives and it will likely take the organization significant time to fully uncover the facts if they fully uncover them at all.

Ultimately, notice to affected consumers may be required once the incident is confirmed to be a breach. When assessing notification to regulators, businesses may want to consider a strategy at the incident's outset of ongoing communication with updates and developments as the matter evolves. Regulators often include state Attorneys General and/or a primary industry regulator such as a Commissioner of Insurance or State Corporation Commission.

3. Large-scale and sensitive incidents

Some incidents will most assuredly garner regulatory scrutiny. For example, a hacker infiltrates a health insurance company's network and exfiltrates the Social Security numbers and health diagnoses information for 15 million patients. She then appears to sell this information on the dark web.

This is clearly large-scale because of the number of affected patients, and it involves information that, while not

protected by all breach notification statutes, may be viewed by consumers as “personal” nonetheless. This breach may draw the attention (and ire) of state Attorneys General that maintain jurisdiction as well as the company’s primary insurance regulators.

In such scenarios an organization must steel itself for multiple and protracted investigations. Early and transparent communication with stakeholders as outlined below is essential.

B. Regulator concerns and mitigation

Within this universe of incidents then, what raises red flags for controlling government entities? Regulators look at several factors when deciding whether to pursue an investigation, including:

- The number of consumers affected,
- The consumer demographic affected (e.g., the elderly),
- The sensitivity of the data at issue,
- The likelihood of consumer harm,
- The type of intrusion,
- The applicable legal obligations,
- The amount of media attention,
- The affected organization’s response, and
- The regulator’s desire to make a broader policy statement.

Not all the above factors need be implicated to trigger regulatory scrutiny. Indeed, only one aggravation can suffice, or any combination thereof, for regulators to launch an inquiry.

Transparency and promptness in breach notifications help mitigate regulatory scrutiny and maintain consumer trust. Below are specific factors to consider when developing a pre-incident plan and navigating an incident.

1. Pre-incident security safeguards

Regulators routinely seek information about security measures and protocols in place before an incident. Establishing an information security program modeled after established frameworks such as the CIS Security Controls or the NIST Cybersecurity Framework demonstrate proactive measures taken to secure data.

Organizations should continuously adapt cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. See Nat’l Inst. of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Apr. 16, 2019). They should also develop an incident response plan and conduct routine tabletop exercises to test the plan’s efficacy. Such steps will positively reflect an organization’s commitment to guarding against ever changing threats in the technological landscape.

2. Timely and transparent communication

Upon a breach, regulators focus on the timing of notifications to consumers and regulators. Each state’s breach

notification law dictates the timing of the notice. Some states require notice in as little as within 30 days after discovery of a breach. Others require notice "without unreasonable delay" after discovery, with reasonableness dependent on the type of breach, the investigation's length, the number of affected consumers, and the ease of identifying those consumers among other factors.

Transparency is also critical. Explaining the incident in general terms and what data was affected, if known, is necessary at the outset, and often required by law. A response should present clear information to affected individuals, along with sufficient self-help resources, like advice on contacting credit bureaus. Where needed, it should also indicate the method the organization will use to contact consumers with updates and a number to call for questions.

The responding party must also carefully discern between those facts that should be disclosed to comply with all pertinent laws from those "facts" that still may not be fully known and may also unnecessarily expose the organization to regulatory and litigative risk. Striking the right balance is essential to avoid further complications.

3. Cooperation with regulators

Organizations must proactively reach out to potential federal and state agencies that may retain jurisdiction over a breach when appropriate. This includes providing an explanation of the timeline from the incident's discovery to the date, or potential date, of notifications and issues that have arisen during the forensic process.

Further, regulators often look favorably upon early notification to law enforcement. Law enforcement may subsequently ask that notification to affected parties be delayed to not compromise the ongoing criminal investigation. Most state breach notification statutes allow for such a delay, but only if law enforcement has requested it.

Many state laws require affected organizations to list steps it will take to prevent future breaches. Detailing changes implemented such as improved security measures, enhanced protocols, and employee training, can demonstrate a committed path forward.

4. Further response strengthening

Regulators typically ensure organizations have executed a response plan throughout a breach and its aftermath. Organizations should coordinate responses with internal and external stakeholders, including deploying forensics with deliberate speed to identify, contain, and assess the incident. Other measures include, where relevant, confirming the extent of accessed or exfiltrated data, conducting dark web monitoring to verify leaked, exfiltrated data, and, for a ransomware attack, weighing a ransom payment with assurances from threat actors.

Organizations should consider offering at least a year of free credit monitoring or identity theft protection, which is required in some states. Finally, continually updating an organization's website with clear and concise language about the breach, along with establishing a call center or a website providing answers to frequently asked questions, reflects positively upon response efforts and will save time. See Fed. Trade Comm'n, Data Breach Response: A Guide for Business (Feb. 2021).

Conclusion

Incidents are not homogenous. By acting swiftly to identify their nature and contain them, take appropriate remedial measures, and notify pertinent parties, an organization can mitigate regulatory scrutiny and position itself for a quick recovery.

In part two of this series, we will cover the key regulators in the data incident arena and how they operate.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber
- Regulatory Investigations, Strategy + Enforcement