
An Investigative Approach to Data Breaches: From Incident to Resolution



STROZ FRIEDBERG

After investigating nearly every angle of a data breach, one common denominator amongst all breaches can be identified: the need for prompt resolution

Overview

Across all industries, data breaches continue to abound and the variety of root causes are just as plentiful: lost laptops, missing backup tapes, stolen computers, compromised servers, and hackers being some of the more well-known culprits. Identifying the origin of a breach is just the first step toward resolution. It is imperative to also immediately investigate the nature and extent of the intrusion. This demands a tactical and intelligent threefold approach – using conventional investigative means, computer forensics, and a savvy cybercrime incident response team.

Addressing Key Questions

After investigating nearly every angle of a data breach, one common denominator amongst all breaches can be identified: the need for prompt resolution. While taking swift action to minimize future security vulnerabilities, key answers must be brought to light for numerous constituents. Board of Directors, corporate officers and information technology executives need to harness the proper knowledge so they can fully assess damages, determine reporting obligations with respect to statutory notifications and law enforcement, and decide whether or not to issue public statements. How? It starts by responding to some critical questions:

- What was on the misplaced or stolen media? This is often far from clear when the media is backup tapes and external hard drives.
- Was the attacker a current or ex-employee, a low-level script kiddy, or a sophisticated hacker employed by a competitor or hostile government? Was the hacker successful in obtaining sensitive data?

- What is the true risk of harm to the victims?
- Did the intruder access credit card information, dates of birth, Social Security numbers, PIN numbers, Protected Health Information (PHI) or other Personally Identifiable Information (PII)? If so, how many, and for what customers in what states?
- How do we meet our notification obligations?
- Was the illegally-accessed data encrypted, in which case notification need not be made? If not encrypted, would the data on a backup tape be so difficult to restore that, as a practical matter, there is no real risk of harm to customers? Under some state statutes, that may exempt notification.
- Should law enforcement be notified, and, if so, when? Such referral may postpone notification requirements under some state statutes.
- How can we return to normal operations as soon as possible?

Business Challenges and Resolutions

To give you greater insight into the numerous ways in which organizations confront threats of data breach, below are some real life business challenges and resolutions that give a better understanding of the importance of promptly taking skilled, proactive and reactive measures to help minimize the potential impending financial, legal and reputational risks of a data breach.

Case Study #1

Investigating Insider Data Breach and Identity Theft at a Public Company

Issue: Two customer service representatives of a publicly traded company that specialized in handling sensitive insurance claims were terminated and arrested after a check-cashing company alerted law enforcement to suspicious-looking checks. These customer service representatives had diverted checks from accounts held for the company's clients to their own use.

Scope: The digital forensics team reviewed the actions taken by the IT staff, to evaluate the scope of the breach, and to determine what additional steps were required to ensure that the internal investigation was thorough and complete.

Solution: Along with the company's IT Department, the forensics professionals worked to preserve relevant data from multiple digital media sources, including workstations of select former and current employees and mainframe log files, maintaining strict chain of custody procedures. The preserved digital media was analyzed to determine whether the breach was limited to the arrested employees and whether additional accounts had been compromised.

Result: The examination revealed that the former employees not only had diverted checks to their own use but, having also stolen clients' PII, they were purchasing cell phones, car rims, sound equipment, and other goods through the Internet in the names of their victims. They also used the stolen PII to apply for credit cards in the victims' names and, in at least one instance, obtained a cash advance from one of those credit cards.

The results of this forensic analysis were provided to the company and used for the successful prosecution of the former employees for fraud and theft.

Case Study #2

Assessing the Impact of an SQL Injection Attack

Issue: When an IT department noticed an enormous spike in queries to its website and corresponding error messages, it correctly suspected it was the subject of an SQL injection attack. In such an attack, the intruder sends intentionally malformed requests to a company's website in the hope that the server will malfunction and either return non-public data in response to the request or grant the attacker a deep administrative access to the server.

Scope: The client's IT department and the digital forensics team worked together to capture a sample of the malicious requests being used by the intruder to replicate the attack on a test machine. The testing indicated the intruder's malicious requests were returning error messages that contained customers' user names and passwords. Further analytic work identified a defect in the code generating the website's error messages, and that code was rewritten.

Solution: The team forensically preserved the web server's logs and the last-accessed dates of all of the customers' account files and correlated those records with the originating IP address of the attack. The purpose of this was to segregate those customers' accounts that had been accessed from the attacker's computer as opposed to the legitimate users' computers. Finally, custom programs were applied to determine which of the affected customer accounts had the kinds of personally identifying data that could be subject to state data breach notification statutes.

Result: With the information in hand, the company and its outside counsel were well-positioned to determine the scope of the company's obligations under the data breach notification statutes.

The team forensically preserved the web server's logs and the last-accessed dates of all of the customers' account files and correlated those records with the originating IP address of the attack.

An Investigative Approach to Data Breaches: From Incident to Resolution

Data Breach Response and Fraud Resolution

When a data breach has been identified it is vital to have a plan in place that addresses possible or actual ensuing occurrences of fraud. As a best practice approach, an organization should have the know-how and right resources to address these key areas:

- **Incident Management** – Who will manage the data breach incident internally and externally? What resources are available?
- **Notification** – What are the requirements based on the type of data breach? How will those affected be notified as required by law?
- **Call Center Support** – Will the company require call center support to field incoming calls with questions about the data breach? What should and should not be said?
- **Identity Theft Protection** – Is it a best practice to offer identity theft protection and what are the benefits to the client?
- **Fraud Resolution** - If identity theft does occur as a result of the data breach, where should consumers be directed for resolution?
- **Reporting** - Will you need to provide statistics on the who, what, and how many affected individuals there were in a data breach incident? Will you also need to know if any fraud cases incurred as a result?

One of the most challenging activities for a consumer can be resolving identity theft. It can take up to **5,840 hours** (the equivalent of working a full-time job for two years) to correct the damage from identity theft, depending on the severity of the case.¹

By providing the tools to consumers and employees to allow them to successfully mitigate the potential risks of fraud after a data breach, an organization can prove that they have taken extra steps to ensure the consumer or employee's best interest is in mind. This helps maintain brand equity during a potentially reputation-damaging experience.

How can a Fraud Resolution Team help?

A Fraud Resolution Agent can drastically decrease the time an individual spends correcting the damage incurred from fraud. Such an agent can be an invaluable third party ally by helping to:

- Remove the confusion and anxiety around how to resolve identity theft.
- Run a credit check and review your credit record to determine accuracy and potential areas of fraud.
- Notify the three major credit bureaus, all of your creditors, all financial institutions at which you maintain accounts, and all of your utility providers of the identity theft.
- Provide assistance with disputing the fraudulent items.

- Work with Law Enforcement or other Government agencies that may be involved.
- Provide copies of all necessary letters to send to creditors, Credit Reporting Agencies or others who may be involved.
- Work with the institutions and agencies involved until the situation is rectified.
- Other assistance as might be reasonable to offer on a case by case basis.

Summary

When a suspected data breach occurs, there is indeed a technical and legal urgency to uncover the who, what, how, when and why. At the same time, it is of vital importance to swiftly address the many looming vulnerabilities that could manifest in reputational injury and moreover, fraud. Synchronizing an effective incident response, one that bears minimal disruptive impact on operations, requires the wherewithal for timely fact-finding and risk mitigation at all levels. Bringing in an experienced third-party is often the recommended best practice to efficiently and effectively navigate the full spectrum of data breach challenges, those ranging from digital forensic investigations to notifications and statutory obligations, to resolving complex fraud issues in order to help ease the lives of the identity theft victims and ultimately preserve the brand name.

For more information about data breach digital forensics solutions, visit www.strozfriedberg.com. To learn more about data breach resolution, visit www.experian.com/databreach, or contact Experian® at databreachinfo@experian.com or 1 866 751 1323.