# Breach Response Buyer's Guide

How to choose the right breach response provider and ensure positive outcomes

![IDX logo]

# Introduction

## Data breaches are an everyday cost of doing business

A proper response can mitigate the negative effects of a breach, but it takes skill, experience, and careful planning. To be successful, the right internal and external resources must create and execute a response strategy that protects affected individuals and meets legal obligations.

**THIS GUIDE WILL COVER:**

**1** What to look for in a breach response provider

**2** Why credit monitoring isn't enough

**3** Scalability and why it's important

**4** How to verify a provider's reputation

# 5 Capabilities of a Reliable Breach Response Provider

A successful breach response depends, in large part, on the data breach response provider you and your privacy team select. While many companies claim to provide data breach response, their actual services vary widely. Our Breach Response Buyer's Guide outlines the five capabilities to look for when selecting the right breach response partner.
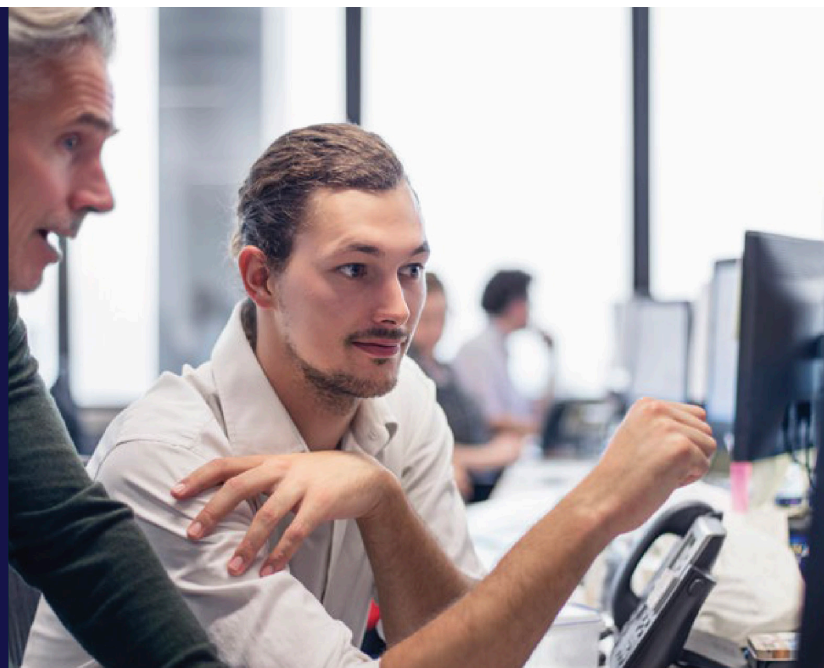
## 1 SPECIALIZES IN BREACH RESPONSE

Seek a data breach response provider whose main business is helping organizations respond to data breaches in the most efficient and compliant way possible. A provider focused on data breach response will work with your privacy counsel to help analyze each breach to understand the regulatory, reputational, financial, and operational risks to your organization. They will then provide whatever support is necessary to best mitigate those risks.

💡 **Beware of credit monitoring businesses that offer breach response services only to gain more subscribers for their monthly consumer services.**

## 2 CUSTOMIZES ITS SERVICES

Your breach response partner should be able to help create a customized response that both fits the situation and complements your internal capabilities. This helps you avoid buying more services than you identity theft protection for patients, for example. In addition, your provider should be able to work closely with your counsel to provide customized communications to the breached population and regulators, if appropriate.
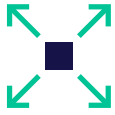
💡 **Avoid buying more services than you need.**

---

> "While data breach costs have been rising steadily, we see positive signs of cost savings through the use of proper planning for incident response, which can significantly reduce these costs."
>
> — **Ponemon Institute**

### 3    SCALABLE: CAN HANDLE BREACHES OF ALL SIZES

Few data breach response providers can handle both small and large data breaches. Some only handle the mega breaches affecting millions of individuals and won't provide services for the smaller and more frequent breaches. Conversely, others lack the capacity to manage large breaches, and service quality suffers when the breach is large. Find an experienced breach response provider that can handle all of your breach needs, whether the breach involves one record or one million records.

**Can the provider you select help with future breaches — no matter the size?**

### 4    OFFERS A COMPREHENSIVE RANGE OF SERVICES

A full-service data breach response provider will provide all of the services your organization needs in the event of a breach: digital forensics, risk assessment, breach planning, U.S.-staffed call center, letter notification and mailing, and a user-friendly enrollment website — and only provide the services you need to fit your breach incident. You do not have to contract with a separate provider for each of these services. Especially when a breach occurs, time is of the essence. Having a single provider that works closely with your privacy counsel during the breach response process will save time and money, as well as reduce the reputational and regulatory impact of a breach on your organization.

### 5    HAS A SOLID REPUTATION

Reputation matters. Given the sensitive nature of data breaches, it's critical to work with a breach provide that holds itself to the highest ethical standards. Before contracting with a data breach response partner, take the time to find out if they have any recent legal troubles, regulatory infractions, or if the organization itself has experienced a breach. Also, verify that the breach response provider has the appropriate industry certifications, compliant with the necessary regulations, such as NIST SP 800-53 Rev 4 standards, and trusted by Fortune 500 companies, top hospitals, and government agencies.

**Working with a single, full-service breach response provider saves valuable time — and money.**

> " Your effective resolution of events combined with a patient and pleasant demeanor make hard times doable."
>
> **— Customer, IDX Breach Response**

# Conclusion

The right breach response provider can go a long way toward ensuring positive outcomes from a negative situation. Look for one who specializes in partnering with your privacy team, has an extensive history in breach response data breach sizes, provides a full range of services, and has a solid reputation you can rely on. After all, your organization and your customers demand the best.

**Will your provider ensure positive outcomes from a negative situation?**

## Don't wait for the inevitable cyber attack.

Choose the breach partner that will work best with your team and protect your customers and your business

📞 855.HELP.IDX   I   ✈ response@idx.us

# Helpful Links & Resources

**WEBSITES**

U.S. Department of Health and Human Services (HHS) on HIPAA Breach, Notification Rule

HHS Office for Civil Rights Breach Portal

HHS Office of Inspector General

List of State Security Breach Notification Law

Cybersecurity Infrastructure and Security Agency (CISA)

FBI: The Cyber Threat

FBI: Cyber Incident Reporting

---

**RESEARCH & RESOURCES**

IMB 2024 Cost of Data Breach Report

A Complete Guide to Data Breach Response

Identity Theft Resource Center

IDX Knowledge Center

Verizon Data Breach investigations Report

---

**SERVICES & SOLUTIONS**

IDX Incident Readiness Services

IDX Digital Forensics & Incident Response

IDX Breach Notifications & Protection