BREACH BASICS: PREPARATION FOR THE INEVITABLE

Recommendations for Breach Victims

By: Alex Rice, Co-Founder & CTO, HackerOne

Data breaches in information security have become an inescapable reality. A common inquiry we receive here at HackerOne is for guidance on how to most effectively respond to one of these unfortunate incidents. There are no easy answers. **Our hope is the following guidance can serve as recommendations for any victim of a breach.**

Before we dive in, I'd like to offer a brief note on confidentiality. HackerOne treats the confidentiality of our customers with the utmost respect. Our policy is to not comment or speculate on any breaches or vulnerabilities impacting the programs we have the privilege of hosting.

In addition, for the majority of the programs hosted by HackerOne, our relationship as a platform provider does not grant us privileged access to information on their breaches, vulnerabilities, or context surrounding individual bounty payments.

- **ALEX RICE**
CO-FOUNDER & CTO, HACKERONE

Breach Response

Your first priority following the discovery of unauthorized access to data ("a breach") should be incident response. That means preparing for a breach before it happens. A proper incident response plan will focus primarily on mitigations that stop the bleeding and remove the unauthorized access to further data.

An effective process should be designed to leave us with clear answers to the following questions:

WHAT data was breached and who did it belong to? (specifically what data types?)

HOW was the data breached?

WHEN was this data breached? (a full time-line of events)

WHO breached it? (criminal, rogue employee, accidental disclosure)

There is often a large amount of uncertainty that remains even after significant evidence gathering has occurred. It is not uncommon for "we don't know" to be the answer that remains to at least some of these questions. Once armed with your best answers to these questions we can prepare your response.

Breach Notification

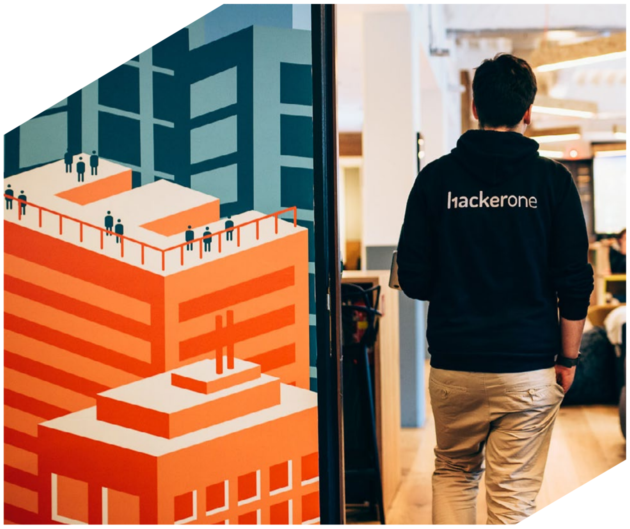
In many significant breaches, notification to individuals whose data was affected, such as customers or employees, may be legally required. Whether notice is obligatory requires familiarity with a dizzying array of state, federal and other countries' data protection laws. There are lawyers who specialize in these laws, and you should consult one if you find yourself in this situation.

Even in the absence of a legal requirement, public disclosure may be in the best interest of both the breached company and the persons whose information was impacted. Should you provide notice? You should strive to have the applicable laws mapped to any data you are in possession of ahead of an actual breach.

Five Questions to Ask Yourself:

1. Are there steps that users can take to protect themselves?

(change their passwords, check their statements, etc) If so, we recommend providing notice as soon as possible to arm victims with the relevant information.



2. Has the breached data triggered any notification laws?

In the United States, 48 states, the District of Columbia and several territories have at least one breach notification law that mandates notification to customers if their personal information has been accessed without authorization. Some states define "personal information" more expansively than others and set different time frames for notification. For example, thirteen states require notice in the event that unique biometric data is accessed, while only four require notice if a person's online login credentials and password are accessed. But they all require notices to describe what data was accessed. That is why it is so critical to understand the categories of data that were impacted by the breach. Some states may also require providing notice to a state law enforcement authority, such as the state Attorney General or the state police. If you suspect personal information of has been breached, we recommend you consult with legal counsel immediately.

In the European Union, General Data Protection Regulation (GDPR) will soon enforce even broader requirements. Article 33 requires a breach of personal information be disclosed within 72 hours to your supervisory authority. A step further, Article 34 reads: "*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*" Additionally, other countries around the world have their own data breach notification laws, and a breach affecting a global employee or customer base may require notice globally. Due to the subjective interpretation of these regulations, we recommend consulting with legal counsel immediately following a breach. You may also consider defaulting to public disclosure given the ambiguity involved.

3. Does the breach expose Protected Health Information (PHI)?

If so, you should assess if the HIPAA Breach Notification Rule applies as it provides clear guidance on disclosure steps. HackerOne customers who are in possession of PHI should contact us to ensure that your program policy and business associate agreement (BAA) specifically authorize expected testing activities.

4. Are you or your industry subject to specific requirements from regulators?

If so, work with your compliance officer to understand these requirements and determine next steps.

5. Is disclosure simply the *right thing* to do?

Public disclosure is often an extremely uncomfortable action but is not without benefits. While it isn't appropriate for many circumstances, we recommend that you at least consider public disclosure even when it is not explicitly required.

Some additional benefits:

- Customers are increasingly receptive to transparency. A confident, voluntary disclosure can set you apart and be a powerful mechanism of building trust.
- Criminals thrive in secrecy. Sharing pertinent information directly contributes to our pooled defense, while keeping it secret increasing the likelihood of future victims.
- Absolute certainty that you've satisfied ambiguous notification laws.

Once you have determined that you will notify the affected individuals, it's time to prepare that notice. A good breach notification accurately addresses the following questions:

WHICH *users are impacted?*

WHAT *time window* did this occur?

WHAT is the *specific data* that was breached?

WHAT do you know about the *motives* behind the breach? Criminal attack? Inadvertent disclosure?

WHAT are *you doing to remediate* the breach and help the persons affected? Credit monitoring? Reset of credentials? Have you notified law enforcement?

WHAT can *affected individuals* do? Reset credentials? Review transactions? Initiate a credit freeze? Stay tuned? Nothing?

You may also consider publishing additional information that goes above and beyond what is required. For example, you may consider sharing specific indicators of compromise or a technical post-mortem to assist other defenders.

For further reading on preparing your first breach notification, we recommend Security Breach 102.

Breaches and Bounties

If you are operating a bug bounty program, it is critical that you employ a vocabulary that distinguishes between vulnerability and breach. A bug bounty program is not an invitation to be breached -- these programs encourage the discovery of vulnerabilities that *could lead* to a breach (if left undiscovered).

A properly structured bug bounty program will authorize participants to search for vulnerabilities so long as a specific set of rules are adhered to. All participants in HackerOne programs are under instruction to Respect Privacy and Do No Harm. Just as with any authorized security test, an inadvertent access of data by an authorized participant does not trigger statutory breach notification requirements.

Criminal Element

But what if someone demonstrates explicit disregard for the rules? They have a name: criminals.

For as long as criminals have been stealing data, some of those criminals have chosen extortion as their preferred method of monetization. Criminals will attempt extortion tactics whether or not you have a bug bounty program. Of course, the likelihood of a breach in the first place is reduced for those running a bug bounty program.

The decision on whether to pay a data ransom is a highly complex topic with significant disadvantages and advantages that must each be carefully weighed. While HackerOne is not in a position to provide conclusive guidance for all cases, we do provide the following general recommendations for bug bounty programs:

DO NOT pay a bounty to a participant who has willfully violated the program rules.

ALL BOUNTY AMOUNTS should adhere to your published policies. (Do not increase your bounty amounts in response to demands)

IMMEDIATELY "Request Mediation" if you suspect a hacker is acting in bad faith.

CONTACT law enforcement and/or a legal expert if you believe you are being extorted.

Be Prepared

"Never let a good crisis go to waste"

- WINSTON CHURCHILL

Now that the dust has settled, it's time to search for a silver lining. There are undoubtedly important lessons learned from this breach that are wasted if no one can study them.

Your technical post-mortem should be packed full of lessons learned that enable you and others to prevent a similar compromise from happening again. Convert these lessons and the story behind them into a rallying cry for your entire organization to implement the necessary changes. You'll never get a better opportunity.

Breach response is one of the most challenging tests of your security maturity. The best teams exercise these muscles regularly. My recommendation: Take one bug bounty report per quarter and immediately hand it to your red team to simulate a full data breach. Now run your incident response progress end-to-end: all the way up to a mock breach notification.

You'll be ready.

Alex Rice
Co-founder & CTO, HackerOne