InfoArmor

How to Create an **Employee Data Breach Response Plan** for HR

GUIDE

www.infoarmor.com

Table of contents

Introduction

Data breaches and security incidents are occurring in record number. Each year, cybercriminals cost U.S. businesses billions in lost revenue and steal millions of employee identities. This guide is designed to help HR fight back.

However, it should be noted that this guide is meant to help HR professionals prepare for future data breaches. If you are currently experiencing a data breach, please reach out to us immediately. You can do so by dialing 1.480.302.6701 or emailing us at info@infoarmor.com.

If you offer PrivacyArmor as an employee benefit, you have likely already been contacted by our dedicated Privacy Advocates. If not, please report the breach by calling 1.800.789.2720.

Step 1: Clarify HR's role in the response

Organize the data breach response team

Before you can create a meaningful data breach response plan, you first need to clarify what role HR will play in the context of your organization's data breach response team. If your company doesn't already have such a team in place, you will likely need to help assemble one.

A data breach response team should include (at mininum) members from the following departments.

- Information technology (IT)
- Human resources
- Legal
- Public relations
- Customer care
- Executive leadership

Map out responsibilities HR will oversee

Next, you'll want to map out the responsibilities your department will oversee. This will vary greatly depending on the size of your company, your available resources, and many other factors.

HR professionals traditionally handle the following responsibilities:

- Working with legal to ensure local, national, and international laws are obeyed
- Notifying employees in a timely manner
- Creating and disseminating FAQs
- Overseeing a live Q & A with employees
- Helping employees correct any issues caused by identity theft
- Working to prevent future data breaches

Identify interdependencies between departments

Once your data breach response team is organized, you can collectively determine the responsibilities each department will oversee and identify any dependencies. There will likely be many.

For example, HR will oversee informing employees that their data has been compromised. Yet, in order to effectively do this, the must work with:

- IT to understand technical details related to the breach, as well as understand what employee data was compromised
- Legal to identify and address any requirements set forth by local or international law (ex: GDPR)
- Public relations to ensure consistent messaging

Step 2: Identify the information you need to collect

The days and weeks following a data breach will be quite stressful, so you'll want to prepare as much as you can in advance. A good place to start is by creating a list of all the information you'll need to collect after a breach is identified.

This information will consist of five core areas: timing, causation, depth, company actions, and legal requirements. Keep in mind that you might not have all of the information immediately available, and what information you're given may change over time. For this reason, you'll need to be particularly careful with the verbiage you use when communicating with employees.

Here are a few of the questions you'll need to address.

Timing

- When did the data breach occur and how long did it last?
- When was the breach or security incident discovered?
- When was the problem corrected?
- If the problem is not yet fixed, when do you expect it to be?

Causation

- What or who caused the data breach?
- Did an internal or external threat cause the breach or incident?
- If the breach wasn't caused by human error, what was the motivation of the attack?

Depth of breach

- What types of data were exposed?
- What types of data were NOT exposed?
- Were healthcare records compromised?

Company actions

- What actions is the company taking to prevent future breaches?
- How is the company going to protect employees following the breach?
- What identity protection service is the company providing?

Legal

- What local and national laws apply to data breach disclosures?
- Are any employees located in the EU or are otherwise subject to GDPR protection?
- What actions can you take to limit corporate liability?

Step 3: Prepare response templates and procedures in advance

You can save yourself a lot of headaches and stress by developing response templates and procedures in advance of a data breach. Here are some of the most important.

3A: Create an employee notification template

We've included a link to a sample breach notification template your organization can use when creating your own template. While certain elements will depend upon breach-specific details, you can proactively fill a a number of fields. Just remember that this template is just a guide, and you'll need to customize it to meet the unique needs of your organization. You'll also need to run it past your legal department to ensure it complies with all applicable local, state, and federal laws.

Data Breach Notification Template

3B: Prepare sample FAQs

Likely, you will have answered many questions an employee might have in your initial breach notification response. However, you should still provide employees with an FAQ that is easily accessed and can be updated with new information as it becomes available. We've included a link to a sample document you can use below.

As is the case with the Data Breach Notification Template, you will need to customize this template to meet the needs of your organization and run it past your legal counsel to ensure it meets all local, state, and federal laws.

FAQ Template

3C: Outline a structure for a Q&A

Following a data breach, one of the most significant duties of an HR professional is to remain calm and provide guidance and reassurance to any affected employees. Hosting or moderating a live question and answer session can be particularly effective at achieving this.

When structuring your Q&A, we recommend you address the following critical areas.

Where will the Q&A take place?

Company dynamics will significantly impact the format your Q&A will take. If you work for a smaller company and employees are centrally located, you can likely host the event in person at your office.

However, if you're a large firm or have employees located nationally or internationally, this format wouldn't be best. Instead, a live webcast might meet your needs. If that's not possible, then consider hosting a conference call. The most important element is that employees should be allowed to participate.

How can employees submit questions or concerns?

You should give employees an option to submit questions in advance of the Q&A. This can provide valuable insight into how you should approach certain topics, and it will help you gauge what issues are the most pressing for your employees.

Additionally, you should allow employees to submit their questions or concerns anonymously. Finally, dedicate a healthy portion of time to addressing employee concerns at the end of your address. It's better to end the Q&A earlier than expected then to run out of time before any outstanding needs.

Who will participate?

Next, you'll need to determine who should participate in the Q&A. It's a good idea to have the entire data breach response team available. If that's not possible, you must have at least the following:

- IT representative — a person with knowledge of the threat/vulnerability should thoroughly explain what happened and outline the steps your organization has taken to prevent future threats from occurring
- Leadership representative — senior leadership should have a strong presence during the Q&A to illustrate that the company is aware of the situation and taking it very seriously
- HR representative — a senior HR representative should be on hand to address employee concerns and provide insight into what actions employees should take to protect themselves

Step 4: Routinely practice your data breach response plan

Practice makes perfect, especially when it comes to your responsiveness during an actual emergency. For this reason, you'll need to routinely practice your data breach response plan. Experts recommend doing this at least twice a year. At an absolute minimum, you should conduct simulations yearly.

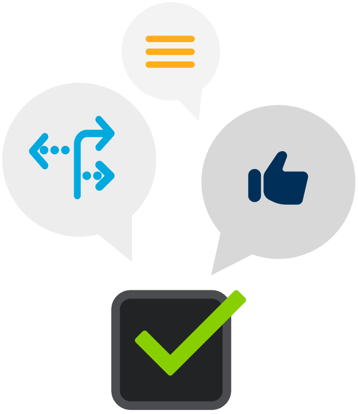
The following tips will help you get the most out of your practice drill.

Hire an outside party to administer the simulation

If possible, hire an outside party to administer the simulation. This will allow you to focus your energy on the exercise. Additionally, by allowing another party to determine critical breach factors, such as the types of data exposed and what event caused the compromise, it will make the simulation more realistic!

If you're not able to work with an outside party, then have a co-worker who will not be participating in the drill make critical decisions about the nature of the simulated breach.

Test multiple scenarios



You've already scheduled a date and committed a significant amount of resources to run a simulation, so make sure you get the biggest bang for your buck. Test multiple scenarios and variations.

For example, consider how different your response would be to each of the following scenarios:

- A hacker exploited a vulnerability in your website and has compromised sensitive data. (For this type of drill, it's best to have a dummy site created with an actual vulnerability. This way your IT/ security team can practice identifying and correcting the issue, while you work on messaging.)
- A cybercriminal is attempting to sell corporate data on the dark web. The identity thief claims that employee records are part of the offer, but the authenticity has yet to be confirmed.
- A rogue employee has accessed sensitive corporate data and is attempting to blackmail the company.

For example, consider how different your response would be to each of the follow

Allow for a comprehensive debrief

At the conclusion of your simulation, plan for a comprehensive debrief. If you're working with an outside firm, they'll likely provide you with a detailed analysis of your performance, along with recommendations for improvement.

If you're running the simulation internally, you'll need to analyze your performance as objectively as possible. Determine what you got right, which areas need a little work, and what parts of your response were just plain wrong.

Don't beat yourself up over the failures. When errors occur during a simulation, you reduce the chances of them occurring during an actual event. That's why the greatest minds recommend "failing often and early!"

Step 5: Take steps to prevent data breaches from occurring

Of course, the best way you can prepare for a data breach is to take steps to prevent one from occurring in the first place. This is something we cover in great detail in our complimentary ebook, The HR Guide to Employee Data Protection and Identity Theft Prevention. The following excerpt from the guide contains action items every organization should enact to protect themselves from the dangers of hackers, identity thieves, and cybercriminals.

5A Provide thorough and continuous training

The risks of identity theft and security breaches

When educating your employees, begin by conveying the risks that identity theft and security breaches pose. Explain that these violations don't just cost the company a fortune; they can also have a tremendous impact on employees. If team members have their identities compromised, it can take hundreds of hours and months of the victim's life to fully repair.

How to handle personal data

Working with your IT department and senior members of management, craft a document that outlines the best policies for handling, storing, and accessing the personal data of employees. A few items to consider might include:

- What information about employees should be stored on the network
- Who should be allowed to view or edit sensitive employee data
- How, and under what circumstances, this data should be shared
- Where it is acceptable to access this information and where is it not (ex: public wifi)
- How this data should be stored and encrypted
- What steps to take if sensitive data is compromised

Recognizing and preventing various cyberattacks

Train your employees on how to identify and avoid cyberattacks, especially phishing emails. If you spot the signs below, chances are the email is actually part of a phishing scam:

- Misspellings and grammatical errors throughout
- Missing or incorrect contact details in the signature line
- The email doesn't sound as if the sender wrote it
- The salutation is oddly worded or contains vague terms like "employee"
- When you hover over a link, it reveals a different URL than stated
- A request for large amounts of private data from a company executive that seems oddly timed or out of place
- Something just feels off

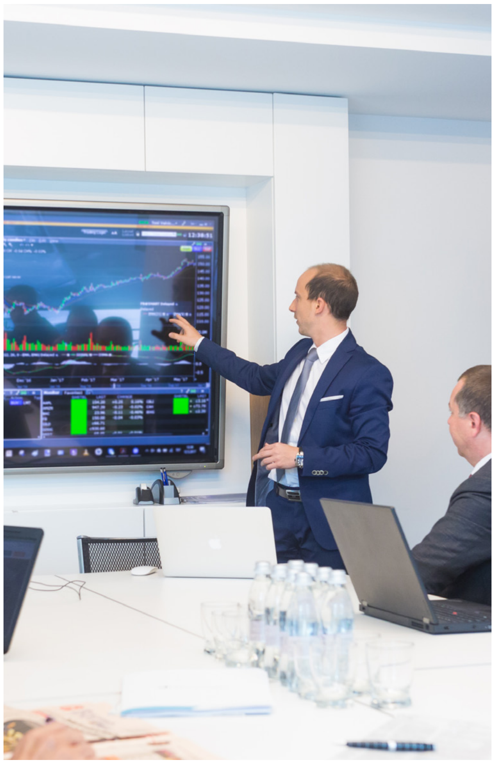
If an employee encounters any of the above issues, they should contact their manager, along with HR and IT immediately.

Warning: When checking email with your phone, you need to be especially careful. Typically, people are more distracted when using a mobile device versus a desktop, and it's also much harder to hover over a link before clicking it and to thoroughly check for misspellings. Make it a practice to always exercise more caution on your phone.

5B: Develop a comprehensive cybersecurity plan

Work alongside your IT department to create a robust cybersecurity plan. While there are many questions you must answer, here are a few fundamentals you should consider when developing your strategy:

- How will you encrypt files that contain sensitive data, like employee records and all other confidential data?
- How will you conduct internal risk assessments?
- Who will oversee continued training for employees and managers?
- Should you hire an outside team to assess your network vulnerabilities?
- Who will compose your in-house team to address security issues?
- How should you structure an incident response policy?
- What will the plan be if employee or customer personal data is exposed?



5C: Offer identity protection as an employee benefit

The chance your employees may become victims of identity theft is staggering — more than 80 percent of working adults had their identity compromised in 2017 alone. That can translate to a lot of lost productivity, missed work hours, and a huge financial loss. However, providing your employees with an identity protection service can help your workers tremendously and insulate your company from many associated risks.

Just as important, an employee identity protection benefit also improves corporate security. Here are a few ways it accomplishes this.

Employee identity protection helps educate your employees

A quality identity protection benefit will provide ongoing education to your employees and update them to any important updates across a wide range of pressing issues.

This education might include:

- Sharing best practices for creating passwords, safeguarding accounts, and taking other actions that bolster corporate security
- Revealing the latest tactics hackers, identity thieves, and cybercriminals are using to attack employees and their employers
- Alerting participants to data breaches and security incidents in a timely fashion

Identity protection can safeguard employee social media accounts

If cybercriminals can gain access to an employee's social media account, they can cause a great deal of harm to the victim's employer. With a hijacked account, a hacker can use it to defame your business, phish fellow employees, and defraud customers, clients, and partners.

A quality employee identity protection plan will monitor your employees' social media accounts and alert them at the first sign of account takeover. This ensures the problem can be remedied in the shortest possible time — significantly limiting the risk to your employee and your business.

Keeping security top of mind

One of the most significant benefits identity protection offers is the least detectable: it helps keep corporate security top of mind for employees.

When an employee is notified of important security risks, compromised credentials, or suspected hijacking, their levels of awareness aren't limited to their personal privacy and security. They begin making better decisions that positively impact their employer as well, including:

- Creating more secure passwords
- Not sharing passwords with co-workers
- Becoming more aware of phishing scams
- Using more secure networks when working remotely

Creating a safer work environment

If you'd like to improve corporate security in your organization, it's a good idea to consider offering your employees a quality identity protection benefit. However, be certain to identify the key features your organization needs and compare those amongst providers, as offerings vary greatly.

If you'd like to learn more about how identity protection can help your corporation, or you're looking for additional ideas on how to keep your employees safe, you can download our complimentary ebook, The HR Guide to Employee Data Protection and Identity Theft.

Would you like to experience PrivacyArmor for yourself? You can request a complimentary, no-obligation demo of our employee identity protection benefit offering.

InfoArmor

InfoArmor, Inc.

7001 N Scottsdale Road, Suite 2020 Scottsdale, AZ 85253
Email: info@infoarmor.com

800.789.2720
www.infoarmor.com