12 Steps to Take Before and During a Data Breach

by | **Lillie Conrad, Zachary Willenbrink** and **Charlie Gibbs**

Minimizing the impact of a data breach requires good preparation and a proactive response from employee benefit plans. Important steps include developing and practicing an incident response plan as well as assembling the right team of experts.

Your organization, like many others, probably recognizes the severe risk that a data breach poses. No one wants their employees' or benefit plan participants' personal information to be stolen. No one wants their computer systems to be down, particularly during critical times (and yes, threat actors often lurk on systems until the moment their attack will cause the most disruption). Certainly, no one wants to deal with the regulatory and litigation headaches that can follow even the least intrusive breaches.

But, also like many others, your organization may not have thought about what to do if—or, more pragmatically, when—a breach occurs. Even the best laid plans to prevent a breach sometimes fail but, with good preparation and a proactive response, you increase the likelihood of containing a breach or at least recovering as quickly as possible.

Employee benefit plans are attractive targets for hackers because they possess a lot of sensitive information and may have access to money. They also use a variety of third-party service providers, which may make them more susceptible to attacks. Health care information also has a high value on the dark web, and some benefit plans may have limited in-house technical expertise.

This article will offer 12 steps you should take before and during a data breach to ensure the best possible outcome for your employees and benefit plan participants as well as the organization as a whole.

Prepare for a Breach

1. Establish an Incident Response Plan

If you've developed an incident response plan, you can respond by seamlessly working through that plan instead of responding to the discovery of a breach as most people do (with head-scratching and/or expletives). Those procedures should be easy to follow, define roles clearly and still leave enough flexibility to address a constantly evolving situation. You won't be able to draft this plan overnight. You should gather input from stakeholders across your organization, identify the employees or positions who will assist, and gather any information that could be useful during the breach (like the contact information of your cyberliability insurer and any experts you previously worked with). If you don't know where to begin, contact your cybersecurity insurer or an attorney, who can help or provide a referral.

Recent cybersecurity guidance from the Department of Labor suggests that benefit plans develop a formal, well-documented cybersecurity program, including a business resiliency program that addresses incident response.

2. Review Your Cyberinsurance Policy—or Get One

First, make sure you have cyberinsurance. Most general liability policies exclude cyber-related losses, so if you don't have a specific cyberinsurance policy, it is important to consider whether you need to get one.

When reviewing coverage, you should consider issues such as how quickly you will hit your policy limits if you suffer a breach. With attorneys, outside experts and reporting obligations among the many costs, this will probably occur sooner than you expect. Find out what types of expenses your policy will cover and what it excludes. It may cover the ransom the threat actors demand, but it may not reimburse for the week-long business interruption you suffered (or vice versa). Often, cyberinsurers will even connect you with preapproved companies to help prepare for or react to a breach, including forensic investigators and public relations specialists. Some cyberinsurance policies cover a limited number of hours for this kind of work, but some policy holders fail to take advantage of it.

takeaways

- Employee benefit plans are attractive targets for hackers because they possess a lot of sensitive data, including health care information.
- One of the first steps in preparing for a data breach is to develop an incident response plan, which will outline procedures to follow and clearly define roles.
- Benefit plans should consider purchasing a cyberinsurance policy and review coverage to make sure they are aware of expense limit and coverage exclusions.
- Communication is a critical element to consider before and after a breach. Benefit plans should prepare basic holding statements to have ready if a breach occurs. All communications should be carefully vetted before being sent.
- Following a breach, benefit plans should pay attention to the forensics data uncovered for lessons on how to avoid similar attacks in the future.

Another item to consider is whether you have met (and sustained) compliance with any requirements imposed by your policy. Given the ever-increasing risk of a data breach, many cyberinsurers now require their clients to train their staff and meet other conditions for coverage to be effective.

3. Identify Outside Experts, Including a Breach Coach

After determining that your cyberinsurance policy offers the right amount of coverage and will work how and when you want, you should work with your insurer to identify the experts to call on in times of crisis. Among those experts, a "breach coach" is perhaps the most important. This coach is typically a lawyer who understands the life cycle of a breach and can therefore help ensure you comply with all short- and long-term obligations, such as notification requirements. Other outside experts you may want to establish a relationship with include information technology (IT) forensics/recovery experts and notification providers. Many of these third parties may even contract in advance so that they can assist you immediately. This can cut hours or even days from your response time in a situation where there often is not a second to spare.

4. Practice, Practice, Practice

A good plan goes only so far and will be of little help if you can't execute it. So, after your plan is in place and you know who you expect to work with (both inside and outside of your organization), practice implementing the plan as if responding to an actual incident. In the parlance of the industry, this is called a *tabletop exercise*. Practicing your response with one or two "tabletops" per year will identify areas that can be improved and give the team a better idea of what to expect when an incident occurs.

5. Map Your Data

To effectively respond to a data breach, you first need to know what data is at risk. *Data mapping* is the process, often conducted by in-house IT departments or outside vendors, of identifying what data you have, where it resides on your systems and how it is protected in each of those locations. With that baseline information, it will be much easier to determine which data may have been affected and the ultimate nature of a system compromise, if any—which, in turn, can have far-reaching implications on reporting and notification obligations.

6. Know What to Say

Every incident differs, but almost all require employers and benefit plans to communicate with large audiences. Sometimes, that means communicating internally with employees; in others, that means communicating with clients, regulators and even the press. Although you can't predict exactly what you will tell those people in the event of a breach, there are often general themes to explain—and some topics to avoid. Having basic holding statements already prepared will cut down on the time preparing communications, allowing you to better focus on the substance of the incident and addressing it as quickly as possible.

Execute Your Plan if a Breach Occurs

7. Assemble Your Team Quickly

Commissioner Gordon had the "Bat Signal." Ron Burgundy had a magical conch shell. Whatever means you decide to use—and, let's be honest, it's probably going to be a boring old phone call or email to a distribution list—your first step is to call in your team. The internal team should include—at a minimum—IT, risk management, legal, human resources (HR), communications and other business representatives, as applicable. Even if you aren't certain that the situation is a full-on, confirmed breach that is impacting all of your systems, it is better to err on the side of caution. An extra 30 minutes for your internal communications team or outside forensic response team can make a world of difference.

8. . . . But Communicate Carefully

Speed, of course, isn't everything, so you'll need to balance your speed with due care. Mindful, careful communications are not always intuitive in a breach situation, but a few concepts based on the most basic questions—who, what, when, where and how—can help put you in the right mindset to communicate internally or externally.

First, be careful *what* you say. Whether a "breach" occurred is typically a legal determination. Exactly what is happening on your systems often can't be stated with certainty in the moment. When sending out your first communication, be accurate but succinct about what is going on: Your IT team has identified suspicious network activity, or there's an ongoing cybersecurity incident that needs a response. Leave any final determinations to the end, after the crisis has passed and everyone can think more clearly and with a fuller

bios

Lillie Conrad is an attorney at Godfrey & Kahn s.c. in Appleton, Wisconsin, where she is a member of the firm's technology and digital business practice, supporting its data privacy, cybersecurity and technology transactions teams. Prior to joining the firm, she worked as in-house counsel for a Fortune 200 consumer products company as the company's lead attorney for global data privacy and protection matters. Conrad holds a J.D. degree from Marquette University Law School and has earned the Certified Information Privacy Professional/US (CIPP/US) and Europe (CIPP/E) certifications from the International Association of Privacy Professionals (IAPP).

Zachary Willenbrink is an attorney at Godfrey & Kahn s.c. in Milwaukee, Wisconsin, where he is a member of the firm's litigation practice and its technology and digital business practice, supporting its data privacy, cybersecurity and technology transactions teams. He helps clients navigate data privacy, intellectual property, noncompetition, trade secret, trade practices and other complex commercial and business disputes. Willenbrink holds a J.D. degree from Marquette University Law School and has earned the CIPP/US certification from IAPP.

Charlie Gibbs is a paralegal at Godfrey & Kahn s.c. in Milwaukee, Wisconsin, where he works in the firm's technology and digital business practice group, supporting its data privacy, cybersecurity and technology transactions teams. He assists in multiple aspects of data breach response such as conducting research regarding state notification requirements and preparing notices to state attorneys general. Gibbs also assists in preparing internal and external-facing client policies and terms and co-presents tabletop exercises to clients. He has served on the board of the Wisconsin Technology Association as vice president for programming.

record. This is particularly important for email traffic, which often must be disclosed in litigation.

Second, be careful *how* you say it. If your email server has been compromised, you might not be able to send an email on your system. Regardless, you probably don't want to since the threat actor might be reading every word of your response strategy. Identify an alternate method in your recovery plan. Some organizations use devoted email accounts on another server that are set up in advance, which means their communications can take place on an unaffected server without commingling work and personal emails. Others agree that they will text each other or use an encrypted messaging app. There is no "right" method of communication here, and it could differ depending on the nature of the breach. So, be flexible—while also being careful—in what you choose.

Third, be careful about the other W's: who, when and where. Any communications beyond your response team should be carefully vetted before being sent.

Who are you sending the communications to? An internal group of employees is, of course, different than an external group of media reporters.

When are you going to send the communication? You don't want to leave anyone—employees or clients—wondering what is going on and whether they've been affected. But, you also want to make sure that you are providing reliable information. Communicating too soon risks giving out information that is bad—in two senses: It can be both unreliable and potentially more detrimental to you than is actually the case—and you may have to retract later, making it seem like you're providing inconsistent answers.

Finally, *where* are you going to publish the communication? Again, there are many scenarios here, each with different implications: a formal, statutorily required breach notice vs. an organization-wide email; a message on your website vs. a press release that you will highlight.

9. Maintain a Time Line

As study after study shows, memory is inherently fallible—and even more so in a high-stress situation like a breach. Don't rely on your memory alone to reconstruct your response efforts after the fact. Instead, maintain a time line of exactly what you are doing and when you are doing it. This will make later determinations and decisions, such

as whether there was actually a breach and whether notifications are necessary, much easier.

10. Preserve Evidence

The unfortunate reality is that a breach is often followed by a dispute. Affected individuals or companies may sue. A regulator or law enforcement agency may start an investigation. That unfortunate reality will only get worse if you destroyed the evidence—such as emails, computer logs or that just-mentioned time line—that plaintiffs, a court or others will ask to see. Even if destruction was inadvertent, perhaps caused by an automatic purging of files, it can still lead to more serious problems later. Talk with a lawyer and your IT team to issue and effectuate a litigation hold, pause any automatic deletion processes or retention policies, and back up other important items like documents and logs.

11. Notify Your Cyberinsurance Carrier

Remember all those benefits we listed in suggesting you review your cyberinsurance policy? None of those mean anything if your insurer doesn't know about the incident. Make sure that you include this notification in your incident response plan and remember to make the call on time.

12. Listen to the Forensics

Whether it's your own IT team or an outside expert, pay close attention to what they determine happened on your system. The data they uncover is important for determining whether you actually suffered a breach or were just a target that successfully defended itself. And that determination will ultimately influence whether you report the incident. Beyond the immediate reporting decision, though, understanding what happened forensically will give you and your team a better sense of how to avoid the same type of attack in the future. Incorporate any lessons learned into your security plans, data defenses and especially your incident response plan.

Conclusion

Whether it's five, 12 or 50 items long, no list could capture every possible suggestion or best practice, and this one is no exception. Your ultimate goal should be to avoid a breach entirely, which entails enterprise-wide cybersecurity training, good hiring practices and tailored training for your IT teams and employees who are most likely to be targeted, as well as investment in your technological infrastructure.

An entirely separate list could be written on that topic. And, even on the specific topic of responding to the worst-case scenario of a breach, others may have entirely different ideas about what should be on this list. The expanse of best practices can be overwhelming to consider, but focusing on the basics of cybersecurity preparedness laid out in this article is a great place to start. With strong preparation and response, you significantly increase your organization's opportunity to contain and recover from a breach.

benefits MAGAZINE

Reproduced with permission from *Benefits Magazine,* Volume 59, No. 3, May/June 2022, pages 18-23, published by the International Foundation of Employee Benefit Plans (www.ifebp.org), Brookfield, Wis. All rights reserved. Statements or opinions expressed in this article are those of the author and do not necessarily represent the views or positions of the International Foundation, its officers, directors or staff. No further transmission or electronic distribution of this material is permitted.

pdf/422