iapp

7-Step Guide to Data Breach Preparedness

How to create your incident response dream team

WELCOME

Forty-three percent of companies suffered a breach in 2013 alone.
—Ponemon Institute

“An ounce of prevention is worth a pound of cure.”

That’s never been more true when it comes to data breach preparedness. Forty-three percent of companies suffered a breach in 2013 alone, so it’s safe to say that data breaches are essentially inevitable for any firm with substantial data holdings.

That puts the onus on CPOs and privacy leads to studiously plan for the day when breach response is needed.

While there are a number of data breach guides out there, this one focuses on how to identify the correct stakeholders and build critical relationships—both inside and outside your organization—to make sure you can respond efficiently and effectively in the event of a breach.

These seven steps will give you a roadmap for building a team that is ready for a rapid and coordinated response. Along the way, you’ll be better prepared to prevent a breach from happening in the first place.

Sam Pfeifle, Editor
IAPP Publications Director

Dennis Holmes
IAPP Westin Fellow; Experienced Associate, PwC

If you’re interested in more information about data breach preparedness and response, the complete whitepaper version of this guide is available online exclusively to IAPP members.

TABLE OF CONTENTS

STEP
01

BRING YOUR A-GAME

BUILDING YOUR INTERNAL INCIDENT RESPONSE TEAM

Companies that suffer a breach without having put an incident response team in place often waste valuable time trying to get organized and assign or define responsibilities, stalling the breach remediation process.

Ideally, the incident response team should include representatives from all of your company's functional groups. There's no way to know in advance what parts of your company will be impacted by a breach, so it's best to have at least one staff member in each functional group who is trained and prepared to handle responsibility of breach response.

This ensures that every relevant employee knows whom to contact, from whom to take direction, and what to do in the event of a data breach. It also ensures that all employees understand their department's role in the incident response process.

KEY PLAYERS

- IT
- Security
- Legal
- Compliance
- Communications
- Customer service
- Executive management

It's important to have a team that is well-versed in privacy and security matters that can take the lead in handling the incident response.

YOUR ALL-STARS: Team Roles and Functions

IT AND SECURITY

Because they're most familiar with your network systems and security controls, your IT and security team plays a central role in helping you identify what information was compromised.

In most cases, the IT and security staff lack the specialized skill set and training to perform digital forensic investigation. However, given their intimate knowledge of your systems and controls, they are best equipped to assist the outside forensic team with their investigation.

LEGAL AND COMPLIANCE

Identifying the notification, legal and regulatory requirements of the breach response is the main purview of the legal and compliance team. This includes determining if there is an obligation, contractually or under applicable laws and regulations, to notify external organizations, clients or business partners and, if so, what the content of the notification must be.

Legal and compliance staff will take their orders/direction from your organization's breach coach/counsel to satisfy legal and regulatory obligations.

COMMUNICATIONS

In our increasingly digital world, good news travels fast and bad news travels faster, so it's imperative that your communications team is involved in the breach response as early as possible.

They're in charge of the internal dissemination of breach information, rallying the internal team and making sure that employees have talking points should they be approached.

TIP

Your communications team should refrain from making any external communications about the breach. A PR firm **that specializes in crisis communication** should handle external communications, with assistance and direction from your communications team.

CUSTOMER SERVICE

After a data breach, customers have lots of questions, especially if they suspect that they are victims of fraud.

Your organization's customer service staff has a crucial role to play in the breach remediation process: rebuilding customer trust.

Customer service staff field the calls of consumers impacted by the breach, answer their questions and explain how to enroll in credit monitoring or identity theft management programs, if offered.

TIP

When the anticipated call volume is higher than can be handled internally, most companies engage a call center and set up a dedicated customer hotline. Other companies have created websites that provide FAQs and information on fraud and identity theft protection. Regardless of which approach you choose, you should **leverage the insights your customer service team has gained** from regular interactions with your clients to win back customer trust in the midst of a breach.

TIP

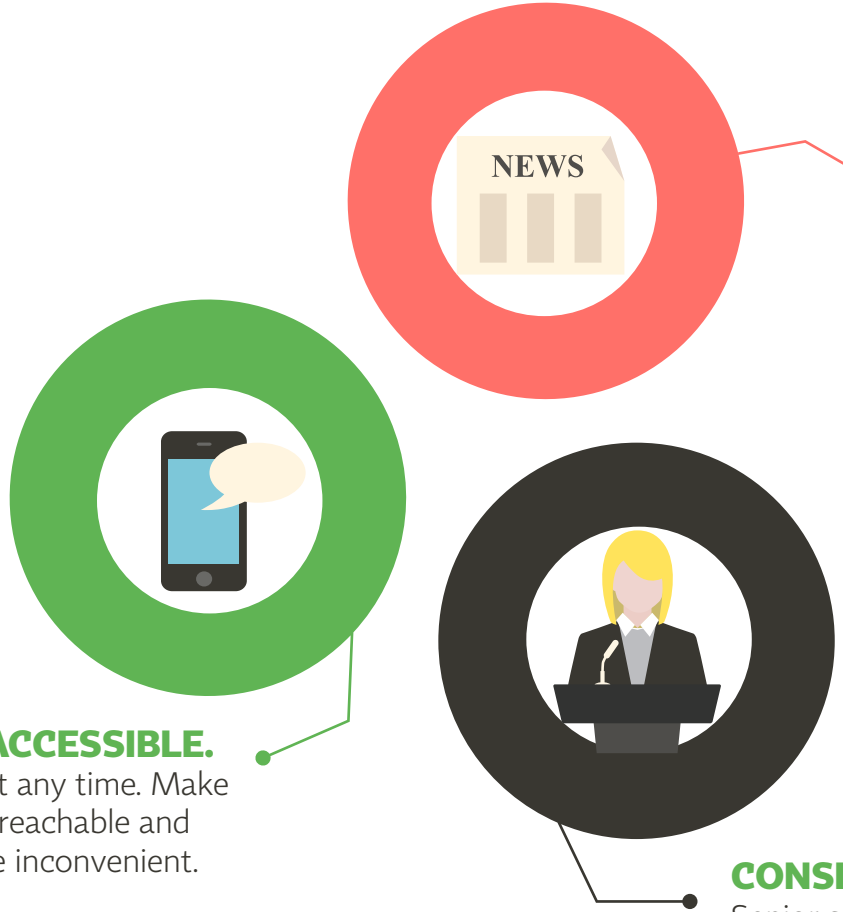
It's not always possible for an executive to commit to being on the team. In lieu of this, some companies have appointed an **incident response team lead with delegated authority** to take certain actions and make decisions. In addition to their leadership responsibilities, this person provides the executive management team with regular status updates. This can be a good alternative if no management-level executive is able to join the incident response team, but it is slightly less efficient when situations arise that exceed the delegated authority and require approval from the executive management team.

EXECUTIVE MANAGEMENT

Ideally, you should have a management-level executive with broad decision-making authority on the incident response team. Their broad authority can help the breach response process move more quickly.

A management-level privacy or security professional is best positioned for this role.

TIPS FOR PICKING YOUR TEAM MEMBERS



YOU NEED MEDIA SAVVY.

Breaches can attract lots of media attention. Have at least one media-savvy person on the team that you can call upon to act as spokesperson should the need arise. Alternatively, you can also offer media training to members of the team after they've been chosen.

MAKE SURE THEY'RE ACCESSIBLE.

A breach can be discovered at any time. Make sure your team members are reachable and available, even when it may be inconvenient.

CONSIDER PRIVACY AND SECURITY KNOWLEDGE.

Senior staff don't always have solid privacy and security knowledge. Consider the level of privacy and security training when selecting staff members from each of your company's functional groups, rather than selecting senior staff by default.

STEP
02

DON’T REINVENT THE WHEEL

RE-EVALUATING EXISTING PRIVACY AND SECURITY SYSTEMS AND PROCEDURES

The most effective incident response plans use existing privacy policies and procedures as a framework. Why do this?

1. It gives you the opportunity to review your policies and get a clearer picture of the preventative measures already in place.

2. It helps to avoid duplication of effort.

   Example: If you already have a privacy incident documentation protocol it probably isn't necessary to develop new protocol for breach incidents as a part of the incident response plan. Instead, just expand the documentation protocol to include breaches.

3. It can highlight your organization's privacy and security vulnerabilities as well as its strengths. Identifying weaknesses is a critical part of developing an incident response plan.

   Example: If your review reveals that it is difficult to locate either physical or electronic copies of established written privacy policies, then perhaps the policies are not the issue but rather the communication and visibility of these policies.

! **THE BOTTOM LINE:** Use your existing privacy policies and procedures to establish a baseline and revisit those policies to identify any latent vulnerability that should be addressed in the incident response plan.

STEP
03

MAKING FRIENDS

ESTABLISHING RELATIONSHIPS WITH LAW ENFORCEMENT, REGULATORS AND BREACH RESPONSE SERVICE PROVIDERS

Establishing these relationships is an important part of your breach preparedness for three reasons:

1. Having a prior relationship with law enforcement can make the process of catching the criminal or criminals who breached your company proceed more smoothly.

2. It prevents a breach investigation from being your first introduction to a regulator.

3. It helps you avoid the de facto practice of selecting a vendor in the midst of a breach crisis.

The ROI on Breach Response Providers

Speaking with breach response service providers can yield some real concrete benefits:

- **Cost-savings.** Without the time pressure of a live breach, you gain the opportunity to negotiate for lower prices.

- **Effectiveness.** Beyond cost-savings, relationships and contracting with breach response service providers before a breach gives you major advantages in the response planning process that can help make your incident response plan most effective.

TIP

Introducing yourself to a regulator before you have a data breach shows that you're being proactive, which could **help you earn the regulator's trust and respect**—especially important if you do experience a breach.

FOUR VENDORS YOU'LL WANT ON SPEED DIAL

1. COMPUTER FORENSICS

Computer forensics services are usually the first provider engaged by the breach counsel after a breach happens. But, you don't have to, and shouldn't, wait until you have a breach to engage a computer forensics firm.

In fact, given the critical breach response function, you should contact a computer forensics firm long before your organization discovers it has been breached.

Why? Time.

The major advantage of identifying and hiring a forensics firm during the incident response planning process is that there's time for the forensics team to get familiar with your IT network.

The systems administrators at your organization are familiar with your IT infrastructure and network environment. They know key details about the network environment, like how the system is backed up and any security controls in place. But the forensics team you bring in after a breach is not. For most companies that will prove to be a huge, time-consuming and cost-increasing problem.

Giving the digital forensics firm you hire time to become familiar with, and understand, the landscape of your company's IT infrastructure will help them work more efficiently when they are called upon to respond to a breach. Time that would otherwise be spent getting acclimated to your IT infrastructure will instead be focused on the investigation of your breach and will likely lead to a more expeditious technical remediation.

Additionally, they can also recommend software and security protocols that can help you increase your chances of avoiding a breach altogether.

The forensics firms consulted for this report explained that the total cost of their services was higher when responding to a breach for a client with whom they had no prior relationship.

2. CONSUMER SERVICES

The main advantage of engaging and contracting with consumer services providers prior to a breach is—you guessed it—financial. Particularly, as it relates to the credit monitoring remedies.

Pre-breach, you have significantly more bargaining power because there's no urgency or immediate necessity for the services. So, rather than paying the sticker price for one variety of the monitoring remedies, you can, and should, negotiate pricing for the remedy or remedies your organization wants to offer affected individuals after a breach.

What exactly are consumer services?

Consumer services refers to a variety of companies that offer one or more of the following:

- Call centers
- Notification to affected customers
- Identity monitoring
- Identity protection and repair

TIP

There are numerous companies in the consumer services market that offer different types of products and services at varying price points. **Devote some time to exploring the different options available** and learn what risk or problem the products seek to address. This ensures that your company can ultimately choose the products and services that make the most sense when a breach happens. If you wait, you run the risk of having to hastily choose a suite of products and services that may not be the most appropriate for you.

3. PUBLIC RELATIONS

Your PR firm is one of your most critical services for breach remediation, and you should develop this relationship as early as possible.

Your message to the public and affected individuals, during and immediately following a breach will have lingering effects—positive or negative. You don't want to put your organization in a position where your message to consumers is hurriedly drafted instead of carefully and tactically composed.

TIP

Working with a PR firm before experiencing a breach can improve the flow of information through an organization during a crisis. **In the midst of a crisis, information tends to travel in a quick, uncontrolled manner without any regard for accuracy—much like a game of "Telephone."** Your PR firm can help you establish a core crisis communication team, build the infrastructure and identify the chain of communication for crisis notification so as to avoid the "Telephone" scenario in the midst of your breach.

Why a PR Firm Should Be One of Your First Calls

Perhaps more than the other breach response vendors, many of these crucial tasks performed by the PR professionals could be prepped, and even completed, before the breach occurs:

- **Crisis communication training for customer service and other client-facing personnel**
- **Template scripts and other breach-explanation content**
- **Identifying your organization's key audiences**

4. LEGAL SERVICES

Identifying and retaining legal counsel prior to experiencing a breach is critically important. It gives you time to shop around and thoroughly vet the firms or attorneys you may be considering. Seems like a no-brainer, but more often than you might think, companies are blindsided by a breach and have to lawyer-up without time to thoroughly investigate their options.

The benefits of developing your legal services relationship now are two-fold:

- **Financial:** Because there's no immediate need for services, you'll have an opportunity to negotiate better rates.

- **Operational:** In the event of a breach, your breach counsel acts as the quarterback for your breach response. Having that person in place and readily available can save important time you would otherwise spend seeking counsel or asking your current counsel, who doesn't have extensive breach experience, to quickly begin research.

SPECIAL SUPPLEMENT: CYBER-LIABILITY INSURANCE

Cyber-liability insurance is a fast-growing, specialized type of insurance that provides policyholders with coverage in the event of a cybersecurity incident.

If you don't already have a cyber-liability insurance policy, part of your incident response planning should include an assessment of whether cyber-liability insurance makes sense for your company.

Generally, coverage falls into one of two categories: first-party or third-party losses. Although there is some variance among providers about what is considered a first-party or third-party loss, typically the following expenses in each category are covered.

First-party Losses
These are expenses incurred as a direct result of responding to the breach. They include, but aren't limited to, costs associated with the following:

- Computer forensics
- Public relations
- Notification of affected parties (mailing and printing costs)
- Legal services
- Call centers
- Restoration of systems or data
- Civil fines and penalties (costs to investigate, defend against and eventually pay fines may or may not be covered)

Third-party losses
These are expenses incurred as a result of claims for damages brought by customers, consumers or outside business entities. Third-party losses also include:

- Attorney fees
- Expert fees
- Defense costs for these third-party claims
- Regulatory fines that may be assessed under privacy statutes

What You Need to Know about Vendor Networks

Many insurance carriers also have guidelines regarding which breach response vendors are eligible for full coverage under the insurance policy. Typically, they use one of three approaches:

1. **Closed Network**—The insurance carrier has a direct relationship with a network of vendors. Policyholders must choose vendors from within this network to get full coverage. If you choose a vendor outside the network, insurance won't cover it.

2. **Preferred Network**—In this hybrid approach, the insurance carrier has a network of preferred vendors that are eligible for full coverage. Policyholders are allowed to use any breach response vendor they choose; however, there's less coverage if you choose a vendor outside the network.

3. **No Network**—The insurance carrier allows policyholders to choose the vendors that they want to use, but prior approval is necessary. Typically, approval is easy and could be as simple as an email.

All companies should consider getting cyber-liability insurance. In the unfortunate event of a breach, the potentially exorbitant breach response costs would be largely covered by your policy. If the insurance premiums are a concern, you should know that some insurance carriers offer reduced rates for companies with an incident response plan in place.

Tips for choosing a cyber-liability policy

- **Research your options.** Understand the various policy structures in the marketplace, so you can get the coverage that is most appropriate for your organization. For example, would a pre-vetted network of service providers be beneficial or does your organization already have preferred providers in mind?

- **Know the rules.** Be sure you understand the policy's rules on vendor selection. The primary reason to buy cyber-liability insurance is to reduce your company's out-of-pocket expense for breach response. Understanding what restrictions, if any, exist on your ability to choose vendors is an important consideration before selecting a carrier and plan.

- **Find out what *isn't* covered.** Pay close attention to limitations for each covered expense, and identify any monetary caps, exclusions or other exceptions to full coverage. Insurance policies can easily look comprehensive if you only consider what coverage is provided by the policy, without identifying what coverage is not provided.

STEP
04

THE DRY RUN

CRISIS SIMULATION

Now that you have your internal and external breach response teams in place, it's time for a dry run.

It's important to know how you would fare during a breach crisis and identify any gaps. There are a number of approaches, but the privacy pros we consulted for this report recommend doing both a tabletop exercise and a live simulation.

THE TABLETOP EXERCISE

A tabletop exercise is a simple but effective way to practice executing your company's incident response plan without the interruption of a full-scale drill.

How it works:

- Members of the internal incident response team talk through a breach crisis scenario in "war room" type of setting.
- The exercise should use scenarios that involve everyone on the incident response team, so that each team member has an opportunity to think through their role during a breach event.
- Typically, the exercise involves a steadily escalating scenario that is revealed over the course of several phases.
- At the end of each phase, the team discusses what is the appropriate course of action under the incident response plan.

THE ADVANTAGE:
It's relatively easy to pull together and can be inexpensive, depending on how elaborate you choose to make the exercise.

THE LIVE SIMULATION

Unlike tabletop exercises, which are usually scheduled, live crisis simulations should be impromptu and perhaps even occur during the evening or over a holiday—like real breaches.

How it works:

- Work with your service providers to develop a simulation exercise that includes all incident response team members, internal and external.
- Rather than simply talking through a breach scenario, in a live simulation systems are actually compromised.
- The live simulation begins with a "discovery" of a breach, such as a lost laptop or a hacking incident.
- Depending on how elaborate you choose to make it, even social media uproars can be involved.
- Response team members should act as though the situation is completely real. Those in favor of "red teaming" would argue that they actually believe that it's real, though some argue this is ethically dubious.

THE ADVANTAGE:
A live simulation is more elaborate and tends to mimic real world conditions more closely than tabletop exercises.

Some vendors, particular PR and computer forensics firms, may have their own simulation exercises. While participating in function-specific simulations has value, it doesn't give you the opportunity to practice and evaluate how your entire incident response team works together.

TIP

The most effective simulations should **involve any breach response vendors** with which you've contracted as well as the internal response team.

STEP
05

Bringing in the Reinforcements

SUPPLEMENTAL EMPLOYEE TRAINING

As part of your organization's privacy program, you've probably already trained your employees on privacy fundamentals like data collection, retention, use and disclosure. But you may not have provided training on basic breach response procedures like whom to call, the first point of contact and what constitutes a breach.

Lack of training can lead to innocent missteps in the early stages of breach response that can have major repercussions later. As a result, it's smart to train all personnel and third-party contractors on basic breach response protocol. Additional in-depth training should be provided to members of the internal breach response team.

It's a smart practice to train all personnel and third-party contractors on basic breach response protocol.

! **THE BOTTOM LINE:** The earliest detection allows for the quickest response. All personnel must be trained to recognize a possible breach and to report it at the earliest possible moment.

STEP
06

When the Regulators and Lawyers Come Knocking

LITIGATION AND REGULATORY INVESTIGATION PREPAREDNESS

After the discovery of a breach, it's almost certain that regulatory investigations and class action lawsuits will follow. **SO BE PREPARED!**

You can begin defense preparation well before a breach has occurred, and it doesn't require the assistance of legal counsel.

Preparing for the inevitable

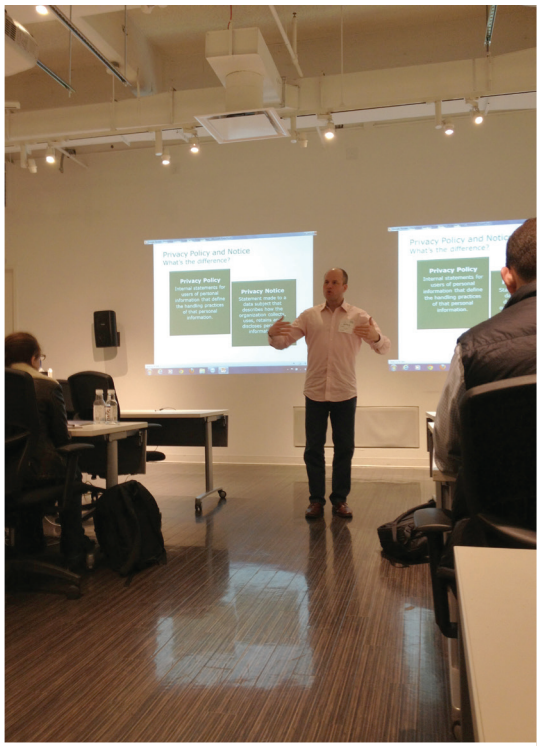
1. **Document. Everything.** Keep impeccable records of all the actions you've taken to prepare for and protect against a data breach, like creating an incident response plan and employee training.

Consider developing a documentation protocol to ensure that all of your preventative actions are captured.

2. **Review policies on an ongoing basis.** If it's not already part of your company's privacy program, you should begin reviewing vendor privacy and data security policies and practices before selection and in regular intervals thereafter.

BEYOND CHECKING THE BOX:
Showing Good Faith

With data breaches making headlines daily, it's no longer enough to just check the box when it comes to compliance. So how do you show a regulator that you've made good faith efforts to protect against a breach?



Get your staff trained. And not just your privacy or incident response teams. We're talking about anyone in your organization who touches data.

Privacy training reduces risk of a breach by:

- Improving the ability of staff to spot issues
- Encouraging people to elevate privacy issues
- Creating a privacy-aware business culture

TALK TO US.
Find out how your staff can learn to institute better privacy practices, drive compliance and build a more effective data protection program with IAPP privacy training.

STEP
07

It All Comes Down to the Dollars

FUNDING YOUR INCIDENT RESPONSE PLAN AND PREVENTATIVE MEASURES

Breach response costs aren't likely to be a line item on the budget sheets of most organizations. But accounted for or not, most companies will eventually experience a breach—and the expenses associated with it.

Identifying funding for action items in your incident response plan is crucial. The best incident response can be rendered wholly ineffective without the appropriate funding.

One way of predictably incorporating these costs into your budget is purchasing cyber-liability insurance.

Read our special supplementary section on cyber-liability insurance.

THE BOTTOM LINE: Regardless of how you choose to account for these costs, it's imperative that they not be overlooked.

YOU MIGHT ALSO LIKE...

- Ten Steps to a Quality Privacy Program
- Security Breach Response Plan Toolkit
- Recommended Practices on Notice of Security Breach Involving Personal Information
- Privacy Industry Index (PII): Vendors
- PII Risk Matrix
- Privacy Policies: How to Effectively Communicate with Consumers

WANT MORE?

Stay connected to the IAPP

SUBSCRIBE
to our daily e-newsletter

Stay on top of privacy news

READ
our blog

Find out what the privacy influencers are talking about

FOLLOW
the IAPP on Twitter

Follow us for all things privacy

WHO WE ARE

The International Association of Privacy Professionals (IAPP) is the largest and most comprehensive global information privacy community and resource, helping practitioners develop and advance their careers and organizations manage and protect their data. Founded in 2000, the IAPP is a not-for-profit association that helps define, support and improve the privacy profession globally.

More information about the IAPP is available at **www.privacyassociation.org.**

iapp
international association
of privacy professionals