iapp

MANAGING YOUR DATA BREACH:

Maximizing the Relationships That Count To Manage Costs and Business Impact

By Dennis Holmes

Managing Your Data Breach: Maximizing the Relationships That Count To Manage Costs and Business Impact

By Dennis Holmes

The old adage that an ounce of prevention is worth a pound of cure has never been truer than in the context of data breach preparedness and response. As general agreement settles in to the fact that data breaches are essentially an inevitability for any firm with substantial data holdings—some 43 percent of companies suffered a breach in 2013 alone—the onus is on CPOs and privacy leads to studiously plan for the day when breach response is needed.

Along the way, your organization will be better prepared to prevent a breach from happening in the first place.

While there are a number of data breach guides out there, here at the IAPP we have chosen to focus on the many relationships and stakeholders involved in breach preparedness and response. Responding to a breach correctly involves a suite of people both inside and outside your organization. Understanding the best way to most efficiently utilize those people goes a long way toward ensuring that your response manages costs, manages business impact and puts the breach behind your organization as quickly as possible.

"Responding to a data breach is a lot like fighting a fire," notes Gerard Stegmaier, CIPP/US, a partner with Goodwin Procter. "Once the alarm goes off, it pays to have a plan and to work immediately to address the safety of anyone in the building, contain the fire and preserve the scene for the investigators. Safety comes first, then investigation and remediation. Keeping calm, being methodical and ensuring access to the right resources for management always ensures better outcomes."

Seems like an obvious truism, but, "Incident response preparedness is all over the map," notes Co3 Systems' Tim Armstrong. "Some organizations are well-prepared. But more often we find that even Fortune-500 companies that have spent millions of dollars on preventive and detective controls have significant shortcomings handling day-to-day security and privacy events, not to mention a major breach."

Oftentimes, that's because the organization hasn't taken the time and effort to develop the relationships inside and outside the building necessary for rapid and coordinated response.

In the following document, we offer up a way of getting the necessary relationships in place and then outline how best to leverage those relationships once the breach has occurred.

Part I: BREACH PREPAREDNESS: Setting up your incident response team and laying the groundwork for proper vendor management

Part II: LEGAL SERVICES: Your breach coach and beyond

Part III: IT SERVICES: Forensics is more than just figuring out what happened

Part IV: PR SERVICES: Making sure you craft the proper message for the intended recipients—including regulators

Part V: CONSUMER SERVICES: How to make things right, retain your customers and come out the other side relatively unscathed

PART I: BREACH PREPAREDNESS

Step One: Assemble an Internal Incident Response Team

The foundation of breach preparedness is having a well-prepared incident response team. It is important to have a team that is well-versed in privacy and security matters that can take the lead in handling the incident response should you experience a breach. Companies that suffer a breach without having put an incident response team in place often waste valuable time trying to get organized and assign/define responsibilities, stalling the breach remediation process.

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

At the very least, your internal incident response team should include representatives from IT, security, legal, compliance, communications and customer service and a member of the executive management team. A smaller firm may not have different people in all of those functions, but this suite of functions should be represented on the team:

IT and Security —The IT and security team members play a central role in helping to identify what information was compromised because they are most familiar with the network systems and the security controls in place. In most cases, however, rather than conducting the forensic investigation, the internal IT and security staff may primarily assist the outside forensic team with their investigation. Even though the IT and security staff possess an intimate knowledge of their organization's network systems and security controls, many lack the specialized skill set and training to perform digital forensic investigation.

Legal and Compliance—Identifying the notification, legal and regulatory requirements of the breach response is the main purview of the legal and compliance teams. 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. The legal and compliance staff will take their orders/direction from your organization's breach coach/counsel to satisfy your company's legal and regulatory obligations.

Communications—In the increasingly digital world in which we live, good news travels fast and bad news travels faster, so it is imperative that your communications team is involved in the breach response as early as possible. The communications team should be 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. On the other hand, your communications team should refrain from making any external communications about the breach. A PR firm that specializes in crisis communication should handle any external communications made, with whatever assistance and direction they might require 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 fields 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. When the anticipated call volume is higher than can be handled internally, most companies engage a call center and set up a dedicated hotline for impacted customers to call rather than be inundated with calls. Other companies have chosen to create a website for consumers that provides answers to FAQs and information on fraud and identity theft protection instead of using call center services. Regardless of which approach your company chooses to take, your company 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.

Executive Management—Having a management-level executive with broad decision-making authority on the incident response team is ideal; this individual's broad authority can help the breach response process move more quickly. A management-level privacy or security professional is best positioned for this role. It is not always possible, however, for an executive to commit to incident response te am membership. In lieu of having a management-level executive on the team, 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 updates on the status of the breach response. This approach is a great alternative if no management-level executive is able to join the incident response team, but it is slightly less efficient because there are likely to be some actions that exceed the delegated authority and require approval from the executive management team.

Here are a few items to keep in mind as you select the members of your incident response team:

» Breaches can attract lots of media attention. Chances are that the members of the incident response team are going to be most familiar with your company's breach, so it is prudent to 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 some media training to members of the incident response team and coach them up after they've been chosen.

» Senior staff from each of your company's functional groups will not always have solid privacy and security knowledge. Consider the level of privacy and security training and knowledge of staff members you choose to be on the incident response team rather than selecting senior staff by default.

» Breaches can be discovered at any time, and you want to be sure that the members of the incident response are reachable and available if and when a breach is uncovered, even if that time is inconvenient.

Step Two: Reevaluate Existing Privacy and Security Systems and Procedures

The most effective incident response plans use existing privacy policies and procedures as a framework. Developing your incident response plan in this way provides you with an opportunity to review those policies and get a clearer picture of the preventative measures already in place and also helps to avoid duplication of effort. For example, if your company has 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, it is more productive to expand the documentation protocol to include breaches.

Additionally, this review 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. For 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 is this: 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 Three: Establish Relationships with Law Enforcement, Regulators and Breach Response Service Providers

Establishing these relationships is an important part of your breach preparedness and helps to avoid the de facto practice of selecting a vendor in the midst of the breach crisis. For example, introducing yourself to a regulator before you have a data breach shows that your organization is being proactive about protecting against a breach, and doing so could help you earn the regulator's trust and respect, which you'll want if you do experience a breach. It also prevents the investigation of your breach from being your first introduction to the regulator. As far as law enforcement is concerned, having a prior relationship can make the process of catching the criminal or criminals who breached your company proceed more smoothly.

Speaking with breach response service providers, however, yields more concrete benefits. The cost savings that result from the opportunity to negotiate for lower prices without the time pressure of a live breach are perhaps the most obvious benefit. Beyond cost savings, establishing relationships and contracting with breach response service providers before a breach gives your organization major advantages in the response planning process that can help make your incident response plan most effective.

Computer Forensics—Firms providing computer forensics services are usually the first provider engaged by the breach counsel after a breach occurs. However, companies don't have to, and shouldn't, wait until they have experienced a breach to engage a computer forensics firm. In fact, given the critical breach response function, a computer forensics firm should be contacted long before your organization discovers it has been breached.

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; however, the forensics firm you hire after a breach is discovered does not. For most companies that will prove to be a huge, time-consuming and cost-increasing problem. Citing the aforementioned reasons, the forensics firms that consulted for this report explained that the total costs of their services were higher when responding to a breach for a client with whom they had no prior relationship. The major advantage of identifying and hiring a forensics firm during the incident response planning process is that there is time for the forensics team to get familiar with your organization's IT network.

The luxury of time cannot be overstated. Giving the digital forensics firm you hire time to become familiar with and understand the landscape of your company's IT infrastructure will help that firm work more efficiently when called upon to respond to a breach. Because of the firm's familiarity, time that would otherwise be spent getting acclimated to your IT infrastructure will be focused on the investigation of your breach and will likely lead to a more expeditious technical remediation. Additionally, the firm can also recommend software and security protocols that can help your organization increase the chances of avoiding a breach altogether.

Consumer Services—In this report, consumer services refers to a variety of companies that offer one or more of the following: call centers, notification to affected customers, identity monitoring or identity protection and repair. Though engaging and contracting with consumer services providers pre-breach will yield some efficiencies, the major advantages of working with these companies before a breach occurs is largely financial, particularly as it relates to credit monitoring remedies. In a pre-breach environment, organizations have significantly more bargaining power that doesn't exist post-breach because there is no urgency or immediate necessity for the services. So, rather than paying the sticker price for one variety of the monitoring remedies, your organization can and should negotiate pricing for the remedy or remedies it wishes to offer affected individuals after a breach.

Additionally, there are numerous companies in the consumer services marketplace that offer many different types of products and services at varying price points. With the amount of variety in the consumer services market, companies should devote some time to exploring the different options available, learning what risk or problem the products seek to address. Doing so ensures that your company can ultimately choose the products and services that make sense for your organization and its stakeholders when a breach happens. Often, companies that wait until after experiencing a breach to procure these services miss the variety of the service offerings in this space and hastily choose a suite of products and services that are not always appropriate.

Public Relations—The public relations firm provides one of the most critical services necessary for breach remediation and is thus a relationship that your organization should develop as early as possible. Perhaps more than some of the other breach response vendors mentioned here, many of the tasks performed by the PR professionals could be prepped, and in some cases completed, before the breach occurs. Such tasks include crisis communication training for customer service and other client-facing personnel, creating template scripts and other breach-explanation content and identifying an organization's key audiences.

Additionally, working with a PR firm before experiencing a breach can also improve the flow of information through an organization during a crisis. Often, in the midst of a crisis, information tends to travel the way information travels in a game of "Telephone," in a quick, uncontrolled manner without any regard for accuracy. Your PR firm can help you establish a core crisis communication team and build the infrastructure for that team, as well as identify the chain of communication for crisis notification so as to avoid the "Telephone" scenario in the midst of your breach.

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.

Legal Services—Similar to the consumer services providers, the benefits that result from a pre-breach relationship with a law firm or an attorney specializing in breaches are very much financial, but they are also operational in nature. Identifying and retaining legal counsel prior to experiencing a breach is critically important. Seeking legal counsel before you experience a breach crisis gives you time to shop around and thoroughly inquire into the credentials and experience of any law firms or attorney you may be considering. While the opportunity to vet your legal counsel might seem pretty banal, more often than one might think companies are blindsided by their breach and have to "lawyer up" before they've had a chance to engage any sort of vetting process. This approach doesn't always work out very well.

The financial benefit of retaining legal counsel pre-breach is an opportunity to secure lower rates. Because there is no imminent need for legal services, companies have a much better negotiating position in a pre-breach environment and, as a result, are able to set price parameters and get better rates than would be offered during a breach.

Further, your breach counsel, as you'll see in the post-breach portion of this report, acts as the quarterback for your breach response. Identifying your breach counsel and having this person readily available for breach response can save important time you would otherwise spend in seeking counsel or in asking your current counsel, who doesn't have extensive breach experience, to quickly begin research.

A Final Note on Vendors: Cyber-Liability Insurance

It is imperative to establish relationships with service providers during the incident response planning process, but our discussion here about these relationships would be incomplete without mention of cyber-liability insurance and the role it might play in the vendor selection process.

Cyber-liability insurance is a fast-growing, specialized type of insurance that provides policyholders with coverage in the event of a cybersecurity incident. Today, a number of large insurance providers, as well as some smaller companies, offer cyber-liability insurance. If your organization does not already have cyber-liability insurance, assessing whether cyber-liability insurance is good investment that makes sense for your company should be a part of your incident response planning.

Generally, coverage under cyber-liability insurance policies 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 and include but are not 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 and settle fines 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 for damages they incurred as a result of the data breach. Third-party losses also include attorney fees and expert fees, and other defense costs for these third-party claims as well as any regulatory fines that may be assessed under privacy statutes.

In addition to the categories of covered expenses, many insurance carriers have guidelines regarding which breach response vendors are eligible for full coverage under the insurance policy. Insurance companies generally employ one of three approaches:

Closed Network—With this approach, insurance carriers have a network of vendors with which they have a direct relationship and policyholders must choose vendors from within this network to get full coverage. If a vendor outside this network is chosen, no insurance proceeds are available to cover the costs.

Preferred Network—In this hybrid approach, insurance carriers have a network of preferred vendors that are eligible for full coverage and policyholders are allowed to use any breach response vendor they choose; however, less coverage is provided for vendors outside of the preferred vendor network.

No Network—In this approach, insurance carriers give policyholders the latitude to choose the vendors that they want to use, but prior approval is necessary. Typically, approval is not difficult and could be as simple as an email.

As stated above, 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 insurance 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. If your organization does decide to get cyber-liability insurance, be sure to consider the following points:

» Research the various policy structures in the marketplace so that you can be sure to 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?

» 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 a vendor is an important consideration to weigh before selecting a carrier and plan.

» Pay close attention to limitations for each covered expense; 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 Four: Crisis Simulation

The jury may still be out on whether practice makes perfect, but it does make you (probably) better prepared. Now that you have assembled both your internal and external breach response teams, it's time for a dry run. It is important to know how your organization would fare during a breach crisis and identify any gaps. There are several ways to approach breach crisis simulations, but doing a tabletop exercise as well as a "live" simulation is recommended by most of those consulted for this report.

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. In a tabletop exercise, members of the internal incident response team talk through a breach crisis scenario in "war room" type of setting. These exercises should use scenarios that involve everyone on the incident response team, so that every 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 the appropriate course of action under the incident response plan. One advantage of tabletop exercises is that they are relatively easy to pull together and can be inexpensive, depending on how elaborate you choose to make the exercise.

Live simulations, however, are more elaborate and tend to mimic real-world conditions more closely than tabletop exercises. Further, unlike tabletop exercises, which are usually scheduled, live crisis simulations should be impromptu and perhaps occur during the evening or over a holiday like real breaches. The most effective simulations involve any breach response vendors with which your organization has contracted as well as the internal response team. Rather than simply talking through a breach scenario, in a live simulation systems are actually compromised, and depending on how elaborate you choose make it, even social media uproars can be involved. Some vendors, particular PR and computer forensics firms, may have their own simulation exercises, and while participating in function-specific simulations has value, it doesn't provide you the opportunity to practice and evaluate how your entire incident response team works together. That said, work with your service providers to develop a simulation exercise that is inclusive of all incident response team members, internal and external.

Step Five: 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 is a good practice to train all personnel and third-party contractors on basic breach response protocol. Additionally, further in-depth training should be provided to members of the internal breach response team.

Remember that the earliest detection allows for the quickest response. All personnel must be trained to recognize that a breach may have occurred and to report it at the earliest possible moment.

Step Six: Litigation and Regulatory Investigation Preparedness

After the discovery of a breach, regulatory investigations and class-action lawsuits are almost certain to follow. Defense preparation for these increasingly inevitable legal actions can begin well before a breach has occurred, and this preparation doesn't require the assistance of legal counsel. Documentation is key. Keep impeccable records of all the actions your organization has 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.

Also, if not already a 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. Being able to show regulators, particularly the FTC, and provide evidence in court that you took "reasonable" steps to prevent a data breach can vastly improve your organization's chances of a favorable outcome.

Step Seven: Funding Your Incident Response Plan and Preventative Measures

Breach response costs are not likely to be a line item on the budget sheets of most organizations. Accounted for or not, most companies will eventually experience a breach and incur the costs associated with its remediation. It is prudent to account for such expenses in your financial planning in some manner. One way of predictably incorporating these costs into your organization's budget is to purchase cyber-liability insurance.

Regardless of how your company chooses to account for these costs, it is imperative that they not be overlooked. Identifying funding for action items in your incident response plan is also crucial, and it can ultimately determine the effectiveness of your plan. The best incident response can be rendered wholly ineffective without the appropriate funding.

PART II: LEGAL SERVICES

In this section of the report, "incident" will refer to security events that require mitigation but may or may not require notification, while "breach" will refer to such events that require notification and mitigation. Even though the above terms are often used interchangeably in general parlance, they each have a particularized meaning in the legal environment. To put it simply, all breaches are incidents but not all incidents are breaches. Legal and technical analyses are required to classify an event as either an incident or breach—a classification that ultimately determines an organization's legal obligations

Choosing a Breach Coach

As discussed in the breach preparedness section, selecting and vetting an attorney to serve as breach counsel is critical to an effective breach response plan (or general). If your company, however, finds itself in the unfortunate position of experiencing a breach without having selected breach counsel beforehand, then retaining counsel is likely going to be hasty proposition. In the haste to retain counsel, many companies make the following errors, which could be detrimental to successful breach response program/breach remediation. When trying to balance the urgency and necessity of retaining legal counsel with the prudence of due diligence, consider the following guidance from industry leaders:

1. Avoid Hiring a Law Firm or Attorney Simply Because There Is a Preexisting Relationship.

Engaging a law firm or attorney that your organization is already familiar with may seem like the practical choice; it isn't always the best choice. Although there are huge benefits to working with an attorney who is already familiar with your organization's business and with whom you've already established a working relationship, often those attorneys are not well-acquainted with the complexities of data breach response and, as a result, ill-equipped to provide adequate guidance.

Obviously, if a law firm or attorney that you have a preexisting relationship with is well-versed in data breach matters or privacy law generally, this warning may not apply. But, whatever you do, don't retain a law firm that your company has used primarily for transactional or litigation matters that lacks a privacy practice or an attorney who focuses on privacy law matters. The efficiency that your organization stands to gain by leveraging an existing relationship cannot make up for any mishandling of your data breach response, which is likely to follow if an attorney is learning privacy law on the job. There are other alternatives, especially if trustworthiness, rather than expediency, is the primary concern.

Instead, do a little research and reach out to other companies in the same industry—and ideally of similar size and complexity—that have experienced a breach in the past. Jeff Corey, owner of a small regional jewelry retailer, had a positive experience when he reached out to Hannaford Supermarkets, a regional grocery chain, and T.J. Maxx to ask for advice upon learning about his own company's breach. Additionally, if you have cyber-liability insurance, chances are that your insurance carrier has established relationships with law firms and attorneys who are well-qualified to handle breach response matters.

Leverage that relationship.

2. Retain an Attorney Who Can Drop Everything and Respond to Your Breach Emergency Right Away.

Given the instrumental role that attorneys play in the breach response process, "it is important the counsel (breach counsel) retained be able to drop everything and respond to the emergency promptly," explains Bill Latham in "Responding to a Data Breach—Best To Have Your Plan in the Can." While attorneys, at times, must juggle multiple client matters at once, your organization and any prospective firms should have a discussion early on about how your breach will be handled and staffed. For instance, one contributor recalled a client who retained a firm with a robust privacy practice but that staffed their breach response with a general litigation attorney in the firm's local office rather than a non-local attorney in the privacy practice group. Having that discussion upfront can avoid confusion and disappointment later as well as help ensure that your breach receives the attention of the privacy law expert.

3. Find Out If Prospective Counsel Have a Breach Response Roadmap or Action Plan Already Prepared.

As this report has stressed repeatedly, expediency is key when responding to a data breach. In keeping with that view, multiple contributors suggested that breached firms hire an attorney who already has an action plan prepared. Because time is of the essence, an attorney who comes prepared with an action plan to guide your organization's breach response efforts from day one might be ideal. Especially if your organization doesn't have an incident response plan in place, an attorney who comes armed with a plan prepared may be in a position to move more quickly with breach response tasks, which could be a great benefit.

Be mindful, however, of any attorney who claims to have a foolproof plan that will work for your company. Some contributors have cautioned that some pre-prepared response plans and roadmaps can actually impede a company's breach remediation efforts. When pre-prepared plans are involved, they argued, there is a tendency for attorneys to spend more time trying to fit their clients' situations into the contours of their plan rather than spending time trying to understand a particular situation to develop a plan of attack. Even legal professionals who come prepared with a general plan of attack should have a flexible approach and should readily tailor their plan to fit your company's circumstances/breach.

What Can You Expect from Your Breach Counsel?

Attorneys who serve as breach counsel hail from a variety of backgrounds, and that variety is reflected in their differing approaches to data breach response. Consequently, it is difficult to say definitively what a breached firm can reasonably expect from their breach counsel. Nonetheless, there are some common tasks and responsibilities that almost any breach coach is likely to undertake. Their responsibilities primarily fall into one of three categories: compliance, project management and litigation preparation.

Compliance

To ensure full compliance with the complex patchwork of data breach notification laws, which encompass state, federal and international laws, organizations should look to their breach counsel for guidance. Attempting to navigate the treacherous waters of breach notification without the guidance of your breach counsel is not advised. With compliance, generally, the investigation and remediation efforts of your breach coach revolve around the answers to the following four questions:

1. Are You Required To Notify?

As mentioned above, not every security incident triggers legal notification requirements, so understanding when your organization has a legal obligation to provide notice is critical to compliance. Because the events triggering notification vary widely between the various jurisdictions in which you might be doing business, your breach counsel should evaluate the nature of the incident, the type of information compromised, whose information was compromised and any details obtained from the forensic investigation to determine whether notification requirements have been triggered.

Additionally, even when there is no legal obligation to notify breach victims, you may be advised to do so by your breach counsel for PR and risk mitigation reasons.

2. Who Must Be Notified?

Breach notification statutes typically specify who must be notified after a breach. Generally, companies can be required to provide notice to individuals, businesses, state and federal regulators and credit reporting agencies. However, the inconsistencies that exist between state breach notification laws in the U.S., specifically, add to the complexity of determining who should be notified. While most state breach notification laws apply only to state residents, the notification requirements of some international laws may extend to individuals who are not citizens and do not live in that country. Determining who must be notified can be a daunting and complex undertaking, but working closely with your breach counsel and leaning toward being over-inclusive rather than under-inclusive can help mitigate any risk of noncompliance.

3. When Must Affected Parties Be Notified?

In many ways, data breach response is a race against the clock, so it may come as a surprise that breach notification laws are often quite vague about when affected parties must be notified. Phrases like "as soon as possible," "promptly," "immediately (24 hours)" and "without unjustified delay" are used in both U.S. and international breach laws to describe the timeframe in which breached firms must provide notification. The lack of uniformity and the interconnected nature of society make it difficult to provide notice of a breach on a rolling basis without bringing potentially worldwide attention to your breach. That said, it is important to work with your breach counsel to develop a notification timeline that makes sense for your business and is permissible under the law. Be sure that you discuss the notification timeline with your breach counsel and that you are aware of the risks of potential courses of action.

4. What Must You Tell Them?

While some breach notification laws delineate the disclosures that a notice is required to contain, others use broadly worded phrases like "describe the nature of the unlawful disclosure and measures to minimize the harm" to prescribe notice contents, and others still are completely silent about notice contents. Further complicating matters, some laws proscribe certain information from being included in notification letters. For example, the Massachusetts law states, "notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use."

If your company finds itself subject to inconsistent content requirements, it may be necessary to draft different forms of the notification letter. A popular alternative to that approach is to identify the strictest law, to which your company is subject and to use a letter meeting those standards to all parties who must be notified. Consult with your breach counsel about which approach is most appropriate for your situation. The final note about content concerns the actual drafting of the notification letter. Your breach counsel should draft the letter that your organization sends to the affected parties or, at the very least, should review the letter and give final approval before the letter is sent. Because the wording of these letters has important legal implications apart from compliance with the breach notification laws, input from your breach counsel is essential. Ultimately, notification is a legal matter that should be principally handled by your breach coach or other counsel.

Project Management

Managing data breach response is like building a house; it takes several workers with different skill sets to successfully complete, and not everyone understands how the others do their job, so coordination is key. Coordinating the incident response team is perhaps the principal responsibility of the breach counsel and crucial to the success of your breach response. This means facilitating the communication, exchange of information and response efforts of each member of the incident response team. If the members of your incident response team do not work together in a complementary fashion, the negative impact of your organization's breach has the potential to be quickly exacerbated.

Some may wonder why the general counsel or other C-level executive does not coordinate these workers and manage their relationship with the company during breach response. The answer is two-fold: legal liability and experience. First, all of these relationships have legal implications that the breach counsel must monitor and manage to make sure that a breached firm is not inadvertently exposed to additional legal liability. Second, the breach counsel should have significant experience handling breach response and should therefore be better prepared to serve the company. Thus, breach counsel is best suited to perform the project manager role. The breach counsel's function as project manager is most pronounced with regard to breach communications and litigation preparation.

Breach Communications

In breach response, effective communication is key. Ultimately, all communications about the breach have the potential to leave your organization open to legal liability. As result, breach counsel should be the master of all communications—internally facilitating conversations between members of the incident response team and curating any external communications.

For internal communications, getting the right information to the right people can make or break breach remediation efforts. When different members of your breach response team are working with different, incomplete or inaccurate information, it can lead to costly inefficiencies and potentially dire errors in the response process. A classic example: the number of records affected. Many companies disclose the number of records affected by their breach only to retract and modify that number later. Promoting conversations between the PR and IT professionals that provide context for any findings can help to avoid such retractions. Without any such conversations, a PR professional may see no need to qualify any numbers or other information disclosed.

Your breach counsel is well-positioned to know which conversations between various incident response team members must be had to avoid a firestorm later. Similarly, your breach counsel knows what pitfalls to watch for when communicating about the breach externally. A careful assessment of your external breach communications by your counsel can help your organization avoid public relations and legal problems in the future.

Litigation Preparation

In the wake of a data breach, litigation is an inevitable reality, and it behooves breached firms to begin preparing to defend any potential lawsuits immediately. Previously, this report mentioned the importance of retaining counsel to secure "privilege." Why is privilege so important? Privilege, or attorney-client privilege as it is formally called, protects communications between you and your attorneys from discovery by the opposing party during pretrial investigation and from being used as evidence in a trial. Hence, securing privilege is an important preliminary step in preparing for litigation. Roberta Anderson, a partner at the law firm K&L Gates, was quoted as saying, "A company's decision to retain outside counsel at the outset is critical, since the results of a breach investigation may be pivotal in avoiding or minimizing liability in subsequent litigation and regulatory investigations."

In addition to helping your organization secure privilege, your breach counsel also assists with the preservation of evidence. Network data and log files can be some of the most useful data and should be preserved so that you can show regulators that your organization had reasonable security controls in place or prove wrongdoing in criminal prosecution. To be used in court, digital evidence must be preserved in a manner that adheres to strict standards. While most attorneys don't possess the technical skills to actually preserve the evidence themselves, the experience of most breach counsels makes their guidance about what should be considered evidence, and thus preserved, very valuable to their clients.

IT and forensic specialists approach the technical aspects of breach response differently than breach counsel. Rather than focusing on the long-term implications of their technical efforts, IT and forensic specialists tend to focus on patching the security vulnerability or removing the malware from the system. This narrow focus can cause the IT professionals to inadvertently compromise valuable digital evidence in the process. Breach counsels, on the other hand, have a much broader focus on minimizing legal liability, which allows them to provide better guidance about evidence preservation.

Cost of Legal Services

In terms of cost, legal services have a reputation for being one of the most expensive pieces of a breach/breach response. The cost for legal services can vary widely and range from less than $5,000 up to about $250,000. Jon Neiditz, a partner at Nelson Mullins, said in an interview with Mark Greisiger of NetDiligence, "I'm astonished whenever I see the costs that are put out there. I have never, in the largest breaches I've dealt with, come close to $100,000 in total legal costs. Small ones are $1,000 to $2,000 and medium-sized ones are between $10,000 to $30,000. If you handle a lot of these cases as I have, you can make the services very cost-effective for clients…." According to insurance claims data, however, on average companies spend about $48,091 on legal expenses. But if those larger figures leave you with sticker shock, then consider negotiating fees and fee caps upfront to manage costs because "vendors, not excluding lawyers, will try to take advantage," says Neiditz.

PART III: IT SERVICES

For the purposes of this report the term "IT services" refers to the wide array of information and security services that companies offer to address the technical aspects of a data breach including, but not limited to, cyber-security incident response and computer forensics.

Depending on the size, maturity, and sophistication of your IT department, the IT services you may require will vary. Larger companies with robust IT departments may need to outsource only a small portion of the IT investigation and remediation, whereas a smaller company may need to outsource those functions completely. Regardless of the specific expertise you may need, an IT services firm should be hired by your attorney as soon as possible, before any other vendor, so that the firm can begin the process of restoring your systems to working order and properly identifying the nature of the breach.

Incident Response and Computer Forensics: What's the Difference?

With IT services, many industry outsiders confuse or conflate (cybersecurity) incident response with computer forensics, but the terms are not synonymous. Of course there is some overlap; for example, both involve some degree of investigation. But they are distinct processes with very different functions.

Computer systems experience breach events more frequently than one might expect, but often times these events are benign or pose no serious risk to the system. In IT parlance, incident response refers to the procedures/process used to fully remediate a computer security incident. This process includes, but may not be limited to, detection analysis, containment, eradication and recovery. Computer forensics, on the other hand, is a discipline in the IT world.

Forensic specialists, it's true, may employ the incident response lifecycle as they investigate stuff. Further, digital forensics experts are usually engaged for very complex, adverse breach incidents that cannot be handled in-house. while principles of cybersecurity incident response are as likely to be employed by IT staff as by a forensics expert, for these more complex types of breach incidents, time is of the essence and specialized training is needed to handle the complexity of these security breaches. There are several niches within the digital forensics field, including root cause and malware analysis, to name a couple.

Both incident response and computer forensics are likely to play a role in your breach response efforts. Understanding the different functions of each service can help your organization make informed decisions about when to engage external IT service providers and how to best utilize their services to address the breach. There a few common mistakes that many companies make with regard to IT activities following the discovery of breach:

1. Relying on In-House IT Staff for (Cybersecurity) Incident Response

Effective investigation and remediation of a breach incident typically requires specialized skills that the IT staffs of most companies usually do not possess. Even if there are some IT staff members with such skills, if they are not using those skills in their day-to-day duties, then a real live breach probably isn't the greatest time for them to get back in the saddle. The bottom line: unless your IT department has staff with the requisite training dedicated to computer forensics, then it is best to outsource those aspects of your breach response. That said, there are some situations, albeit rare, where the digital forensic investigation could be handled internally, but it is best to outsource that task to minimize your legal liability.

2. Limiting the Scope of the Computer Forensics

The increasing complexity of cyber-attacks has made it very difficult, even for the most experienced forensics experts, to identify all affected systems and platforms. Even so, all too often, companies narrowly draw the scope of their forensic investigation to their detriment. Usually, this is done to mitigate the high cost of computer forensics or because the role forensics plays in breach remediation is not fully understood. Prematurely limiting the scope of a forensic investigation, by examining only the servers on which suspicious activity has been recorded, for example, can leave latent threats undiscovered for extended periods of time. On the other hand, beginning investigative and discovery efforts with a broad scope, which explores all potentially compromised systems, can reduce an organization's risk of overlooking exposed system components.

3. Failing to Involve Senior Leaders in Incident Response

At first blush, it may seem completely logical to leave the leaders of the information security functions in charge of managing incident response. After all, many major breaches are the result of cyber-attacks. This approach, however, is flawed because IT professionals have a tendency to concentrate almost exclusively on the technical aspects of a breach, which leaves important business considerations largely ignored. Ideally, incident response efforts should be holistic in nature.

Aside from leaving business concerns unaddressed, there are other reasons why senior leaders should take part in managing incident response. First, excluding senior leaders can stall the remediation process because there will inevitably be decisions that must be made that will require approval from senior leaders outside of the IT and security functions. In addition to increased efficiency, involving leaders across your organization can lead to cost-savings. Because business unit leaders understand the information infrastructure and how information flows through your organization, they can help third-party forensics investigators get up to speed quickly, saving your company valuable time and money.

4. Not Preserving or Improperly Preserving Digital Evidence

For most companies, legal damages account for nearly half of the total of cost a breach, according to a study by NetDiligence on cyber-liability and data breach insurance claims. Poor evidence handling practices have the potential to increase that figure. Whether you are defending civil suits brought by injured business partners or insurance companies resisting claims, or pursuing criminal action against the parties responsible for the breach, proper preservation of digital evidence is critical. If you compromise key evidence in either case, the chances of obtaining a favorable outcome are drastically diminished.

In any event, as Winston Krone explains in his paper Legal and Technical Issues Concerning Evidence in Data Breach Cases, "Key evidence will relate to whether a company ... had fallen below minimum standards or its contractual obligations as it related to information security… In these cases the affected organization will need to collect and preserve a full picture of its security infrastructure at the time of the breach and during its remediation efforts." Often, a company's internal IT staff compromise the evidence even before forensic experts can preserve it. Be sure that your IT staff is mindful of proper evidence-handling protocol, and that forensics experts you hire are well-trained in digital evidence preservation.

The Cost of IT Services

Like other crisis services the exact cost of IT services will vary depending on the specific circumstance of your breach. The cost of forensic investigations ranges from the $20,000 to $50,000 mark well into the million-dollar range, depending on the complexity and size of the breach. The average cost of computer forensic services, however, is about $200,000 based on insurance claims data.

PART IV: PUBLIC RELATIONS

The experts consulted for this report agreed that engaging a public relations firm with significant experience dealing with data breaches is essential. Almost all insurance carriers who offer cyber-liability insurance cover the costs of hiring a PR firm. However, as stated before, if you have cyber-liability insurance, be sure that you understand terms and extent of your coverage for first party or breach response costs.

Communicating about a breach can be tricky, but in the sections below, this report attempts to remove some of the guesswork and identifies important considerations for companies to bear in mind as they work through breach communications strategy with their public relations firm.

Timing of Communications: When Should You Make a Comment?

Many companies have a tough time deciding when to share information about a data breach with the public and regulators. People have come to expect that all things happen quickly—we've evolved into a society that craves "instant gratification and quick fixes," as this story from The Guardian by Rob Weatherhead about the attention span of the modern Internet consumer notes. For regulators and consumers, this applies to data breaches as well. Both groups expect all the relevant facts posthaste. Providing this information, however, involves a process that is typically slow and long.

Breach situations are extremely fluid, and thus, information initially thought to be correct could later turn out to be incorrect. There is nothing worse for a company dealing with a breach than having to recant or update information to the public. Leveraging the experience and expertise of a public relations firm can make it easier to navigate the delicate balance between expediency and conducting a thorough investigation. There are few factors, however, that every company should always consider when deciding when to release this information:

1. Do You Have Accurate Information To Report?

It is difficult to obtain conclusive answers to many of the questions surrounding a data breach like: How many individuals were affected? What information was compromised? How was your system breached? Hence, whether the information you have to report is accurate will likely include a degree of speculation.

Obviously, if a company is unsure about the accuracy of breach information, then it is probably too soon to communicate about the breach. Jason Maloni, senior vice president and chair of the litigation practice at Levick, stressed the importance of giving the forensic investigation all the time it deserves. Waiting until a report from a third-party forensics team has been received and thoroughly reviewed before sharing any information externally can help a business minimize the speculative nature of key breach facts. While it may be more expedient and cheaper, breach information based on findings of an internal IT department is probably more speculative and more prone to retraction. In the meantime, companies can use a "buy-time" statement created by their PR firm, such as, "We have a handle on the situation, but we don't have any facts to report at this time."

2. Is Disclosure Within a Specific Timeframe Required by Law?

Timing of disclosure is often dictated by statutory and regulatory requirements, so companies don't usually have full discretion to decide when to disclose a breach. Some U.S. states are very specific, only allowing 45 days from breach discovery to provide notification, whereas others require notification "in the most expedient time possible" and/or "without unreasonable delay." That said, timing the public disclosure of a data breach can be as much a public relations matter as it is a legal matter.

You might also wonder what to do when affected parties live in states that have differing requirements. In this day and age, information travels too quickly to try to keep parties in different states from knowing about one another, so the consensus is that it's best to notify everyone at once, even if that means complying with the more stringent jurisdiction's requirements.

This is a point where your breach coach and PR team need to be in very close communication.

3. Has the Incident Been Leaked?

Nothing accelerates a company's disclosure timeline more than an unanticipated leak by journalists or bloggers. In such situations, it is critical to respond quickly to take control of the message concerning your breach event and mitigate any false information. This type of situation underscores the value of having an incident response plan because it helps companies to respond more quickly. Similarly, it is important to evaluate whether there are other stakeholders (businesses) affected by your company's breach, increasing the risk of an uncontrolled leak. In this situation, it is important to respond so that your organization can take control of the message, even if your organization doesn't have all of the facts. When that is the case, explain that you are aware of the situation; you are working hard to address breach, and you will provide more information to consumers once it becomes available. It may also be helpful to correct any inaccuracies reported in the media, though that might begin to seem like playing whack-a-mole.

The Tone of the Message—What Should Be Said?

When communicating with individuals affected by a breach, "It's not what you say, it's how you say it!" As described earlier, the attorney is responsible for the content of breach communications, but the public relations team also plays a key role and is typically responsible for the tone and consistency of the messages. Setting the right tone can be tricky, but being mindful of the following principles can put you on the right track.

1. Be Measured in Your Comments

Data breaches are unpredictable—what may be true at one moment may not be true later. Michael's, for example, hired two forensics firms that found nothing before a third forensics firm found that 2.6 million records had been breached. Companies that refrain from making conclusive statements, even after there has been some investigation, can avoid further damaging their relationship with consumers. For instance, Levick's Jason Maloni said this could mean focusing initial comments on the steps being taken to investigate the breach rather than supplying specific numbers or causes. When comments are carefully calculated, speaking out about the breach fairly early doesn't usually pose a problem and presents less risk for companies. Before speaking definitively, however, companies should be certain that the key facts are settled.

2. Acknowledge What You Do Know and What You Don't Know

Ensuring that consumers feel fully informed is an integral part of reclaiming consumers' trust. Transparency is key. Robert McEwen of public relations and reputation management firm McEwen & McMahon is just one of many on record advising that companies should be transparent and admit their culpability in the breach. Companies that are more forthcoming not only display confidence but also lend credibility to their breach remediation efforts. Further, companies that are upfront with consumers have an opportunity to shape and manage the expectations of affected individuals. Contrary to popular belief, sharing that you don't know something can be a good rather than a bad thing.

3. Speak to Your Audience

Beyond the entity breached and those whose information was compromised, breaches can affect a number of different stakeholders, including banks, shareholders and business-to-business (B2B) service providers. Appropriately addressing the interests of various parties will require companies to employ different tones; generic expressions of remorse are not enough. Understanding the risk a breach poses to the various stakeholder groups is important to bear in mind when trying to strike the right tone of communications. Achieving the appropriate tone requires companies to identify the threatened interests by the breach and the risk posed to those interests.

The message you put out to consumers should not be the same message you put out to the B2B community. If you're speaking to a media outlet, understand who their audience is and make sure you're keeping to the talking points that have been prepared for that population.

4. Focus Your Messages on Reassurance

Reassurance should be the primary goal of post-breach communications. However, a company cannot effectively reassure breach victims unless, as mentioned above, it has identified the risks created by the breach. Once those risks are identified, companies must communicate to breach victims that the situation is under control and that their efforts will sufficiently remedy any problems caused by the breach. The best way to convey that message is to link remediation efforts to the specific concerns of a stakeholder group. For example, when addressing consumers who've had their Social Security numbers (SSNs) stolen, describe the effectiveness/efficacy of credit monitoring and fraud protection services being offered to protect or mitigate the harm to consumers. Failure to redress the concerns of breach victims dramatically reduces the likelihood that your company will be able to restore its brand reputation. Hence, reassurance should be a key component of your post-breach communications.

Reputation Management Strategy—How Should We Communicate with the Public?

Knowing what to say and how to say it are fundamental to successfully managing post-breach public relations, but companies should not underestimate the importance of choosing the appropriate platforms on which to share their message. Many companies primarily use traditional media channels like TV to disseminate information after a breach, while others have engaged nontraditional social media platforms with great success. According to Maloni of Levick, "More companies need to use social media to their advantage." The bottom line is that social media should not be an afterthought in a crisis communications strategy.

That is not to say that companies should employ social media to the exclusion of traditional media channels. The truth is, in this day and age, news of a breach will wind up on social media regardless if it is posted by the company itself or a disgruntled breach victim. Companies' reluctance to use social media to break bad news probably stems from their discomfort with how quickly information circulates on such platforms. This type of thinking reflects a poor understanding of the public relations benefits of social media. When companies embrace social media as part of their crisis communications, they are able to help shape the conversation and inform affected individuals more quickly.

Not all companies, however, are in the dark about how social can be leveraged to enhance their crisis communications strategy. Zappos was widely applauded for its use of Twitter and Facebook to inform its customers about its breach. Based on the public response to Zappos' use of social media there are few lessons other companies can learn about social media and breach communications.

1. **Social Media Can Be Used To Create an Information Hub and a Community for Affected Individuals.**

Not only did Zappos create two one-stop shops by posting all of the available information to their Facebook and Twitter accounts, but it also provided a forum for breach victims to assist each other with remediation, which, in Zappos' case, involved the resetting of passwords. Additionally, because social media is one of the fastest ways to share information, Zappos was able to inform more people more quickly.

2. **Companies Can Interact with Breach Victims in Real Time on Social Media Platforms.**

Zappos actively engaged consumers by fielding questions on both Facebook and Twitter. Rather than setting up a call center—in fact, Zappos shut its phone system down and opted to handle initial inquiries via email—and awaiting customer calls, Zappos went to consumers armed with helpful information and ready to answer questions. Another benefit to this strategy was that any responses to customer inquiries on social media were visible and potentially helpful to anyone viewing Zappos' Facebook page or Twitter feed.

3. **Sharing Information Via Social Media Can Bolster Transparency Efforts.**

In the wake of a breach, transparency is huge for consumers. Breaking the news about a breach on social media signals to the public that nothing is being hidden from public view. Much of the praise received by Zappos was due in large part to its level of transparency. Social media is a simple way to demonstrate your company's commitment to transparency, even in the midst of a breach.

Costs of PR Services

How much are the services of a public relations firm with data breach experience going to set your company back? The cost for high-end, comprehensive public relations support ranges from $60,000 to $100,000. However, companies on average, according to insurance company sources, spend about $13,000 on post-breach public relations.

PART V: CONSUMER SERVICES

Further, as Scott Aurnou, vice-president of SOHO Solutions, noted in "After Data Breach, the Best First Responder Is a Law Firm," to ensure that the attorney-client and work product privileges attach, it is critically important that your breach coach hire the consumer services provider your company needs to effectively respond to the breach.

If your company has cyber-liability insurance, advises Holly Towle, a partner with the law firm K&L Gates, then your insurance carrier should be contacted before contracting with any consumer services vendors. Some insurance carriers have a list of preferred vendors who may offer discounted rates to policyholders. Other insurance carriers, however, go so far as to require policyholders to use preapproved vendors to receive coverage, notes Meredith Schnur, senior vice president at Wells Fargo Insurance Services. Be sure to fully understand the scope of your coverage before any contracts are signed.

Next, it must be determined which services to obtain; not all breaches require the entire suite of consumer services. The size, type and the kind of data involved should dictate which services are necessary, says Bo Holland, CEO of AllClear ID. For example, a breach caused by a lost laptop that exposed approximately 500 employee addresses, phone numbers and Social Security numbers doesn't require call center or notification services but may warrant credit monitoring. A breach of that size and type can probably be adequately addressed in-house by using existing personnel to provide notification and field questions. As you'll see in the following focus sections, both the nature and size of the breach can affect the need for these outside vendors.

Call Center

In large part, it's the magnitude of the breach that governs whether call center services are necessary to adequately respond to customer inquiries. Call center support is also a great way to facilitate enrollment in any credit monitoring or identity protection services you offer as part of your response. In addition to preventing your company from exhausting internal resources, call center services also help to mitigate business interruption. Taking internal employees and shifting them to contacting or responding to affected customers can serve only to double the impact of a breach. Not only are you paying vendors to help you respond, but now your company's productivity is shot as well.

Typically, call center support providers/vendors create a toll-free number dedicated to your breach event that is staffed with live agents to field questions from consumers during specified hours. When deciding to offer call center support services as part your breach response plan it is important to consider the following issues/questions:

1. Is Call Center Support Necessary?

After a data breach, it is imperative that an organization provide affected individuals with the opportunity to inquire about the incident and express their concerns. To that end, setting up a dedicated call center is often necessary. However, companies should weigh the anticipated call volume against their ability to effectively field calls to decide if external call center support is needed. Large companies with in-house call centers might have sufficient resources to handle the inquiries, while smaller companies with fewer staff might require call center support.

However, there are other factors besides numbers to consider. What type of relationship does your company have with members of the affected population? Is your company's staff well-prepared to respond to agitated callers? Would handling inquiries internally significantly disrupt business operations? For example, Day's Jewelers, a mid-sized regional jeweler, used staff at their retail locations to handle customer calls in lieu of call center support. Though unconventional, says CEO Jeff Day, this approach worked for Day's Jewelers, whose brand is founded on treating customers with a personal touch. Using a call center staffed with unfamiliar agents would have hindered their efforts to regain customer trust in the wake of a data breach.

2. How Long Should Call Center Services Be Offered?

Determining how long call center services should be offered is more of an art than science. Organizations need to weigh several factors before deciding the appropriate length of time to offer call center support. These factors include, but are not limited to, the number of affected individuals, how much media attention was given to your breach incident, the number of notifications sent, whether the affected population is concentrated geographically or otherwise; i.e., employees enrolled in specific retirement plan. All of these factors influence caller volume and can be used to help your company scale its call center support offerings.

Additionally, findings demonstrate that the initial 60 to 90 days following a breach tend to be the most delicate. During this period call volume usually reaches its highest point. Beyond 90 days, firms report that call volume tends to drop dramatically. Thus, offering call center support services during this period of time is highly recommended, with the dedicated number then reverting back to some kind of internal customer service department or person.

3. Who Drafts the Call Center Script?

Call center agents are typically drawing their responses to consumer questions about breach details and remedial measures from a script provided by the breached firm. The breach coach should draft this script in concert with the public relations and internal communications teams. Content should be the primary focus of your breach counsel, while consistency and tone should be the principle focus of the public relations and internal communications teams. All messages communicated about the breach should be reviewed thoroughly.

4. Hours of Operations?

The hours of call center operation can vary; however, 24/7 service is most common. Additionally, depending on where impacted consumers reside, you may need to offer call center support in multiple countries and languages. Customers will not take kindly to discovering they can only communicate in English with the company that has just lost their personal information.

5. Cost of Call Center Support Service?

The cost of call center support services is usually bundled with notification services. Prices for the bundled services are discussed below in the notification section. Nevertheless, call center services can be used to manage your breach response costs. For instance, if you choose to offer affected consumers a full suite of remediation services, which is likely to score big in the court of public opinion as well as with consumers, then you can leverage the call center agents to counsel consumers on which of the offered services best address their concerns. This approach helps to avoid unnecessary enrollment in costly services.

Call center services serve a critical customer service role at a time when excellent customer service is paramount for your organization because your relationship with your customers is likely strained. Thus, it is important that you are confident that call center service you choose can not only effectively respond to customer inquires but also can strengthen customer trust by providing excellent customer service.

The pricing for call center services usually takes into account call volume, the length of time the center will be dedicated to fielding questions and the hours of operation, such as 24/7 versus normal business hours. However, since this service is usually bundled with notification, these factors also impact the total cost of for notification and call center services.

Notification

While notification is ultimately a legal matter to be handled by your breach coach, vendors offering data breach notification services play a critical logistical role in breach response. Mailing houses, as these vendors are often called, allow organizations to send thousands of notification letters to multiple jurisdictions in accordance with statutory timing requirements. In addition to mailing notification letters, many mailing houses also offer notification letter templates and handle the letter printing. Some vendors offer additional services, such as address verification. The price for this service is influenced by several factors including, but not limited to, volume, the number of jurisdictions involved and the weight of the letter. Typically, the charge per notice is decreased as the number of records or individuals increases. The prices for notification services range from 50 cents to $5 per notice.

Monitoring Services

After learning about a data breach, affected individuals can become emotional and very concerned about identity theft, fraudulent charges and other unscrupulous uses of their compromised information. In response, firms routinely extend an olive branch to breach victims in the form of an annual subscription to a monitoring service at no cost. Even though several types of monitoring services exist in the market, by far the most common monitoring service offered is credit monitoring.

The conventional wisdom that credit monitoring is the go-to, one-size-fits-all data breach remedy is just plain wrong. Recently, there has been more public awareness about the limited utility of crediting monitoring as a breach remedy, but it bears repeating here—credit monitoring is not always the best, or even a good, data breach remedy. The particular monitoring service your organization chooses to offer consumers should be based on the type of information compromised because different types of data pose different risks to consumers. Target is easy to pick on, but more than one person consulted for this report wondered why the company offered credit monitoring to affected customers when that really has little to do with the exposure of payment card data. There is some confusion, however, about the utility of the different monitoring services. It is important for your organization to fully understand the various types of monitoring services so that the service your firm offers addresses the risk created by the particular data exposed by your breach.

1. Credit Monitoring

Credit monitoring allows consumers to ensure that any changes to their credit report accurately reflect their credit history. This service alerts subscribers, usually via email, when certain changes on a credit report are detected, such as the opening of new accounts.

Although credit monitoring can detect fraudulent activity, it cannot prevent fraud in the first place. Further, rather than exposing fraudulent or suspicious activity on an existing account, credit monitoring merely detects the creation of new accounts or lines of credit that might be fraudulent. Accordingly, this form of consumer redress is not appropriate for all breaches. Credit monitoring subscriptions are most effective when a breach involves the loss or exposure of SSNs.

In terms of cost, credit monitoring is the most expensive monitoring service to offer. With prices ranging from $1 to $1.25 per person affected, offering this service could rapidly increase the price tag of your company's data breach. One way to save money, for instance, is to pay for credit monitoring on an enrollment basis rather than a per-record basis; only 10 percent of people will actually enroll in the service, so that way you're not paying for services people aren't using, Kilpatrick Townsend's Neiditz suggested in his interview with NetDiligence's Greisiger.

2. Identity Theft Monitoring and Protection

Many consumer services firms offer identity theft monitoring, protection or both. The distinction between the two services, however, is not always clear. The confusion is due in part to inconsistent use of the titles "identity theft monitoring" and "identity theft protection." In this report, identity theft monitoring refers to any service that scans non-credit report sources for suspicious or fraudulent activity and alerts subscribers if any is found.

Interestingly, many credit card companies now offer this kind of service as a matter of course. If a customer makes transactions, say, in two different states, or countries, for that matter, within a short period of time, a credit card company will communicate with that customer to make sure the transactions are both legitimate—provided they've opted in to the program. One way to potentially save costs is to utilize your call centers to let customers know about this kind of service and counsel them to opt in. In this way, you've provided valuable protection without having to pay for it yourself.

Identity theft *protection*, on the other hand, refers to any service that, in addition to monitoring, provides identity theft resolution assistance and/or identity theft insurance.

Identity theft monitoring and protection subscriptions are the most appropriate redress for breaches involving the exposure or loss of protected health information, passwords, SSNs and credit or debit card information. Misuse of these types of data, with the exception of SSNs, is not likely to show up on a credit report. As a result, to adequately mitigate the risk posed to consumers from the exposure of this information, it is necessary to offer identity theft monitoring.

On average, identity theft monitoring costs 75 cents per person affected. Identity theft protection services are not usually sold a la carte, but the total cost for credit monitoring, identity monitoring and restoration can range from $10 to $30 per individual per year.

One final note on identity theft services: Even if you think it unlikely that lost information will be used for identity fraud—for example, it's most likely that a stolen laptop will simply be wiped and resold—offering this kind of protection, say many commenters, has real PR value. It sends the message that "you're willing to do anything to fix the problem you've created," which has ancillary brand value beyond the remediation of the breach itself.

Pease International Tradeport, 75 Rochester Ave., Suite 4, Portsmouth, NH 03801 USA
+1 603.427.9200 www.privacyassociation.org