

Avoid a Meltdown: Reacting to a Security Breach

How your company handles a data breach can make the difference between survival and extinction.

By James Christiansen

Over the past year we have seen many examples of breach notifications that range from affecting hundreds to millions of victims. Looking further into the business impact of the post-breach processes, we quickly see that the way an organization reacts to the security breach can make the difference between a minor financial impact and a complete corporate meltdown.

Given the potential financial losses and other substantial impacts that can cost well into the millions of dollars, an investment in preparedness can really pay dividends regardless of when—if ever—an event does occur.

Looked at from the opposite perspective: "A firm's failure to communicate effectively after an emergency strikes can be more destructive than the emergency itself," as Richard Bierck says in an article for *Harvard Management Communication Letter*.

Remember the 1982 Tylenol case in which capsules of the famous painkiller were tampered with? It is one of the most important business cases in managing brand image. After a breach in the Tylenol packaging (and poison in the bottles), Johnson & Johnson took complete responsibility. It remedied the situation with decisiveness, leadership and effective communication. Tylenol as a brand survived the incident and continues its brand leadership where other brands and companies with less foresight might not have. The real costs in any security breach are in the long-term financial impact and productivity reduction, not the immediate remediation costs. Long after the event, the effects will be felt in increased oversight by regulators, clients and business partners. Whether that additional scrutiny reveals an effectively managed organization deserving of the continued trust of stakeholders is entirely in the hands of top management in the moments following a major emergency.

What a Breach Can Cost

To understand the true cost of a security event, you need to look not only at the reaction of the consumers involved (if you are facing a breach of consumer or cardholder data), but also at the reaction of your business partners and clients. How many of your clients will switch to a new provider? Some of the consumers you might lose are the same people who go to work every day in the procurement departments of your business clients. Do not underestimate the potential cascading effect of the loss of faith in your company because of a major consumer breach.

And yet, the impact of a major consumer data breach may be more muted on your corporate relationships than on your consumer relationships. It can take a year or more to move business from one company to another given contract restrictions, partner sourcing (e.g., RFPs) and the ability to find similar products for a competitive price. The old saying "time heals all" enters into the equation. In many cases, moving to a new provider is a more emotional decision for individuals than it is for large companies. "I am taking my business elsewhere!" for a person may be expressed by a company as, "Let's see how they react before we incur the cost of moving our business with them." So even though the people who make decisions in corporations are also consumers, the inherent delays and costs in the ability to shift the relationship will lower the percentage of companies that actually switch providers.

But how many lost "strategic accounts" does it take to add up to a much greater financial disaster than the simple remediation costs to close the immediate source of the breach? This emphasizes the importance of the immediate public reaction your company mounts—the one you meticulously planned before the breach took place.

Other serious but less obvious costs may result from a breach handled poorly. Your company may get sued by people or companies who claim (often in media-covered statements and press conferences) that you were negligent—that you knew or should have known this could happen and failed to take adequate precautions. These lawsuits will be costly and time-consuming to defend and in many cases will lead to settlement payments. The regulators who oversee your business may find that you must take certain costly steps to double-check and triple-check that such a breach will never happen at your organization again. Regulatory sanctions may include fines in the millions of dollars as well as regular review by independent auditors of your program of protections. Recently, one such penalty entailed biennial reviews over a 20-year period.

Internally, you may need to hire a new chief privacy officer and staff other positions dedicated to bringing about the proper level of controls. And the overhead in terms of productivity of professional IT staff devoted to integrating controls into your operations will likely be substantial. Many, if not most of these costs and impacts are uninsurable. Any way you look at it, your breach is going to cost you a lot. But does it have to cost you the company?

What Is an MIRT?

Establishing a management incident response team (MIRT) is key to making a difference. The MIRT is sometimes called the crisis response team and is very different from the commonly understood cyber incident response team (CIRT). The CIRT is focused on identifying: *What happened? How did it happen? What damage has been done? And how do we prevent it from happening again?* The primary task of the MIRT is to take the information from the CIRT and begin the process of managing the event from the perspective of the critical stakeholders you depend on.

The MIRT is a cross-functional team consisting of the CISO/CSO, chief privacy officer, general counsel, chief compliance officer, business line presidents and public relations (or functional equivalents). The primary role of the team is to first ensure that *accurate and complete* data is gathered concerning the incident (when, where, what) and to determine the appropriate parties that must be notified both under the law and consistent with corporate values. (Many organizations will decide to go beyond the legal or contractual requirements to protect the clients and consumers.) The MIRT also gets regular reports from the CIRT about necessary remediation and may set corporate funding and capital spending priorities on specific remediation initiatives.

But the MIRT's primary role involves communicating to its stakeholders in a highly targeted manner. The goal of this communication is essentially to uphold and serve the relationships that have been built up over the years in the face of the breach incident and assure key stakeholder groups that your organization understands how the breach affects them and what you intend to do about it.

Step by Step

Start by developing realistic scenarios that could possibly occur sometime in the future. A small number of different scenarios that deal with possible events such as external fraud, a malicious insider, a technology hack, lost media, data center disaster and an external security breach is a good start.

The next step is to create a high-level set of tasks that must be accomplished in each scenario. Examples include notifying the MIRT of the incident (this task is usually assigned to the CIRT, members of which may also be part of the MIRT), gathering the *facts* of the incident, determining who should be notified, and creating the notification letters and notices. Given that the members of the MIRT are leaders in your organization, a detailed task plan is not necessary or appropriate. But a list of tasks in the form of a RACI (responsible, accountable, consulted and informed) chart can be very effective. Compile a reading file for members of the MIRT consisting of studies and thoughtful news stories covering similar events in your industry and elsewhere. Don't forget developing markets where your firm is just getting established; different cultures may require a different communications approach. This background material may contain video clips of broadcast news interviews and/or testimony that others have given in the aftermath of incidents.

It will be interesting when you discuss with your MIRT the question of the notification letters. Who writes the notification? Who will be consulted, and who will approve the letter for distribution? But if you want to see the group head for the hills, ask the question, "Who will sign the letter?" Should it be the chief privacy officer? Should it be the business line president or should it be the chief security officer? Most likely it will be whoever missed the meeting when it was decided.

During the excitement of an event, time is important and will seem to pass very quickly. Decisions must be made promptly about what to say publicly, and what to say to key business clients, employees, city leaders, members of Congress from your state and so on. These decisions often may require detailed consultations with subject matter experts and senior managers in charge of legal, public relations, insurance or governmental affairs, etc. Making as many of these decisions in advance is required not only to meet your own team goals, but also to meet any regulatory requirements.

Communication Is the Key

As part of your scenario exercise, prepare the press releases and major stakeholder communications. This allows an important added benefit of preparing communications that can be reviewed ahead of time by your executive team, internal public relations and your external public relations firm. The style of the communication is very important: It should be informative, take responsibility and reassure your audience that the matter is being handled. It should state how importantly your company views the matter and establish how clearly your company understands the impact on its customers and partners. Your best decisions are not made during a crisis, nor are your best communications written then. A key advantage of in-depth planning will be in being able to pull out that document, which has already been reviewed, and change a few words to meet the situation. Being able to review and create these communications during times of less stress results in a better product consistent with your corporate values and public marketing strategy. Thorough advance preparation will put your company in a position to truly minimize the impact of a breach. Without preparation, you may be lucky even to survive it.

Once the reporting requirements are determined, the team focuses on defining the target audiences and the form of communication they require. Key audiences that need to be considered are the affected clients and consumers, partners, law enforcement, government regulators, investors, board of directors, executive management team, corporate affiliates, foreign country operations and employees. Each of these bodies requires a consistent message but certainly will differ in the style of communication that works best.

Here is where all the preparation pays off. Your organization will communicate to the target audience with accurate information presented in a way that will reassure rather than alarm the audience.

Recently my aunt received a security breach notice and called me for advice. It was obvious from her tone that she was very upset and she said, "It says here in the letter that I should call them if I have any questions, but I don't even know what to ask!" Remember that the general public is not going to have the same level of understanding as we do working with identity theft and account takeover. Make sure the communication includes key FAQs targeted to the audience so that the reader can understand the risks and what you have done to mitigate them.

Now Execute!

How are you going to take responsibility? One way is to offer assistance to your customer. Consider such things as telephone hotlines to assist the customer in understanding what the risks are and how you are willing to help. Offering free monitoring of a customer's credit report in the event of a breach of consumer-oriented information is another way to help alleviate concerns. Depending on the nature of the breach, you may want to tailor some special services to those of your customers most seriously affected.

Make sure your executives are prepared to answer the questions that are going to come hard and fast from the media, customers, employees and even suppliers. If there is an event, all the work will pay off. The main mission is to retain the trust in your brand that has been built over years of hard work. Take responsibility, sympathize with your

customers, and provide accurate and complete information to your stakeholders. Remember that lightning can strike anywhere, and as a prepared organization you will be able to weather the storm.

James Christiansen is chief information security officer at Experian.

2002-2006 CXO Media Inc. All rights reserved.

Reproduction in whole or in part without permission is prohibited.

Dated: August 01, 2006