Don’t Wait for a Data Compromise

When it comes to a data breach, the question is not “if” you will become a target, the question is “when.” Operational preplanning and readiness can control costs, improve customer loyalty and preserve your reputation.

By:
By Krista Tedder
Product Owner, Risk Management and Fraud Solutions
First Data
Data Compromise: Are We Really Prepared?

On Feb. 20, 2009, one of the largest payment card transaction processing companies in the United States reported a security breach. Information about the incident emerged slowly and few realized the magnitude and widespread impacts. The final tallies proved shocking: over 100 million card accounts and 100,000 merchants impacted. The company’s stock plunged by 75 percent within six weeks.

This breach event was the ultimate nightmare, a “perfect storm” data-compromise scenario:

→ Consumers learned of the breach via sensationalized media reports.

→ The company was obliged to make public statements in the absence of necessary facts.

→ The company’s business suffered a major setback, a financial and public catastrophe.

→ Issuers had to act quickly, with little information, to notify customers and determine if cards should be closed and new cards reissued.

Stunning as it may be, this incident is merely one event in a growing trend of evermore sophisticated and frequent data compromises.

→ Privacy Rights Clearinghouse, a consumer advocacy organization, states that more than 340 million records containing sensitive personal information have been breached in the United States since January 2005—a figure that does not include the records impacted in the breach discussed above. Furthermore, the true number of records at risk cannot always be ascertained, and thus the number of files impacted during this period could be significantly more than reported.

→ No financial institution or merchant is immune. While traditional data breaches like insider fraud and lost laptops remain common, new threats such as Web application attacks and keylogging trojans are on the rise—and still more innovative techniques continue to surface. According to the 2009 Ponemon Institute U.S. Cost of a Data Breach study, approximately 85 percent of businesses have experienced a data breach, up from 60 percent in the 2008 study. The fourth annual U.S. Encryption Trends Study by Ponemon exposed similar statistics.

→ In addition, HIMSS Analytics discovered unsettling news in a recent survey of hospitals and businesses: 50 percent of large hospitals experienced at least one data breach in 2009.

Data breaches continue to take organizations of all types and sizes by surprise, and responding to data compromise comes at a staggering price. A 2009 survey conducted by Ponemon Institute shows that organizations spend on average $6.6 million per incident and more than $200 per compromised record.

As employees divert their focus from core activities to crisis management, new-account generation and cross-sales stall, and revenue suffers. According to the Ponemon Institute study, this accounts for roughly 70 percent of costs associated with a data breach event. The total damage, however, may take years to calculate.

→ Damage to an institution’s reputation. When a data compromise occurs, media reports can have immediate, painful effects on an unprepared business. The news may slow over time, but the scars remain: Reminders of past data compromises are likely to revisit headlines as new major crises occur.
Don’t Wait for a Data Compromise

→ **Loss of customer loyalty, confidence and relationships.** According to consultations with First Data financial institutions, consumers cast equal blame on the entity responsible for losing their data and the account issuer. After a data compromise, customers who are reissued credit cards decrease their transactions by 30 percent, and an additional 20 percent never activate the new card.

→ **Unnecessary and lingering expenses.** A company with poor contingency planning is likely to throw more money at the problem over time in an effort to regain control over its brand and operations. In addition, litigation costs may linger long after the breach has been resolved.

It is no wonder that businesses targeted by data thieves are often unsure of how best to respond. As events unfold, companies often react in an ad hoc, unscripted fashion, rushing to put out fire after fire as they arise. The cycle is difficult to break as long as a company remains in crisis reaction mode.

However, there are things you can do now—before a crisis—that can help you manage a data compromise more effectively should you become the victim of such an incident. You will be in a better position to control costs by taking swift and efficient action that is appropriate to the scope of the event, and you will avoid the self-inflicted harm that can be caused by response improvisation.

An important element of any rapid response plan is a thorough communication plan that lets you create thoughtful and articulate messaging that enables customers and partners to understand the risks and recognize what you are doing to protect them. Meticulous risk analysis and a well-designed communication plan can mitigate the effects of a data compromise event and may actually help you build customer loyalty during a difficult time for everyone.

So what are the key elements of a good risk analysis and communication strategy?

**Taking the Initiative With an Effective Response Strategy**

Security breaches will continue to happen, in spite of continuing efforts to prevent them.

You cannot anticipate every internal and external threat, nor can you predict when an employee will prove dishonest or capable of a major mistake. No security system is bulletproof, and there is never a shortage of motivated, educated individuals capable of exploiting your every vulnerability.

Prepare your mindset: The question is not “if” your data will be compromised, it is “when.” And when a breach does occur, how can you respond? Though you cannot predict when a breach can occur, an effective response plan will limit the eventual cost to your business.

A successful data breach response strategy consists of three elements, each determined by your business model and business processes:

1. **An Event Response Team** consisting of key executives and personnel from areas of the business that would be affected by a data breach.

2. **A Risk Assessment and Response Matrix** that guides your team in determining how harmful a particular breach event would be and how you should respond to it.

3. **A Communication Plan** designed to control outbound messaging related to the event and to maintain public confidence.

A survey by research firm Millward Brown found that more than half of companies surveyed either do not have a plan for dealing with a data-compromise event, or they say their current plan is not adequate.
Building Your Event Response Team

Members of the Event Response Team represent a variety of operational groups within the business, such as:

- Audit and compliance
- Branch administration, including representatives from all customer-facing groups
- Human resources
- Key executives and senior decision-makers
- Legal
- Marketing and public relations
- Operations/information technology
- Risk management and security

The composition of the Event Response Team will vary from company to company and is dependent upon the way the organization is structured. It is critical, however, that senior executives be part of this team: the actions taken post-breach will have a profound impact on the future of the business. Event responses must be coordinated and consistent with your business objectives; each member of the team should understand his or her specific role and how the event response strategy works. Engage the team by providing every member with a sense of process ownership through active participation in the response strategy development.

Creating Your Risk Assessment and Response Matrix

Once the Event Response Team is in place and each member understands his or her specific responsibility, it is time to build a Risk Assessment and Response Matrix that is specific to your business operations.

Creating this matrix is the most challenging part of building a response strategy and is first and foremost the work of the Event Response Team—with some help from outside resources, which will be discussed later in more depth.

There are many kinds of data breaches: Some are harmless and pose no real threat to individuals or organizations, while others expose everything and have a high probability of resulting in significant financial loss. The purpose of a Risk Assessment and Response Matrix is to provide event responders with a tool to help evaluate the seriousness of a data breach and provide guidance as to how to respond to a specific event.

Points to Consider:

- Everyone should have a backup. Being single threaded in any organization does not provide stability. You will need to carry on even if someone is sick or on vacation.
- You can assemble more than one team:
  * Working teams are responsible for carrying out the tasks.
  * Decision teams are responsible for making key decisions.
The above illustration is a very simple but holistic example of a Risk Assessment and Response Matrix, comprising the three essential elements of an effective risk assessment and response plan:

→ **Risk of Unauthorized Use** – a measure of how accessible the compromised data is to whomever has it.

For example, if a highly secure disk drive is stolen, perhaps the data is encrypted and/or the device itself will operate only on a specific computer system on your premises. In this particular case, you can determine that although the data is in unauthorized hands, it is unlikely that the data will be accessed. If, however, the disk were instead a common device with unprotected data, it should be assumed that the data contained within has been exposed.

Many factors can go into evaluating the risk of unauthorized use. How do you store and process confidential data? How can you protect data accessed by multiple employees from different departments? Risks are specific to your organizational structure and business model, and therefore your response must accommodate each of the various ways your data can be compromised: for example, a server breach, a malware attack, a stolen device, or internal/external fraud.

→ **Risk of Harm** – a measure of how damaging the data is in unauthorized hands.

For instance, if the compromised record contains only a phone number or place of birth, it can be determined that the risk of misuse and consequence is very low. If, however, a credit card account or bank account is compromised, the risk of serious loss is far higher and the subsequent resolution more complex.

The scale you use to measure the risk of harm depends a lot on the types of confidential information you handle and how it can be accessed. For example, if you store data such that accessing one type of record does not necessarily compromise other data, this may partially dictate how you define the risk. Or you may need to take into consideration the risk of multiple pieces of data being compromised. In the case of a breach involving card data, the risk of harm may be dependent upon other variables: card number only, card and expiration date, card and CV2 code, card and full magnetic-stripe data, or various combinations, each presenting a unique risk.

**Risk of unauthorized use and risk of harm** work together in the matrix to define the aggregate risk in a potential data breach, and responses are built based on severity of threat.
→ **Risk Response** – a measure of possible responses to various degrees of compromise.

The example in the illustration shows very simplified response options. In reality, there are many possible responses you can undertake or may be required to perform based on the type of data compromised, the severity of the risk and also on your business model. For example, if the compromised record involves card data, you would assess the breach, monitor affected accounts, issue communications to customers, block and reissue cards, or initiate a combination of these responses.

Three key factors should determine the layers of your response:

1. **Ongoing risk assessment and business impact** – When a breach is detected, you will need to research the severity and extent of the compromise. You need to determine as quickly as possible the scope of the breach and the risks associated with the compromised data. It’s important that you understand its impact on your business, and how it affects your partners and customers. You must also take immediate actions to prevent further data compromise.

2. **Legal notification requirements** – As you determine the nature and severity of the breach, you will need to be compliant with laws governing notification of a data breach. In the United States, 44 states have specific laws governing notification of data breaches (in addition to potential federal guidelines). If you have operations or customers in those states, the legal representative on your Event Response Team should be conversant with regulations in those various jurisdictions. State regulations governing breach notification are published in a number of locations, including the Web site for the National Council for State Legislatures (www.ncsl.org).

3. **Customer and partner communication plan** – One of the most important aspects of your Event Response Strategy will be the way you communicate to your partners, customers and the press about a data breach event. Ideally, you will want to be in as much control of the messaging as possible. Additional details about communication planning are provided in the next section.

Like other aspects of the event response, you can define the details of outbound messaging such that the Risk Assessment and Response Matrix becomes an effective tool for triggering the right communications at the appropriate times.

An effective Risk Assessment and Response Matrix provides clear definitions of all risk factors, defines the trigger events for different levels of response, and outlines in detail the appropriate responses for different types of events and different levels of risk.

It is imperative that the Event Response Team play a central role in developing the Risk Assessment and Response Matrix for the following reasons:

→ Each team member was selected for his or her expertise and familiarity with business processes, the various types of confidential data handled internally and via partnership, and the potential impacts a loss of data will have on the business. This knowledge is the key to creating an effective matrix.

→ The team consists of the front-line responders, and therefore it is critical they possess an intimate familiarity with the plan.

It is recommended that you engage the services of a consultant or service provider who specializes in handling data breaches and responses. Professionals accustomed to managing data-compromise events on a regular basis can provide a unique perspective to your planning and can work in collaboration with your team to minimize the impact to the daily operations of your organization, create efficient and effective communication vehicles, and enable your business to focus on maintaining its brand integrity. Strategic outsourcing of tasks will reduce overall costs of managing data breach events while improving customer response.
A Solid Communication Plan – The Key to a Successful Response

All too often, especially in large-scale breaches involving major businesses or millions of card accounts, public communications are managed poorly. With limited facts and no prior planning, a company pressed for information and answers will frequently issue public statements that introduce erroneous information and unneeded confusion—the end result being disgruntled customers and angry business partners.

As part of building the response plan in the Risk Assessment and Response Matrix, you need to give careful consideration to how you will handle public communications. You must stay compliant with the law, and you need to assure your partners and customers of your exact plan of attack.

The best communication policy, and one that customers and business partners will respect even if they don’t like the news they are getting, should be guided by these simple principles:

→ When a breach is contained, announce what you know when you know it.

→ If there are things you do not yet know—perpetrator, details of how the attack was done or who was responsible for the breach—do not guess or speculate about them. Be honest about what you do not know, and do not attempt to provide speculative details. Avoid spreading misinformation that you will eventually have to correct or retract.

→ Explain why you cannot reveal certain information. For instance, some information may compromise an investigation or future security. Do not use this as an excuse for withholding information unless this is truly the case, as doing so can present a future public relations problem.

→ Describe, in specific detail if possible, what you are doing and why you are doing it. Partners and customers need to hear what you are doing to protect them.

→ Be honest, above all else. Your customers and partners will appreciate it.

Using these basic principles as guidance, there are many channels available for rolling out your communication response: press releases, press conferences, notifications by mail, toll-free hotline numbers and call centers, Web site information and announcements, as well as any other form of communication common to your business. Your Risk Assessment and Response Matrix should specify in detail when you will initiate communications related to the discovery of a breach. If you need to prepare specific communications covering certain aspects of the breach, or if you need to set up a call center to respond to questions, the triggers for these responses should be built into the matrix and response plan.

When it comes time to release communication specific to a data breach event, the goal of a bad-news management plan should be containment and positive counteraction. Follow these critical steps:

→ Prepare for the worst by envisioning the best: Hypothesize the worst-case scenario and then determine what would be the best possible outcome. Structure your communication plan by working backward from this desired outcome, identifying steps needed to reach this goal.

→ Go from start to finish in words and pictures: Ensure members of the Event Response Team agree that the communication plan is consistent with the response matrix.

→ Do a dry run: Conduct simulations as close to reality as possible, in both time and scope. Include vendors and outside experts you may rely upon in your tests.

→ Establish leadership contingencies: Think through the “what ifs” and determine a second and third chain of command in all critical areas.

→ Coach and train spokespeople: Make sure they are trained once the plan is in place and then provide ongoing training to ensure that they are well prepared. They will be the voice and face of your company;
how well they manage the message can make or break your ability to control the damage.

→ **Know where everybody is and how to contact him or her.** Keep phone and e-mail contact information accurate. Ensure the plan is updated with information about vacations, medical leaves or out-of-office assignments.

**Conclusion**

Your company will be affected by a data-compromise event. The only uncertainty is when. Through the development of an upfront, organization-wide response strategy, you can be ready tomorrow, next week or next year.

A proper response strategy needs to include:

→ **An Event Response Team** consisting of key executives and personnel from areas of the business that would be affected by a data breach.

→ **A Risk Assessment and Response Matrix** that guides your team in determining how harmful a breach event is and how you should respond to it.

→ **A Communication Plan** designed to control messaging around the event and maintain the confidence your customers and partners have in you.

Avoid These Common Communication Errors:

→ **Winging it:** Top executives pride themselves on speaking off the cuff to the media, but style cannot trump substance in a crisis. Ensure company leaders and spokespeople will communicate a unified message and ensure the plan includes giving each of them the facts and figures they need to answer media questions.

→ **Wandering:** Straying from the main issue, and your unified message about it, can be dangerous in a crisis. Be concise, stick to the facts and do not provide additional or irrelevant information.

→ **Getting waylaid:** Questions from the media may be tough, but they should not surprise you if you have prepared for bad-news scenarios. Remember that the answer to any question contains an opportunity to get your message out.

Being prepared can help you save money and time by taking swift and efficient action that is appropriate for the scope of the event. It can ensure you have a well-thought-out communication plan that lets you shape the message during a crisis. And, most important, planning ahead gives you the ability to transform a crisis into an opportunity to strengthen customer loyalty and retain business.
The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

About the Author

As product owner for Risk Management and Fraud Solutions for First Data, Krista Tedder is responsible for the development of risk management, fraud and collection solutions that meet the market challenges faced by financial institutions. During her tenure with First Data, Tedder has consulted with financial institutions to mitigate risk exposure while improving cost control and customer relationship management. Prior to joining First Data, Tedder spent five years with MBNA in various positions focused on risk management and fraud.

For more information, contact your First Data Sales Representative or visit firstdata.com.