Preparing for the Worst: How to Effectively Communicate to the Press and the Public Before and After a Data Breach

CYBER SECURITY

FMI

THE VOICE OF FOOD RETAIL

TABLE OF CONTENTS

Just as a company's management and IT teams need to plan how to respond internally to a breach of the company's card data, so do its communications personnel need to plan its public response.

This brief guide recommends how to prepare for the worst while fielding work-a-day questions from reporters during quiet times so as to place the company in the best possible public position should a breach occur.

We recommend a collaborative approach among senior managers, tech experts, legal experts and a public relations team, just as the larger group that will manage the entire crisis will be a collaborative combination of experts. And - like your tech advisers - we urge you to start detailed planning now, so you will have a solid media strategy in place should it ever be needed.

This guide is in two parts. The first section addresses tactics to consider before a possible breach, how to prepare for the future and how to position the company now. The second part provides guidance for dealing with a crisis should it occur.

PART ONE: GETTING READY BEFORE A BREACH

PUTTING TOGETHER A TEAM

Your company will probably already have a big team of experts identified to deal with a breach should one occur. We suggest a smaller group that prepares specifically for crisis communications in the event of a breach while simultaneously formulating responses now to field run-of-the-mill questions from the press about security.

We suggest picking a security expert inside the company to respond to less urgent questions before a breach occurs. This should probably be a senior tech executive who would respond to big publications and technical publications, since that person will know the most about the technical aspects of security. You may need to give him or her media training, which includes a dry run session answering potential questions about the company's security.

A senior PR person can give general prepared answers to smaller publications for which the senior tech person does not have time.

The combination of the PR folks and senior tech staff plus a representative from the company's legal team should round out a communications group to formulate general responses about the company's security precautions while working on a crisis communications plan.

A single person should be in charge of the group and enforcing deadlines for accomplishing the strategies below.

Make sure everyone on the team is at least conversant with the company's IT system and can talk capably about information security procedures.

RESEARCHING THE AUDIENCE; LEARN MORE ABOUT THE REPORTERS

One of the first steps should be to identify all reporters who cover the industry and all who cover data breaches, both as a business issue and as a government issue on Capitol Hill.

If you have the resources, prepare a short briefing on each reporter: look at their latest stories to discern a particular focus, check their LinkedIn profile to learn more about their employment history, and have your PR team contribute any personal knowledge about past stories.

LEARN MORE ABOUT THE CUSTOMER

You're really speaking to your customers through the press when you talk about security. Know all you can about them: How many use credit or debit cards? Do they use a PIN, get cash back? What's their average purchase? How many are using government issued benefits cards - as you may need to address security on those cards as well? Are there any demographics that impact payment preferences? It helps to know as much as possible about your audience, and the more you know about the group the more likely you are to address its concerns in your messaging.

CRAFTING THE MESSAGES

This group needs to work from a set of major points to set the tone for the company's response both to run-of-the-mill questions and questions after a breach.

The messages for the questions before a crisis should include:

- "We're aware of and deeply concerned about security. We are taking all possible precautions, investing a great deal of time and money in keeping our customers safe."

- "We will be as open and frank as we can in discussing security with press and customers in order to reassure our customers."
- "And most importantly, our main concern is our customers. From the safety of the food we sell to the security of our customers' financial information, we are committed to our customers. We take our duty to our customers extremely seriously."

And while you may disagree internally with the following point, it is important to be and seem as honest and realistic as possible. That is why you should remind reporters in your interview that no system is fool-proof, but you are doing all that is humanly possible to make yours so close to impenetrable that it will discourage all but the most sophisticated hackers.

In other words, prepare a reasonable, realistic response for reporters if they call to ask what you are doing to safeguard customers. Recount the usual safeguards all grocers and retailers are doing, and recount anything grocers, and your company in particular, are doing in addition to the usual practices. This could include certifications or extra security features.

RESPONDING TO TOUGH QUESTIONS

Smart reporters will try to find places where they believe you have not done all you can to protect data. They will do this by citing security experts who may see perceived weaknesses in your company or they may do it by comparing your measures to some standard they believe is superior.

Either way, identifying possible shortcomings and either fixing them or showing they are not problems should be one of the top priorities of the committee, working closely with the IT department. They should question IT personnel the same way a reporter is likely to challenge the company spokesman, and the committee should find good answers to every question and critique it can conceive.

You should also anticipate questions about food and beverage companies being the biggest targets of cybercriminals, as some statistics seem to indicate. If asked, the company should be honest about the statistics and have formulated a response as to why this is the most targeted industry or formulate a response as to why the figures are not accurate.

BANKS AND BREACHES

You can use these low-key, non-crisis interviews to make the larger points about security breaches and the banks and credit card companies, although you must be careful not to seem to be shifting blame to the banks or trying to score points on the swipe fee debate.

It must be up to each company to decide if it wants to go there. But it may be worth the risk to make the points and inform the public about how pervasive breaches are across all industries, most extensive in the financial sector, but least reported publicly.

If you decide to talk more extensively about this area, you may want to mention:

1.) PIN is currently the most cost-effective way to reduce payment card fraud and can be implemented the fastest. It cuts fraud to one-sixth of the level than a transaction without PIN. Every card should be enabled with a PIN, even those with a computer chip should also have a PIN to be more secure, yet Visa and MasterCard's new system doesn't require a PIN. Issuing CHIP-only cards, instead of PIN-enabled, is a missed opportunity to add a much stronger layer of security to the card. Our industry is trying to push financial institutions to move in the same direction many state WIC programs have already gone with a more secure PIN and CHIP option. Additionally, all SNAP and E-WIC cards are PIN-enabled, even if not CHIP cards.
2.) There are also open chip technologies other than the EMV (European MasterCard Visa) system, which is owned by Visa and MasterCard. We need an open technology that encourages competition and more security, not one owned only by the dominant players.
3.) MasterCard and Visa control the security standards for cards and payment card data for banks and merchants alike via a group called the Payment Card Initiative or PCI, yet they bear none of the costs of fraud. The people who take the costs of fraud - merchants and issuers - need a voice in the leadership development of standards bodies like PCI Co and EMV Co. to ensure customer's and retailers interests are represented and protected.
4.) In short, merchants have skin in the game - we absorb as much or more in losses - than the other players, the banks and the card companies. Yet we have the least opportunity to influence standards for the best ways to protect our customer's cards and systems from hackers.

MONITORING THE MEDIA

Stay abreast of developments, such as news of new breaches. Adjust your prepared responses, if necessary, such as to say how the new breach does or does not affect your customers and your company and why.

Just as important, follow the *mood* and the *tenor* of the coverage. Are certain themes developing in the coverage, and do they favor retailers or disparage them? The communications committee must closely monitor breach coverage every day - in trade publications, the mainstream media and the blogosphere - and making adjustments to your responses accordingly.

If consumers seem angry, take note of that if pressed for an interview: "People are angry, and we understand that. We're angry too. " Are there ways to address customer fears? Anger?

Then turn it into a positive, and show how retailers bear the brunt too (without seeming insensitive to consumer concerns): "But we're taking every step we can to protect people. When customers are reluctant to use their cards out of security fears, it hurts all of us - consumers, retailers, even the entire economy. That's why we're so concerned about getting this right and thwarting hackers, especially to protect our customers."

WHAT ACTIONS TO TAKE?

Try not to be too proactive in shaping media coverage yet. That comes later if you have a breach. Otherwise you generally don't want to insert yourself into a negative story like this if possible.

Again: Unless you have an absolutely fool-proof method of foiling data thieves or have caught a hacker red-handed, you should not be pushing your company as a source for this story in an attempt to shape coverage. You run too great a risk of being made to seem overconfident if in fact a breach does occur.

That is not to say you play dead or avoid commenting on questions. This is where your safe, vetted, stock answers hammered out by the communications committee come into play. You are not out in front pushing this story, but you are not ducking it either.

It will be hard to resist the temptation to trumpet some major, expensive new safeguard the company has installed. But it does put your company in the forefront of a largely negative story, at least temporarily; it sets you up for a fall if you are later hacked; and it makes the company seem reactive to a longstanding phenomenon, prompting questions about why you didn't install this new advance sooner.

DON'T FORGET THE REAL AUDIENCE: THE CUSTOMER

When questioned by a reporter, you want to convince the press you are taking every precaution and worrying foremost about your customers. That is crucial, because if the reporter doesn't believe you, then your customers are not likely to either.

Speak to them through the press if you are interviewed. Be as honest and transparent as possible; show them proof that you have their best interests at heart and are constantly on the lookout for hackers. Haul out your accreditations and show how much money you are spending on security, just as retailers as a group are spending billions of dollars on protecting against hackers.

But again, if you have not had a breach, your customers are not specifically worried about your company. Don't give them cause to worry now by drawing attention to your company unnecessarily.

On the other hand, quietly ensure that your company and trade associations are members of all the anti-hacker, pro-cyber security groups. Develop a list of those groups your company participates in.

In short, don't dodge interviews about data breach if you have not been breached; but don't seek them either.

HOW TO MEASURE YOUR PROGRESS

At the first stage of this process, you should have:

- Assembled a team and appointed a leader and public spokesperson
- Made someone responsible for monitoring breach stories and analyzing them
- Set a deadline and assembled a briefing book of reporters covering your company and breach stories
- Set a deadline and created a set of messages to be the backbone of any response to any non-crisis breach questions
- Inventoried the company's data security, anticipated questions and formulated effective responses
- Media-trained the spokesperson for non-crisis stories
- Researched your customers' payments preferences and fears and shaped your messages accordingly
- AND be well on the way to finishing the crisis response plan, which is the subject of the second section.

PART TWO: AFTER A BREACH

BREAKING THE NEWS

It is important that your company breaks the news of a breach itself, if possible, law enforcement and legalities permitting - and preferably through a press conference where reporters can ask questions.

In assessing the breach, the first step regarding communications is determining what your company can legally disclose, when and how. Once you have that nailed down, it's time to start thinking about what to disclose.

WHAT QUESTIONS TO EXPECT

The first questions reporters will ask are the same questions you will be asking internally:

- How serious is the breach; what is the impact on consumers and the company? In other words, which systems are affected?
- What information/customer data was stolen?
- What is known about the hackers?
- How did they breach the system?
- How, if possible, could your company have prevented the breach? What are you doing to seal the breach and prevent another?
- If law enforcement is involved, how is the investigation progressing?

SETTING UP FOR THE FIRST PRESS CONFERENCE

As soon as possible, you need a press release and talking points for your spokesperson.

Your crisis response plan should designate a spokesman depending on how serious and widespread the breach is. If it's minor, perhaps your media person on the committee or your designated pre-crisis breach spokesperson can handle it, signifying to the media a proportionate response. If it's widespread and serious, one of your top officers should address the press.

For the press release, you need to be as candid and informative as possible, given the circumstances, to build trust with the press and reassure customers.

Be especially careful to tell affected customers what to expect and how they can guard against fraud on their cards.

Emphasize any extraordinary measures the company is taking. And set up a special section of your website for customers and for press addressing the breach, incorporating an overall statement reassuring customers and expressing abject regret; your latest releases;; and any other information and services the company may offer.

Take care to make this section as simple and consumer-friendly as the other portions of your website intended for the general public. It's especially important to explain, for instance, highly technical legal or IT terms and the like. Make sure the advice about protecting customers' cards is the freshest, is highly visible and easily understandable.

A SAMPLE PRESS RELEASE

An initial, brief release might look like this:

XYZ Corp. said today that computer hackers had stolen credit card information affecting as many as 2 million customers who bought groceries from all XYZ's 250 stores - which are in Delaware, Pennsylvania and New Jersey - from July through September.

The grocery chain is working with law-enforcement authorities to determine the impact of the theft. Meanwhile the company advised customers who suspect unauthorized activity on their cards to call 800 528-7900.

Customers will have zero liability for any fraudulent activity on their cards.

"Our customers are always our foremost concern," said XYZ Corp. CEO George Wilson. "We will do everything we can to minimize the impact on them, and we deeply regret the inconvenience and concern this has caused."

XYZ has hired a leading forensics firm and a computer-security firm to help in the investigation.

For more information, go to: www.XYZCorp.com/databreach.

XYZ started with a single store in Wilmington, Del. in 1946 and with its low prices and high quality has built the third-largest grocery chain in Delaware, Pennsylvania and New Jersey.

TALKING POINTS

Now that you have a release, you will need talking points for the press conference and handling reporters' questions.

You may question whether at this point the release is enough and whether it's too soon to face a lot of questions at a press conference for which you may not have the answer.

Our advice is that reporters will only bombard you with questions anyway. Better to show them you are trying to be open to generate more trust and cooperation by holding a conference and taking their questions all at once.

WHAT KIND OF PRESS CONFERENCE

One way to minimize the risk is to hold the briefing via conference call. That way you guarantee no television images of your spokesman being pummeled with hostile questions; your legal and IT advisers can confer on answers with the spokesman offline, if needed, during the call; and finally, you can include every reporter across the country who is interested, not just reporters in your headquarters' city, especially if you are not in a major media center.

Very important: Your talking points should include any extra precautions you have already taken before the breach to protect your data, including certifications like the credit card companies' PCI standards, hiring consultants and other relevant actions.

But above all, continually make clear that your customers are foremost in your concerns and that you are doing all you can to protect them and restore their confidence.

SETTING A TONE

You must set a tone of *openness, concern, contriteness and determination* right from the beginning.

If you don't know something, say so, but be sure to add that you are working on getting the information. If you can't disclose information for security or legal reasons, say so, if possible.

Using the press lists your media department has already compiled to contact reporters by phone and email, schedule the press conference (but don't say what it's about) for as soon as possible to prevent leaks. It is best the news comes from your company, not an outside source.

If the news has already broken, then it becomes even more urgent to get your message out. In this case, you may want to consider putting your press release out on one of the press-release distribution services, as soon as your breach committee vets it, with a notice that you will hold a follow-up press conference at a certain hour that day.

HANDLING THE ISSUE OF BANKS AND CARD SECURITY

There is one talking point you must be extremely careful about: Your company is the victim of a crime, too.

This is no excuse for lax security, and it's extremely important that your company is not seen as using this as an excuse. But it's also important that your spokesperson notes that cybercriminals are becoming increasingly sophisticated and harder to stop.

According to American law enforcement agencies, such as the Secret Service, which investigates breaches, hackers are increasingly operating offshore, which means our law enforcement needs cooperation from foreign companies. This is the context in which retailers operate, and it is worth pointing out to reporters.

But there is another delicate aspect of this talking point: These hackers target the U.S. because its data security for debit and credit cards is not as advanced as other developed countries, both in embedding sophisticated computer microchips in cards and requiring PINs for all card transactions instead of signatures only. Half of the global fraud involving debit and credit cards occurred in the U.S. in 2012, according to the latest figures available.

Here's where the problem arises: "Who is to blame for this state of affairs?" is a natural question with which reporters will follow up.

Your company must be careful not to be seen blaming its breach on the banks. Instead you must find a way to get across the point that banks and card companies are a major part of the problem without seeming to be shifting or shirking responsibility.

There are myriad ways to handle this question. But start with these facts:

- While bankers loudly complain about their costs after a breach, retailers pay the banks' costs multiple times over - with both up-front fees when consumers use cards and in reimbursements after the fact.
- Almost a fifth of U.S. retail terminals are equipped to take cards with security chips embedded in them. But less than 1% of the cards banks issue have the chips.
- Retailers have spent billions - indeed, a disproportionate amount of the costs - of fixing our payments and IT systems.

But again, remember: This is context for telling the story of your breach, not an excuse or justification. It is imperative your company makes that crystal clear. Use background meetings with reporters to make these points again and more fully.

TO SPEAK OR NOT TO SPEAK?

There will, of course, always be a need for caution when working with media about a breach. And there may be some who argue for releasing as little as possible and as slowly as possible, and they may have good reasons.

But remember that reassuring your customers and reestablishing trust is not just the right thing to do; it will also affect the business and minimize the number of disaffected customers and skeptical reporters. It is job number one for the company after fixing the breach.

As big disclosures emerge - the actual impact on customers, for instance, or major improvements in your security - you will want to repeat this press-conference process.

HIRING OUTSIDE HELP

You may want to consider retaining one of the communications companies that specialize in "crisis communications." Companies and institutions often hire these companies when there is major trouble.

If you do, remember that these companies may not know your industry or its reporters very well; they may be expert at formulating winning strategies to get you out of a jam, but you will still need to rely on the expertise of your in-house media staff.

In other words, go ahead and make a crisis plan now in-house. Your consultant may change it in the event of a crisis - you can even have the consultant evaluate the plan before a crisis - but at least you have something to which to compare your consultant's advice.

AFTER THE FIRST PRESS CONFERENCE

Once the story is in the open and developing, it's time to work the reporters. Offer reporters who cover your breach most closely briefings via phone or in-person with your designated IT breach spokesperson or even, if the reporter is important enough, with your CEO.

Some communications people recommend leaking important positive stories to a single important publication to get better play. We generally discourage that because it alienates all the other reporters working hard on the story. A good, informative, breaking story will get play - there's no need to alienate reporters you are going to need later on this and other stories.

So be fair and impartial. Let these briefings be briefings: Background and context to help the reporter understand the story only, not to leak news. (Although all backgrounders should address not just the past - how did we get here? - but more importantly to reporters, where is the story going next? You can help them with this in a general way, and also help them fit your breach into the overall data security problem for context.)

Your media department will be monitoring coverage on digital media, broadcast and the mainstream print press all the time. One way to win over reporters whose coverage is hostile would be to invite them in for a briefing (or, if they're out of town, over the phone.)

Always couch invitations to these briefings as friendly, informal background sessions, not hostile corrective action. This is where your media department's existing relations with reporters will be useful.

And of course remember to use digital media, not just the new breach section you create on the corporate website but also all the other usual tools of corporate communications - Facebook, Twitter and other social and digital media platforms.

SORTING OUT THE COVERAGE

Look for themes in the coverage. If they are negative themes, and persist - such as allegations that the company's security was lax - you can address them through these informal briefings. (Don't feel the need to address every single negative tweet or blog post.)

If the themes are positive, push them harder in your statements and releases. Add them to your talking points, which should be under constant revision as the story develops. Look for reasons to reassure customers their cards are safe to use at your stores.

For a while, a breach is likely to be your company's major focus. In communications, that will be the temptation, too, but don't fixate on it. Be sure to keep up a steady flow of corporate news - don't let reporters perceive you are transfixed by this one story, for they watch the flow of releases closely. On the other hand, avoid at all costs being seen putting out a barrage of hokey "good news" press releases that are mindless and not newsy, lest reporters suspect you of trying to divert their attention. They won't take it kindly.

Yes, for the time being, reporters will always add your breach as background to any corporate story, like a big acquisition or earnings.

For perhaps months or even a year, also expect to see your name, if you are large enough, in trend stories about security breaches. Reporters will always cite some of the biggest ones in putting background in their stories.

There's nothing you can do about that except try and handle the press fallout on such a story adroitly from the start, being as honest and helpful to reporters - and by extension, to your customers - as you can.

WHAT IF YOUR COMPANY IS JUST A BYSTANDER?

It is likely that reporters who cover retail breaches will call your company for comment after a breach - even if your company was not hit - if you are in the same geographic area or industry.

Don't give a "no comment" under normal circumstances. Think of this as an opportunity to reassure your own customers. As recommended earlier for breached companies, cite your certifications and the steps you have taken to secure your data and your customers'.

Obviously don't crow and don't criticize a competitor, even if it's merited.

If you have a breach crisis plan in place, you already have the information and talking points you need to handle a reporter's request for comment about a breach elsewhere. On the other hand, you clearly want to avoid being sucked into a story like this over the long term, so a short statement is probably best.

If continued coverage of another company's breach seems to be making your customers nervous, only then consider contacting reporters for informal briefings or posting more information about your own security measures on your website.

A useful statement after a competitor is breached might go like this:

We sympathize deeply with XYZ Corp. and its customers and hope the security issues can be resolved quickly for everyone's sake.

All retailers face this growing threat from sophisticated cybercriminals. The U.S. needs to beef up its security measures against these hackers.

At ABC Corp., we have complied with the credit card companies' own security certification, known as PCI, as well as the code for our industry. In the last two years we have also strengthened our security by hiring two prestigious consultants to advise us.

IN THE LONG TERM

The breach story in general is clearly not going away as thieves target more U.S. companies. Therefore, if you are breached, you may expect intense coverage for a while and then possibly to be mentioned in trend stories later. But remember: You will be in good company with some of the nation's largest retailers and financial institutions.

That may be small comfort in disclosing a breach, but in the long run, it will work for your company.

Even when the furor from a big breach dies down, you can expect your conference call discussing first quarterly earnings after the breach (if you are a public company) to be largely about the impact of the breach. And while your annual earnings report will be more complicated, it will still likely prominently concern the impact of the breach on the company and customers.

That is why it is import to utilize these opportunities to get your message across: Yes, you got hit; yes, some customers stayed away; but you have benefited from the hard-won knowledge gained during the breach and improved your security systems; you have made your customers whole; and even if your sales haven't recovered, you are optimistic they will soon.

Have the breach communications committee and the entire breach committee inventory the coverage, the impact on the company's reputation and the company's handling of the story every day at first after the breach and then later every few weeks or months until the breach is just a bad memory. Use these

assessments to fine-tune your plan so that you are actively and effectively mitigating the harm to the company's reputation in every way possible at all times.

REPUTATION

Ultimately, over the long haul, this is about your company's reputation. You can ameliorate that by handling the press expertly and reassuring customers, or do serious and lasting damage to your name by mishandling reporters, either by misleading them or being seen to try and manipulate them.

So start thinking the unthinkable now: Plan for a breach as if one is going to occur at some point not too far off. Even if you contract out media to a consultant, you can be rest assured you've thought long and hard about how you want to handle the problem.

Michael Flagg is a former financial reporter and senior editor for the Los Angeles Times, The Washington Post, The Wall Street Journal and Bloomberg, where he supervised 80 reporters and editors in a dozen bureaus over as many time zones and managed the only foreign investigative reporting team in Asia at the time. He has since been a senior vice president at MSL Group, one of the world's largest communications firms, where his clients included Deutsche Bank and the Robert Wood Johnson Foundation; vice president of communications at the prestigious nonprofit Center for Responsible Lending, which battles banks over predatory lending; a senior investigator at the Financial Crisis Inquiry Commission, created by Congress to investigate the financial crash; and communications director of the D.C. Department of Insurance, Securities and Banking; and has worked on breach and swipe fee issues as a consultant for the Merchants Payments Coalition, a group of retail trade associations. He has broad experience in media relations, crafting messages and in crisis communications. He lives in Washington, D.C.