Overview
How a company communicates about a breach is an essential part of breach response. In the age of social media and the 24/7 news cycle, the amount of public scrutiny companies face as they go through a major incident is at an all-time high and can have significant long-term impact on corporate reputation. This interactive discussion will examine how, what and when companies need to communicate about a data breach. We will take attendees through a hypothetical breach scenario examining the proper tactics and messages to deliver throughout the lifecycle of the incident; from discovery through resolution.
Overview of Current Landscape
<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.8%</td>
<td>of U.S. consumers worry about the security of their personal information.</td>
</tr>
<tr>
<td>72.5%</td>
<td>of U.S. consumers don’t believe organizations care about their private data and keeping it safe and secure.</td>
</tr>
<tr>
<td>40%</td>
<td>of global consumers believe failure to keep customer information secure has a significant negative impact on trust in a company.</td>
</tr>
</tbody>
</table>
The Reality of the Data Breach News Landscape Today

• Incidents are often leaked to the press prior to completion of a full investigation
• The pressure from the media to disclose more information quicker is higher than ever before
• Companies often face several waves of news cycles over the course of the breach that must be managed
• Social media is making it possible for information about a breach to spread quickly
Breaking Down a Breach
Overview

• We will walk everyone through the various phases of a typical Payments Breach from a media perspective
• For each phase we will explain:
  1. The “trigger” that prompts a communications action
  2. Key considerations that must be discussed on how to move forward
  3. A sample of what a press statement or other material might look like
Phase 1: Prior to a Breach

The CEO asks if your company has a plan to respond to a breach.
Preparation is Key

- Proactive steps to take:

<table>
<thead>
<tr>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify internal and external crisis team</td>
</tr>
<tr>
<td>Develop communications chain of command for multiple scenarios</td>
</tr>
<tr>
<td>Meet your state’s legislators, regulators and policy makers</td>
</tr>
<tr>
<td>Determine your lobbying, forensics and legal firm before a crisis</td>
</tr>
<tr>
<td>Conduct a mock crisis situation</td>
</tr>
<tr>
<td>Keep the team lean and empower a decision-maker</td>
</tr>
</tbody>
</table>
Phase 2: Learning of the Breach

Trigger: You are alerted from either your IT team or payments brands or processor that there is a breach, but it is not public yet.
Phase 2: Key Considerations

- Based on the limited amount of information are we at the point where we have something to disclose?
- What information do we need to craft a response?
- What can we start preparing now that we will likely need later when we have more information (dedicated page of website, call center QA, media statements etc.)?
- Will this require formal notification under state laws?
Phase 2: Key Actions

• Convene the incident response team to gain situational awareness and discuss approach
• Develop a holding statement to use with press focused on it being under investigation
• Start social and traditional media monitoring for leaks
• Identify the potential avenues for a leak
Phase 3: Breach Gets Leaked

Trigger: Brian Krebs or Robin Sidel/WSJ learns that you have been breached and is going to make it public mid-investigation
Phase 3: Key Considerations

• Do you want to provide a statement?
• What would you disclose (do you give numbers or other details or actions taken)?
• Are you ready to confirm the breach at this point?
• How far along are you in the investigation and can you confirm a breach?
Phase 3: Key Actions

• Provide a holding statement focused on the actions taken as part of the investigation. Including:
  – Who is engaged/you are working with
  – Steps taken and being taken
  – Promise to provide updates
  – DO NOT speculate on numbers affected
  – Continue preparing materials for a larger disclosure WHEN you have more information
Phase 4: Breach Confirmed; Forensics Ongoing

You learn from IT and forensics that there was in fact a breach and have a understand of the potential size and scope. You know the type of information affected, but there is still uncertainty of the scope pending a complete investigation.
Phase 4: Key Considerations

• What do you communicate at this point?
• Do you offer interviews and who would do them?
• Are you sharing with regulators and policymakers at this point?
• How are you getting your message out (press release, website, social media)?
• What are you doing for customers?
  – Do you offer credit monitoring or fraud resolution
  – Call center
Phase 4: Key Actions

- Communicate with the customer as the North Star
- Be careful claiming the issue is fully resolved; be cautious of numbers being communicated
- Focus on steps to protect them versus getting caught up in technical discussion or how to get them back in stores
- Rely on controlled communications channels to keep messaging consistent
  - Create a centralized place on your website for all information that’s made public
  - Set up a call center to answer questions from concerned customers
- Engage regulators and policymakers on what’s known and commitment to update
- Prepare formal notification process (if necessary)
- Prepare for AG and Congressional inquires
Phase 4: Website Example

Customer update on payment breach

On Sept. 8, we confirmed that our payment data systems were breached, which could potentially impact customers who used a payment card at our U.S. and Canadian stores in 2014, from April to September. Today, we are able to tell you that the malware used in the recent breach has been eliminated from our U.S. and Canadian networks.

We also want to know that we have completed a major payment security project that provides enhanced encryption of payment card data at point of sale in our U.S. stores, offering significant new protection for customers. The rollout of enhanced encryption to Canadian stores will be completed by early 2015. Canadian stores are already enabled with EMV "Chip and PIN" technology.

We apologize for the frustration and inconvenience this breach may have caused.

We also want to emphasize that you will not be liable for any fraudulent charges to your accounts, and we’re offering free identity protection services, including credit monitoring, to any customer who has shopped at a Home Depot store in 2014, from April on.

You can learn more about the identity protection services and how to sign up for them at https://homedeapot.flock.com.

It is important to closely monitor your payment card accounts and report unusual activity to your issuing bank.

KEYS TO CUSTOMER PROTECTION

- Self-service tools to help you query, purchase, or manage your payment card accounts and addresses
- Self-service tools to help you query, purchase, or manage your payment card accounts and addresses
- Tools and resources to help you manage your payment card accounts and addresses
- Tools and resources to help you manage your payment card accounts and addresses

Helpful Links

- Payment Card Accounts
- Identity Protection Services
- Self-serve Tools
- Help & Support
Phase 5: Investigation Complete

Forensics issues their final report confirming the extent of the incident. Media coverage has died down, but customers may still be unsettled.
From a business perspective, the goals are clear:

- Protect client relationships through the initial forensics report and subsequent industry dialogue.
- Respond swiftly to client concerns, reinforcing the company commitment to data security and citing improvements already underway.
- Chart an operational course to help inoculate the company from future risk.

Strategies:

- Creating a consistent, credible story about company’s strengths, areas for improvement and commitment to excellence in data security.
- Setting a sustained course to build awareness, comprehension and thought leadership for the company and its executives.
- Maximizing our efforts through an engagement model that crosses multiple channels, drives message penetration across audiences and leverages third parties for credibility, where applicable.
Brand Recovery

• Tactics:
  • Develop a message framework that will and address information security to demonstrate the company’s commitment to setting a new standard for security within the industry
  • Establish relationships with information security industry influencers, including NGOs, media, industry experts, etc.
  • Partner with a group such as the RILA, the Ponemon Institute or many others
  • Leverage existing industry events and their attendees as expanded platforms for the company to demonstrate it’s commitment to information security
  • Create content whether it’s in the form of bylines/op-eds, infographics, Q&A series, videos, etc.
  • Develop an expert positioning document that can be easily shared, identifying individuals as thought leaders to key media
Other Considerations

• Size, scope and brand recognition largely influence media and policymaker attention
• You may never know the complete size/scope of the incident
• Applying a typical crisis model doesn’t work for modern attacks/breaches
Questions