360°

of IT Compliance FOR BUSINESS

COMMUNICATING A BREACH WITH CONFIDENCE

Communicating a Breach with Confidence

Presented by: Linda Varrell, APR
November 5, 2015

When you know that you're capable of dealing with whatever comes, you have the only security the world has to offer. — Harry Browne

2014 is being coined the "Year of the Breach"—with 1541 breaches reported and well over 1 billion records compromised or stolen, according to SafeNet-Inc.com.

What's both encouraging and discouraging is that according to the FBI, Secret Service and other law enforcement, 90% were avoidable.

Today's Session: What do I want to get out of today's session? What is my biggest challenge?

_____
_____
_____
_____

91% of adults "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by companies (according to Pew Internet Research Project released in November 2014), companies still need to make sure they have control over the response and communications around a breach.

It's the NEW NORMAL!

It's about "balancing regulatory requirements with business needs and consumer expectations. Success is moving from a perspective of compliance, the minimum of requirements, to one of stewardship where companies meet the expectations of their customers." – Experian

Are all Breaches a Crisis?

What was different about each of the following breaches?

Heartland Breach

_____
_____

Anthem

_____
_____

Sony

_____
_____

Office of Personnel Management (OPM)

_____
_____

What is the difference between bad news and a crisis?

_____
_____
_____
_____
_____

COMMUNICATION IS KEY

According to Forrester, "Customer facing communication following a breach is a critical component of incident response and the first step in reassuring consumers that your organization is handling the incident appropriately." It is also a key factor in whether a breach simply is bad news or becomes a full-blown crisis.

Having a tested emergency communication or incidence [response] plan in place is vital to being good stewards of the private personal information that your organization is entrusted with and potentially avoiding a crisis.

Do you have an emergency communication plan? ❑ Yes ❑ No

Do you have trained spokespeople? ❑ Yes ❑ No

Do you know what to do if you had to communicate a breach or other incident? ❑ Yes ❑ No

ESTABLISH YOUR INCIDENCE RESPONSE TEAM

It starts with the right team in place that includes both internal and external representations. Who is on your team?

Internal	External

LAW ENFORCEMENT AND INFORMATION SHARING

Just last week the new Cybersecurity Information Sharing Act (CISA) was enacted to allow law enforcement to share information regarding breaches.

According to Security Info Watch, in theory, the information to be shared would be limited to "threat indicators" – data such as technical information about the type of malware used, internet addresses, and origins of the attack, the ways the attackers covered their tracks, etc. Presumably, the government can use this information to stymie further attacks on other companies and the government itself.

The bill requires the federal government and entities monitoring, operating or sharing indicators or defensive measures: (1) to utilize security controls to protect against unauthorized access or acquisitions; and (2) prior to sharing an indicator to remove personal information or identifying a specific person not directly related to a cybersecurity threat.

What it doesn't do according to those opposed to the bill **is require increased attention and vigilance for companies and organizations to upgrade cybersecurity policies.** [Krebs]

Law Enforcement to Consider

- U.S. and State Attorney General
- State Police
- U.S. Secret Service & FBI

KNOW YOUR REPORTING REQUIREMENTS

In the event of a breach, before you can tell anyone, you really need to know what happened and what type of information was involved. Was the data in the form of the following?

- Social Security Numbers
- Financial Account Numbers
- Driver's License or Identification Numbers
- Medical, Health or Insurance
- Other Non-Protected Information (IP, etc.)

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

If a breach happens in my organization:

Who must be notified and when?

_____
_____
_____

How must they be notified?

_____
_____
_____

In what instances do I need to notify the press?

_____
_____
_____

What's different in a breach involving protected health information?

_____
_____
_____
_____

MANAGE CONSUMER EXPECTATIONS

As discussed, 91% of consumers feel that business and organizations have lost control of data that is collected and stored. With that in mind, how you respond to a breach is the most vital aspect of the process.

- Timely and clear notification
- Delivered in a manner appropriate with their needs
- With the highest degree of urgency based on data compromised
- With remediation and credit reporting provided free of charge

What's important to my consumers?

_____

_____

_____

_____

MESSAGING – WHAT EXACTLY HAPPENED AND WHAT DO WE SAY (Follow CA guidelines)

The single most important aspect of messaging is to stick to the facts. No marketing speak, no embellishing or minimizing – clear and transparent is the only way to go. And avoid omitting information (unless you've been advised to do so by law enforcement because it is part of an ongoing investigation) as that may be more harmful than being straightforward.

Omission can also be considered non-compliant with reporting requirements. Remember it's a time for stewardship not for cowering.

- The organization the breach involved (with so many partners the breach may have been a vendor) – communication should come from those closest to the customer
- Description of what happened, how, when, what, etc.
- Be clear on timing – date of breach, estimated date of breach, date range of breach, date of notice, other relevant dates
- Types of personal information subject to the breach
- What law enforcement is involved and if there were delays in notification due to the investigation
- If breach involves SSN or ID (Driver's License) – information on credit bureau reporting agencies and identity theft
- What's being done to protect the individuals whose information was compromised
- Advice on what individuals can do to protect themselves

AUDIENCE IDENTIFICATION

What audiences do I need to consider?

_____

_____

_____

_____

_____

How do I reach them?

TIPS ON WRITING EFFECTIVE BREACH NOTIFICATION (from Online Trust Alliance)

- Take responsibility and apologize for the inconvenience
- Be clear and unassuming – explain in clear language what happened, be honest and transparent
- Write at a 6th grade level (consider vulnerable victims)
- Explain versus scare and provide assistance (phone number and resource)
- Think like an individual not a corporation
- Explain steps the company is taking to make sure it won't happen again
- Apologize again and mean it

MONITORING, EVALUATING AND EVOLVING

Reputation monitoring is how we stay on top of what is being said about an organization that is involved in a breach. Monitoring takes on a whole new level with social media.

What formal process do we have in place for monitoring our reputation and what's said about us online and in the media?

It's not enough however, to simply monitor. With today's interactive media and citizen journalists, there may be cases where an organization needs to respond.

Responding to inquiries will happen both internally and externally. Having all of the tools makes that process easier.

Who monitors our reputation and responds? How can I help?

EVALUATE (Post-Mortem)

As soon as the breach is mitigated and you are in the restoration process, conduct a meeting of your team(s). Review the materials from the breach, feedback from the audiences, message analysis of coverage, questions asked, timelines, incident reports, etc. This is the time to uncover what did and did not go well. Keep the focus on what happened, how it happened and how it was responded to.

BUILDING YOUR PLAN

Decide in Advance:

- Who should be involved
- What roles different people will hold
- How decisions will be made
- Who will speak for the organization (depends on situation and expertise)

Document Today (if not already started)

- Trigger Events
- Policies
- Audiences
- Messages
- Templates
- How the plan will be tested
- How often it will be adjusted
- Who will be trained

It's time to BRACE for a Breach

In general, it's advisable to follow a **B.R.A.C.E.** protocol to respond to crises, incidents and catastrophes. This framework can help communicate the seemingly mundane (technology changes), the panicked (layoffs, security breach, mergers and acquisitions), and the tragic (deaths, inappropriate or unethical conduct).

We all agree, having a tested playbook ahead of time can be a game-changer. Though the very nature of crisis response often implies a lack of forewarning. In any case, it's important to **B.R.A.C.E.** for a breach.

- **B**e the first to tell your story.
- **R**esearch facts & impacts thoroughly
- **A**ssess audiences completely
- **C**ommunicate confidently and consistently
- **E**valuate and evolve

Final Notes:

RESOURCES

Krebs on Security - http://krebsonsecurity.com/

Online Trust Alliance – https://OTAlliance.org/breach

Experian – https://Experian.com/DataBreach

Department of Health & Human Services - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Security InfoWatch - http://www.securityinfowatch.com/article/12132882/the-impact-of-the-senates-passage-of-the-cisa

National Conference of State Legislatures - http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

State of Maine Statutes - http://legislature.maine.gov/statutes/10/title10sec1348.html

State of California Statutes - http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29

Federal Trade Commission - https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule

CHECKLIST FOR HANDLING BREACH COMMUNICATIONS

- ☐ Bring together your team
  - Internal
  - External
- ☐ Ensure contracts are in place with team (in advance)
- ☐ Know your reporting requirements
  - State
  - Federal
  - Regulator
- ☐ Research and document the facts
  - What happened?
  - Who was involved?
  - What systems were affected?
  - What information was compromised?
  - What information was not compromised?
  - Will there be an impact on information compromised?
  - When did you first find out about it?
  - Over what timeframe was information compromised?
  - Is the breach mitigated?
  - What are you doing to ensure it doesn't happen again?
  - How will you be notifying those affected?
  - Where can the public get more information?
  - How will you make those impacted whole?
- ☐ Develop an overarching communication plan
  - Goals
  - Objectives
  - Roles
  - Risks
  - Strategies
  - Tactics
  - Action Plans
  - Budgets
- ☐ Identify all audiences
- ☐ Identify messages (Messaging Document, FAQs, etc.)
- ☐ Identify spokesperson(s)
- ☐ Brainstorm "hard" media questions
- ☐ Conduct media "coaching" or full "training"
- ☐ Identify communication channels and timing
- ☐ Develop deliverables
  - Letter
  - Email
  - Posters
  - Press Release
  - Statement
  - Web Page
  - Social Media Posts
- ☐ Set up monitoring
  - Google Alerts – "As It Happens" settings
  - Social Media listening
- ☐ Respond to feedback
  - Create messaging guidelines and policies for appropriate response
  - Who should respond?
  - What information is ok to share?
  - What is the tone of responses?
  - Where should you respond?
- ☐ Update emergency communication plan