
# Stories from the War Room

## Lessons in Breach Communications

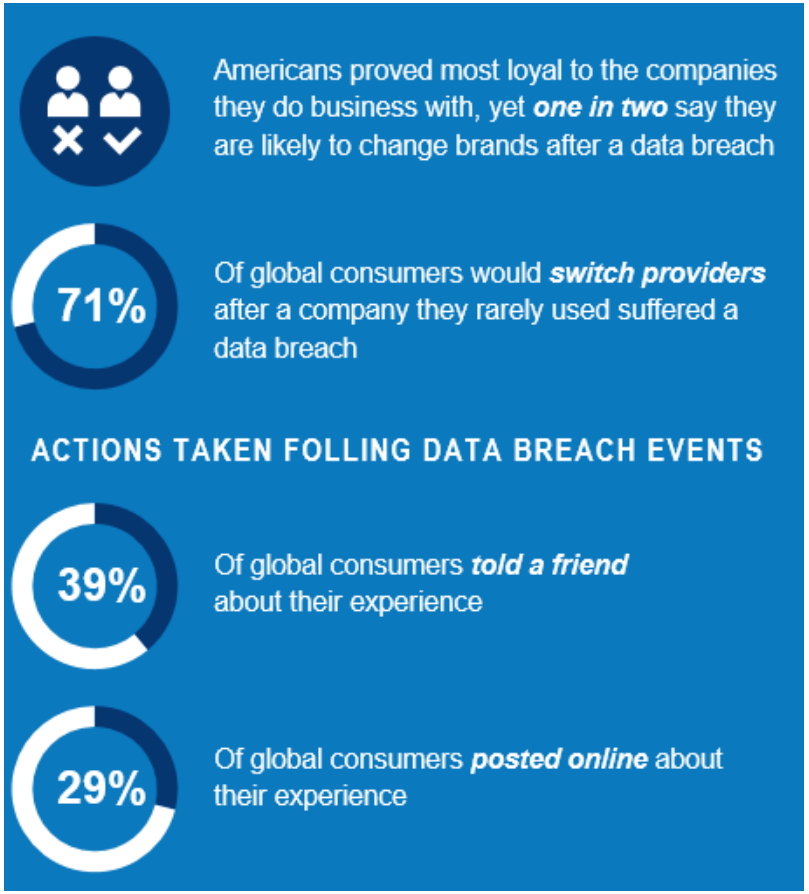

# Today's Operating Realities

- The speed of risk has become 140 characters or less.
- The traditional concepts of containment are no longer possible.
- Facts are negotiable.
- There are no safe havens from digitally empowered agendas and social exposure.
- Data security and privacy has moved from the backroom to the board room.


# Communications Lesson #1: *Playing for Keeps*

EDELMAN'S SECURITY STUDY SHOWS:

- A gap between consumer expectations and what businesses actually deliver
- A relationship between effective data protection and business success
- Data security and privacy considerations impact purchasing decisions




# Communications Lesson #2:
# *Have a Strong Bench*

- Keep the team lean and empower a decision-maker
- Legal, regulatory and communications must work in lockstep
- Integrate legal, IT, PR and business group into communications planning

REUTERS

**Yahoo must face litigation by data breach victims: U.S. judge**

FORTUNE

**Uber To Settle With N.Y. Attorney General Over 'God View' Privacy Breach**


# Communications Lesson #3:
## *Be Ready for Audibles*

- Forensics is critical to messaging and communications strategy
- Prepare for a fluid situation
- “Facts” are very fluid - so rushing public statements can result in a number of bad outcomes for a company

The New York Times

**For Target, The Breach Numbers Grow**

Forbes

**Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming**


# Communications Lesson #4: *Timing is Everything*

- Move quickly …
- …but remember that in a data breach going out with information too early can hurt an organization
- Balance regulatory disclosure requirements with remediating systems and getting the facts right

PUGET SOUND BUSINESS JOURNAL

**Secure your computers, then disclose cyberattack**

PREMERA | BLUE CROSS

An Independent Licensee of the Blue Cross Blue Shield Association

**CEO Jeff Roe explains cyberattack announcement timing**


# Communications Lesson #5:
## *Sometimes Defense is the Best Offense*

- Brand recognition and broader context can sustain the lifecycle of news coverage
- Avoid amplifying the story or inadvertently creating additional news cycles
- Set up the appropriate media/social monitoring and listening posts
- Think through planned content on social media

TechTarget

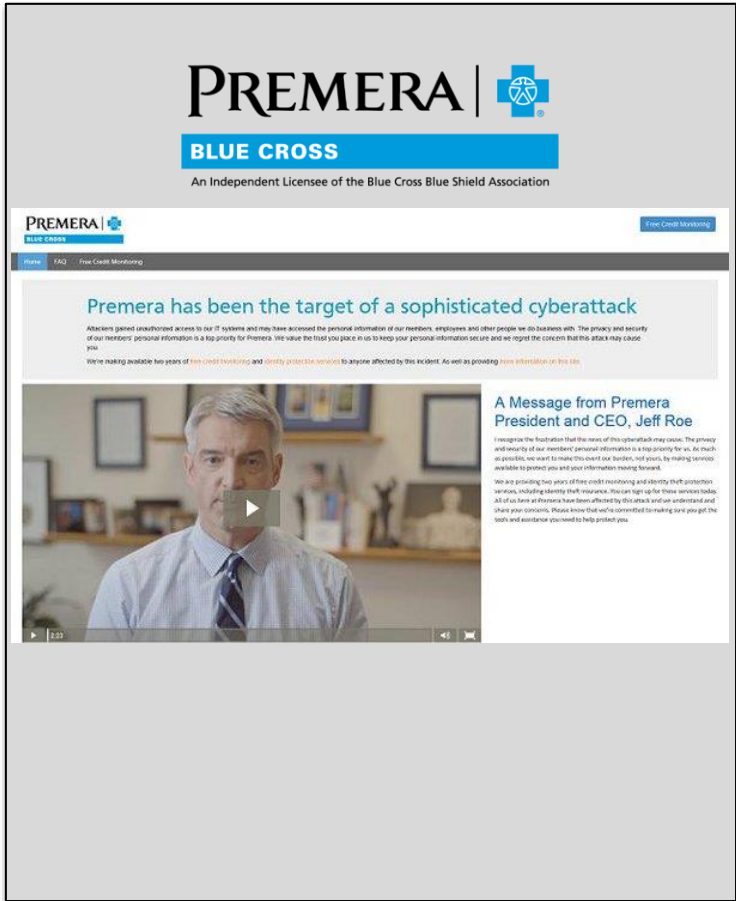
**Risk & Repeat: Second Yahoo data breach uncovered**

SC MEDIA

**Data on 1B Yahoo users stolen in second breach**

# Communications Lesson #6: *See the Whole Field*

- Customers must be your north star
- Don’t neglect other critical external stakeholders, including policymakers, regulators (state and federal) and industry stakeholders (e.g., payment brands)
- Employees are your most credible spokespersons – keep them informed




# Communications Lesson #7:
## *Avoid Unsportsmanlike Conduct Penalties*

- Show humility
- Communicate support for impacted individuals
- Focus on steps taken to prevent similar incidents to regain trust
- Demonstrate a bias toward action

**FORTUNE**

**How Home Depot CEO Frank Blake kept his legacy from being hacked**

**THE WALL STREET JOURNAL.**

**"If we rewind the tape, our security systems could have been better. Data security just wasn't high enough in our mission statement."**
***– former CEO Frank Blake***


# Communications Lesson #8:
# *Practice and Train Before the Big Game*

### ANALYZE & ASSESS RISK
Assess any current crisis plans and protocols as well as the company's current privacy and security protocols; identify gaps and areas of opportunity

### BUILD INCIDENT RESPONSE PLAN
Create a purpose-built crisis preparedness plan that identifies team roles and responsibilities, explores key response scenarios and includes sample messaging along with forms and checklists to ensure rapid response capability

### TEST THE PROCESS
Pressure test the plan and team through simulating a priority risk scenario, such as a data breach; identify gaps and areas for improvement

### OPERATE AND MANAGE
Activate 24/7 crisis response as needed

***"An ounce of preparation is worth a pound of cure"***

The average data breach in the United States costs an organization more than $6.5 million in investigations, customer notification, lost business and reputation management.

Organizations with an "incident response plan" at the time of their breaches saw an average cost that was $42 per record less than the national average per compromised record.

Ponemon INSTITUTE


# Communications Lesson #9:
# *Play the Long Game*

- Create a consistent, credible story about company's strengths, areas for improvement and commitment to excellence in data security

- Set a sustained course to build awareness, comprehension and thought leadership for the company and its executives

- Maximize efforts through an engagement model that crosses multiple channels, drives message penetration across audiences and leverages third parties for credibility, where applicable


# Communications Lesson #10:
## *Game Plan in Advance*

**NO** organization is immune to a cyber attack or data breach

**NO** amount of technology can account for human error or deception

**DON'T WAIT** for a breach to occur

**BE PROACTIVE...** create a plan, practice and develop muscle memory