Cyber Solace
BUSINESS TECHNOLOGY RISK ADVISORY

Crisis Communications During a Cyber Incident

©COPYRIGHT 2025 | CYBERSOLACE LIMITED

Contents

1. Crisis Communications During a Cyber Incident
2. Why Crisis Communications Matter
3. Preparation Equals Protection
4. Immediate Activation—First 24 Hours
5. Speak Early, Even With Limited Facts
6. Own The Narrative: Embrace Transparency
7. Internal Briefing Before Public Messaging
8. Consistent Messaging Across Channels
9. Prioritizing Affected Parties in Communications
10. Handling Insider Events Differently
11. The SPEAK Method for Crisis Messaging
12. Post-Crisis: Brand Rebuilding Through Communication

Crisis Communications During a Cyber Incident

This is a brief business guide for organizations aiming to become cyber-resilient in the face of a cyber incident. Effective crisis communications are essential not only for mitigating damage but also for maintaining stakeholder trust throughout and beyond a security breach. As organizations face increasing threats, knowing how to communicate and respond when an incident occurs is a strategic imperative, relevant to leadership, communications, IT, legal, and HR teams alike.



Why Crisis Communications Matter

1

Trust Is Easily Lost

According to Experian's 2024–2025 Data Breach Response Guide, 66% of consumers lose trust in an organization after a data breach, highlighting the immediate and lasting nature of reputational damage.

2

Customers Demand Security

Post-breach, customers frequently attribute the incident to poor security practices, making effective communication essential to win back trust.

3

Strategic, Not Supplemental

Crisis communications are not simply a support function but a pivotal strategic discipline that shapes public perception and long-term business outcomes.

Preparation Equals Protection



Integrate Communications Into Response Plans

Organizations should include a dedicated communications annex within their incident response plans to ensure crisis comms are not overlooked in the heat of the moment.



Establish Roles and Templates

Predefine roles, create message templates, and set clear approval chains to enable a rapid, coordinated response when incidents occur.



Cross-Functional Alignment Is Critical

Legal, HR, IT, and Executive teams must be aligned ahead of time to streamline communication and mitigate internal bottlenecks.

Immediate Activation—First 24 Hours

1 **Confirm Facts Rapidly**

Quickly verifying the facts of the incident is crucial to prevent misinformation and guide messaging.

2 **Assemble Crisis Comms Team**

Identify and unify the crisis communications team without delay to ensure an organized approach.

3 **Alert Stakeholders**

Notify leadership and stakeholders as soon as possible to keep them informed and prepared for public messaging.

4 **Draft Holding Statements**

Prepare initial public statements—even if all details aren't known—to prevent a vacuum that misinformation can fill.

Speak Early, Even With Limited Facts

1

Acknowledge Awareness

Promptly confirm that the incident is recognized and being addressed in public communications.

2

Outline Response Steps

Share what steps are being taken to contain the incident, reassuring stakeholders with concrete actions.

3

Leadership Tone Is Vital

Focus on the tone and confidence of leadership over excessive technical detail, especially during early communications.

Own The Narrative: Embrace Transparency

Be Clear and Honest

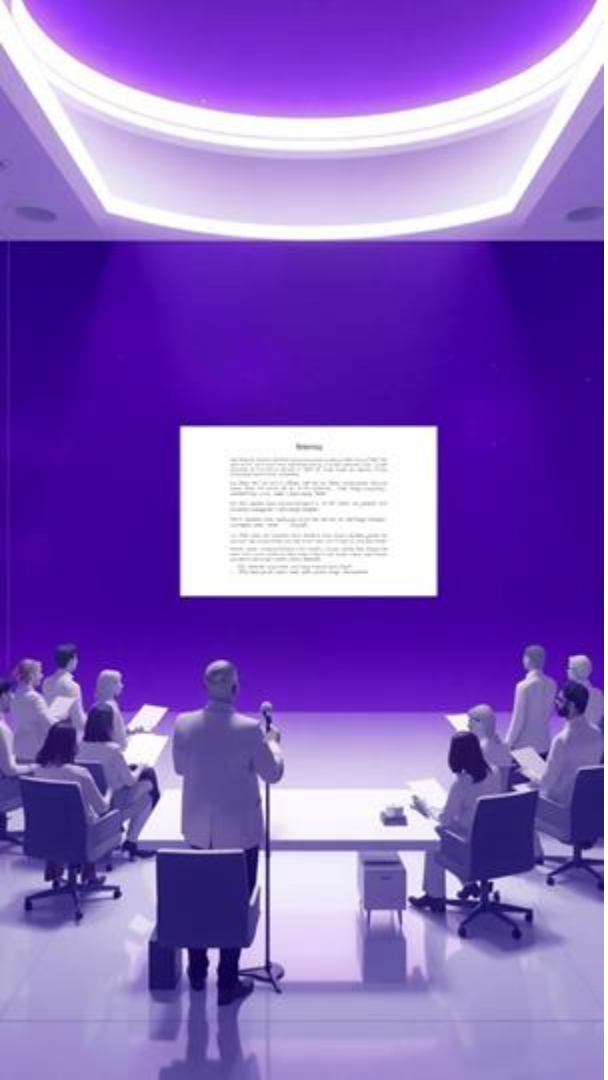
Directly acknowledge the breach and offer transparent updates, even about unknowns, to build credibility.

Set Update Expectations

Establish a clear cadence for future updates so all audiences know when and where to expect further information.

Trust Built Under Scrutiny

Managing trust during crisis scrutiny is far more effective than attempting to rebuild it afterwards.



Internal Briefing Before Public Messaging

Inform All Staff First

Send clear internal memos to employees, ensuring they are informed and prepared before external communications begin.

Share FAQs and Talking Points

Equip staff with FAQs and talking points to minimize internal confusion and prevent accidental information leaks.

Identify Spokespeople

Designate and brief official spokespeople to maintain message discipline and consistent external communication.

Consistent Messaging Across Channels

Align Internal and External Messaging
Messages delivered internally should be consistent with those shared externally to avoid contradictions that can erode trust.

Centralize Content Approval
All statements should be reviewed and approved by a central authority to ensure coordinated, accurate messaging.

Media Training Is Essential
Media-train spokespeople so they confidently handle tough questions and high-pressure situations.



Prioritizing Affected Parties in Communications

1. **Start With Customers and Affected Individuals**
   Those directly impacted by an incident should be notified first and with sensitivity to their needs and concerns.

2. **Next: Employees and Regulators**
   Employees and regulators follow as secondary recipients, all before engaging with the public media.

3. **Pre-Draft Message Templates**
   Having pre-approved, audience-specific templates ensures timely and appropriately toned outreach.

Handling Insider Events Differently

Avoid Blame-First Narratives

Focus communications on facts and ethics rather than rushing to assign blame, promoting an environment of learning and improvement.

Preserve Trust Internally and Externally

Balance transparency to protect the organization's brand while also safeguarding employee trust during internal crises.





The SPEAK Method for Crisis Messaging

Use The SPEAK Concept

Speed

Respond quickly to maintain control and accuracy.

Position

Assert authority to build trust.

Empathy

Connect with emotions to gain understanding.

Admit

Acknowledge mistakes to build credibility.

Kosher

Be authentic to foster genuine connections.

Monitor Media Sentiments Live

Continuous monitoring of social and news media provides real-time feedback and allows rapid adjustments to messaging strategy.

Post-Crisis: Brand Rebuilding Through Communication

Share Lessons Learned
Communicate openly about what went wrong, steps taken to correct course, and transparent changes implemented post-incident.

Demonstrate Investments in Security
Showcase tangible actions and investments made to strengthen future data protection, increasing stakeholder confidence.

Reaffirm Mission and Values
Use the recovery phase to reinforce the organization's core mission, vision, and commitment to trustworthiness.

THANK YOU

www.cybersolace.co.uk