oak engage

Crisis comms best practices: How to create a crisis comms plan

Contents

How an organisation manages a crisis is crucial to its reputation. The CIPR defines crisis management as “having a plan in place that can be effectively actioned when something goes wrong for an organisation.” Although you cannot predict when a crisis will break, the key to effective crisis management is having a crisis communications procedure in place so that you are prepared when one does arise. It is essential that you ‘prepare for the worst’ when it comes to dealing with a crisis.

The crisis could go either way and if dealt with in time, could disappear. That’s why we’ve included best practices and everything you need to create your very own crisis communications procedure for your organisation.

Types of crises

Each crisis is unique but there are a number of possible scenarios that can be defined as a potential trigger point for your organisation. Here are some examples of the types of crises and some real life examples:

Product failure or recall

In 2016, Samsung had to initiate a recall of 2.5 million Galaxy Note 7 handsets due to faulty batteries that overheated and exploded. This was a disaster of unprecedented proportions that ended up costing them £4 billion in losses and lost sales. Samsung tried to contain the situation, stating that the faulty batteries came from one factory and they had shifted production to another supplier.

They warned customers who owned the devices to switch off their handset and began shipping replacement devices to retailers so they could replace the affected models for safe phones. However, the crisis went from bad to worse, when the replacement phones began exploding. The way Samsung handled the crisis was less than admirable.

People swarmed to social media labelling the Samsung device 'Death Note' and shared pictures and videos of their phones exploding and catching fire.

Misinformation spreads quickly and there were rumours of other Samsung devices exploding. Samsung's approach was not urgent enough, highlighting their poor crisis management plan, or lack thereof. They were slow to respond which had a detrimental effect on their reputation. Practitioners need to be able to track what is being said and respond immediately.

Data breach

One of the most catastrophic data breaches of recent times occurred in 2017 when credit advisors Equifax were hacked. 148 million records that included social security numbers, addresses and credit card information were compromised due to several security vulnerabilities in their system. These breaches went undetected from May 2017 to July 2017.

The thought of any type of customer identity or monetary theft is enough to send any internal comms or marketing professional into a state of fright, never mind on this scale. Equifax's response came under intense scrutiny. Not only did it take until that September to report the breach, they were criticised for poor planning and execution of messages that only served to heighten distrust in the organisation.

Technology magazine, Wired stated:

> "The company's official Twitter account has mistakenly tweeted a phishing link four times, instead of the company's actual breach response page."

Equifax's crisis mitigation strategy did not serve to mitigate at all, instead shelling out $700 million in compensation.

A swift, but well-intentioned comms strategy that aligned with the messaging that they had learned from their mistakes, may have brought some good-will. Instead, it was haphazard and cost them dearly.

Failure in technology

In May 2017, an IT system outage cost British Airways over $80 million and ground operations to a halt for nearly a week. Perhaps even more damaging was the impact on reputation both internally and externally, with thousands of flights cancelled, leaving passengers stranded and crew members unaware of where they needed to be.

Whilst BA took to social media to apologise, it is reported that employees were not well informed and could not assist affected customers. Aviation Consultant, John Strickland said about the crisis: "If your manpower is not up to proper planned establishment then you're really floundering even more."

The annoyance this caused demonstrated the need to equip employees with real-time, accurate information in order to deal with customers and keep them informed during a crisis.

Furthermore, despite a BA spokesperson saying they were "undertaking an exhaustive investigation to ensure that this can never happen again", a similar system breakdown in August 2019 caused more flight cancellations and further comparisons with the crisis two years prior. Ensure that your messaging is backed up by actions in order to rebuild and maintain trust often lost in a crisis.

Financial crisis

Online furniture retailer Made.com had to stop taking orders and was plunged into administration in November 2022 as a result of supply-chain problems and soaring costs.

When dealing with the news that Made's leadership ultimately mitigated responsibility by blaming factors outside their control, Made.com's Chief Executive, Nicola Thompson said:

> "Made is a much loved brand that was highly successful and well adapted, over many years, to a world of low inflation, stable consumer demand, reliable and cost efficient global supply chains and limited geo-political volatility. That world vanished."

Despite retailer Next agreeing to purchase product and naming rights, Made.com were criticised deeply over their communication with staff about redundancies, resulting in many outgoing employees threatening legal action. 573 staff were made redundant over Zoom and many pursued compensation for the employer's failure of duty. By law, they did not follow the proper consultation process for making staff redundant.

Comms in a significant financial crisis, particularly if legal considerations are needed, must be well planned and executed in accordance to any relevant policy or legislation, or risk even further damage to the organisation.

Our blog on Priorities for Internal Comms outlines how you can manage fallout from a comms crisis.

Characteristics of a comms crisis

PWC reports that **69% of business leaders have experienced a crisis over a period of five years.** They're nothing new, but how do you define a communications crisis? A crisis situation has distinct characteristics and can be further defined as follows:

- is unexpected
- has elements of the unknown and escalating intensity
- interrupts normal business operations
- impacts your organisation's external reputation
- impacts your organisation's financial performance
- impacts customers

There are a number of early warning signs that may hit your organisation. Having a crisis communication plan establishes a structure and procedure to be followed once any of the following early warning signs are observed:

- contact from the media
- customer complaints
- notification of a legal issue
- contact from a customer or third party supplier
- publication or broadcast of a negative news report
- increased internet and social media discussions

Defining the crisis

A systematic approach should be used to help determine the best actions to ensure that negative consequences are proactively managed. You should consider the following questions:

Timing

- How urgent is the crisis/event?
- Is a deadline for communications externally and internally agreed?
- What will happen if nothing is communicated?

Trend

- Will the problem get worse?
- Does the crisis/event have the potential for growth?

Impact

- How serious is the problem?
- What are the effects on people, products, reputation, organisation, etc.?

Process

- What are the PAST reasons/events or who was at fault?
- How do you correct the PRESENT issue or situation?
- How do you prevent future issues or situations?

Agreeing the response

The JOTW Communications Survey found that **55% of business communicators do not have a documented crisis communication plan.**

A well-planned, structured response is essential to getting it right. Once you have evaluated the situation, you need to determine the appropriate action and a written or verbal statement or response will be needed.

The agreed response may need to be approved by key stakeholders, depending on the severity or risk level of the crisis.

After the response has been approved, key audiences will need to be communicated with honestly and openly, and in a timely fashion. An omni-channel strategy should be prepared to ensure all audiences are communicated to.

💡 The message map should cover the following:

- Stakeholders: who the message is going to
- Question or concern: the issue to address and focus on
- Key messages (1-3): 3 key concise messages, brief (9 seconds), and clear (27 words) written in plain English for increased audience understanding
- Supporting information (1-3): amplifies the key messages by providing additional facts or details. Supporting information can also take the form of visuals, analogies, personal stories or citations of credible information sources

Key questions to consider when mapping responses:

1. What happened?

2. Who is in charge?

3. Has the issue been contained?

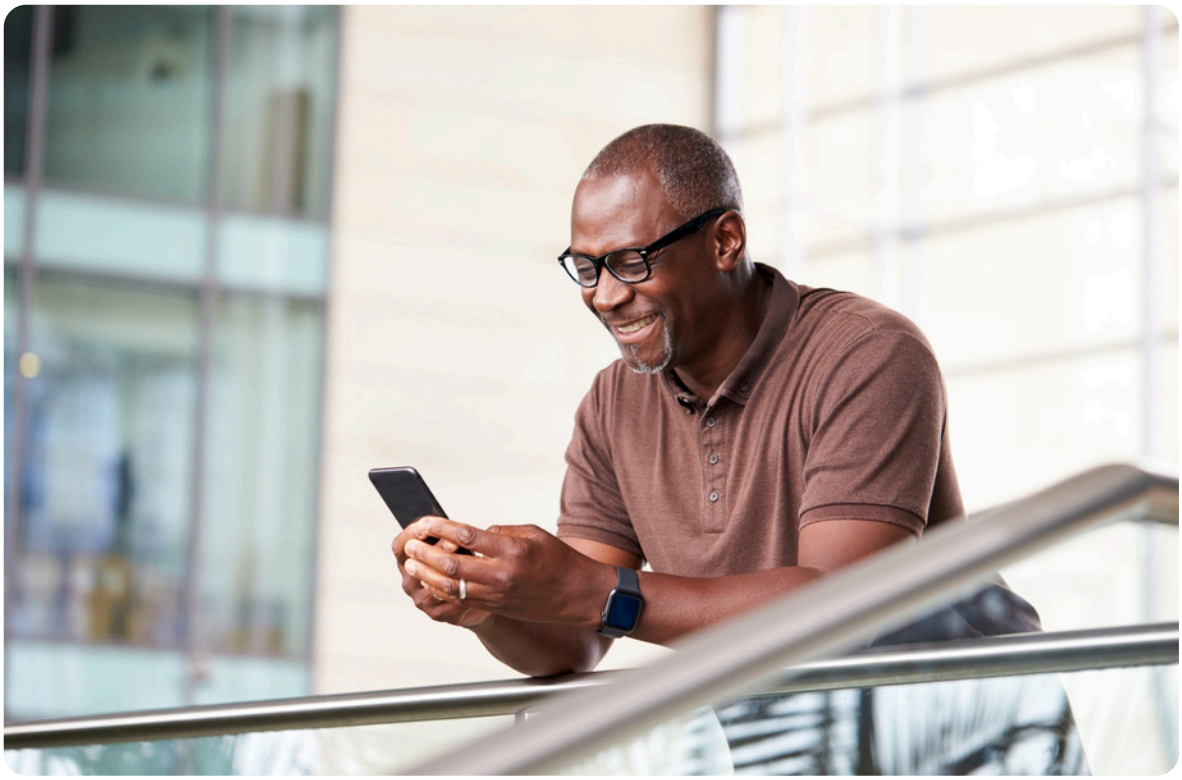
4. Are customers being helped/how?

5. What can we expect?

6. What should customers do?

7. Why/how did this happen?

8. Did you have forewarning?



The following "Four Rs" of crisis communications should also be considered, but may not be applicable in every situation:

Regret	The first thing you should do is express concern that a problem has developed - even if it was not your organisation's fault.
Responsibility	Whether the cause of the problem was your organisation's fault or not, your organisation should be prepared to take responsibility for solving the problem. Your actions will reinforce words and provide a credible demonstration of your organisation's commitment to doing the right thing.
Reform	Your various stakeholder audiences must know you are taking steps to ensure the problem will not happen again.
Restitution	If appropriate, detail how you will help those who have been affected by the problem.

A five-step model for preparing messages

Answers should:	By:
1. Express empathy, listening, caring or compassion as a first statement	• Using personal pronouns, such as “I” “we” “our” or “us” • Indicating through actions, body language and words that you share the concerns of those affected by events • Acknowledging the legitimacy of fear and emotion • Using story-telling, if appropriate and bridging to the key messages
2. State the key messages	• Limiting the total number of words to no more than 27 (sound bite standard) • Limiting the total length to no more than 9 seconds • Using positive, constructive and solution-oriented words as appropriate • Setting messages apart with introductory words, pauses and inflections
3. State supporting information	• Using three additional facts • Using well thought out and tested visual material, including graphics, maps, pictures, video clips, animation, photographs and analogies • Using story-telling • Citing credible third parties or other credible sources of information

4. Repeat the key messages	• Summarising or emphasising the key messages
5. State future actions	• Listing specific next steps; and providing contact information for obtaining additional information, if appropriate

Stakeholder/audience evaluation

A Deloitte study found that 28% of businesses that have been through a crisis would communicate more effectively if they were to go through one again.

This suggests that each audience group requires careful thought. Consider which key audiences or stakeholders need to be targeted. Prepare a comprehensive stakeholder map. Revisit the list of potential stakeholders as the crisis evolves to reflect changes in audiences as needed. Develop a quick view contact list.

Response channels/media

Normally, you would need to consider the most appropriate channels for contacting key audiences, appropriate to the crisis event. However, using Oak Engage's curated content system means you can spend less time worrying about how your internal audiences will receive the message and can focus more time and effort on making sure the content you send is compelling and actionable. It enables you to cut through the noise and get the right message to the right people at the right time and that everyone is kept informed in the best possible way for them.

You also need to determine possible "starting questions" that can be utilised to help quickly determine any misinformation that might be circulating within your organisation and allow for targeted responses, such as:

- What do they need to know about the source of the problem?
- How is the company resolving the situation?
- What are our people expected to do regarding the situation?

A key risk that needs to be considered with crisis communications is an internal leak and the risk that staff may share information externally that your organisation may not want to share. Here are some controls that you can put in place to mitigate this risk:

- Comprehensive internal communications that promote two-way communication with your staff and help share with them what information is available externally
- Training of frontline staff will be important to help them understand how to deal with media enquiries
- Q&A should be prepared and made available for all staff (especially frontline staff)

Another risk is that the crisis becomes a viral or trending conversation on social media or that the crisis news becomes top on search listings. 56.8% of the global population use social media and Ofcom claim that half of all adults in the UK use it as a news source. Make sure you work closely with your organisation's PR team to make sure these controls are in place:

- Awareness of social media conversations is key. Social media will need to be closely monitored by your organisation to ensure that you are protecting your organisation's reputation as much as possible. Use custom queries to monitor this along with sentiment analysis.
- Standard responses should be developed to use in the case of a crisis, and a recommendation to point people to one location to get all available information would help mitigate online conversations that we may not be able to control

Crisis comms and social media

Social media itself has become a hotbed for 'cancel culture' in recent years. One slightly 'off' message, or something interpreted in a different way than anticipated, could lead to a comms crisis.

Cancel culture can affect brands as well as individual celebrities or influencers. It can be triggered by a single post and could result in boycott or protest, neither of which are helpful for brand reputation. Cancelling has become especially prevalent in the area of social and cultural movements, where a tokenistic approach to supporting such causes can have a knock-on effect, particularly when 'activism' contradicts the actual business practices of an organisation.

An example of this is greenwashing from global brands who claim various environmental initiatives with no concrete proof. Consider H&M's green 'conscious' labels where most claims held no evidence of being environmentally conscious, or in Barclays' case, promoting investment in renewables while equally funding large investments into fossil fuels.

Something as simple as an ill-advised social media post could have the potential to affect someone's career, especially those in the public eye. Even if a post is deleted, someone may have screenshotted or saved it before it was removed.

Communicating with your people

Usually when some kind of comms crisis surfaces on social media, it can escalate quickly. As such, your employees may be aware of it before you can communicate about it. There remains a definite need to acknowledge the issue, no matter how public it is at that point, and reinforce how your colleagues should behave online, such as abstaining from commenting or engaging with related content.

You can preemptively make staff aware of the protocol for general social media use with training, depending on the size and type of your organisation. You can also include information around a crisis comms procedure by storing it on your company intranet, that they can access at any time. Your PR team should have a reporting process that will alert them to any defamatory or negative mentions of the company across digital and social media platforms. It may be useful getting them to share that with you, so you can be aware and communicate with your people if needed.

Preparing your people to communicate externally

Careful briefing of communications teams, public-facing staff, brand partners and senior leaders who are active in the digital space, is paramount. Doing so will provide clarity on the extent to which there is a stance on social, political, economical and environmental issues, and this should be communicated proactively and often, not just reactively when crises arise.

Training staff on the impact that words can have and the nuances in how things can be misinterpreted online will ensure that everyone is on the same page. Giving individuals the awareness and opportunity to question such things internally is encouraged.

Often by having these discussions, the reason for a specific approach becomes more clear, and any concerns can be ironed out before messages are shared with the wider public. Work with your marketing or social media colleagues to ensure that relevant training has been given to your employees. An extra layer of protection could be to ask that posts on specific subjects are vetted by your social media teams before being posted, and this can be worked into your policies then communicated on your intranet.

If something does come to light in a digital space, whether it is a corporate comms faux pas, something an individual has shared or something that has been identified and shared online by a member of the public, there must be a strategy in place to address, rectify and overcome.

A transparent approach to setting the record straight is preferred. Trying to sweep an issue under the carpet or pretend it never happened will most likely have its own repercussions. Taking ownership, offering a legitimate apology or explanation and working to rebuild that trust in the digital space is the best approach. Refer back to the four R's - Regret, Responsibility, Reform, Restitution - to help you craft your response.

The threat of deepfakes

A modern-day threat that requires accurate crisis comms planning is the use of deepfakes. Taking an individual's likeness, and then manipulating it with AI to sound and look like the person is saying certain things can be utilised to:

- Imitate senior leaders for intelligent cybercriminal activity
- Imitate existing employees to gain trust before scamming colleagues
- Phishing through voicemails and video
- Bypass security with voice recognition to facilitate fraud

From audio to video, deepfakes can take a variety of formats, and when done well can unfortunately be extremely convincing. Often, these people can do a lot even with limited access to existing video footage or voice clips.

These attacks could come from disgruntled employees, malicious competitors, or even members of the public who might not realise the detrimental impact their actions could have on the targeted individuals' reputations.

Social media platforms may not be quick to identify or respond to flagging of inappropriate content. As such, responsibility tends to lie with the victim organisation or individuals to initiate the correct narrative for damage control.

Nowadays, many of us are familiar with and well-trained in identifying phishing scams via email or text message, with robust internal reporting processes to avoid scams or data theft. The difficulty with deepfakes is the extent to which the target's appearance and voice can be replicated; there is much more to be aware of than bad spelling, grammar and unusual email addresses.

Your response

In the age where a single viral post on social media can build or shatter a reputation in an instant, time is of the essence. Detecting sophisticated manipulations is not always obvious. As such, proactive preparation of a carefully crafted response or an approved template to follow, is crucial. When such content spreads on social media, urgency in issuing a succinct press release shared on verified owned social media channels is key to damage limitation.

Informing your staff of the issue and how it is being dealt with is also paramount, especially if their is a knock-on effect to how they do their jobs. When preparing your external response template, you should also create an internal alert notification to accompany it.

When customer data, employee data or a significant risk to business operations is identified, your employees should be informed first. This enables them to know what to say if customers reach out, but equally lets them know that steps are being taken to protect their data and jobs. Pre-approved templates for both internal and external comms should be checked by a legal or compliance team where possible.

Educating your people

Prevention is the best course of action. While some super-sophisticated scams may be too hard to identify, some steps can be taken to ensure your people are empowered with the information required to identify deepfakes.

Educating your people on validating information, taking the same types of precautions they would take with suspicious emails, and creating a clear reporting process for suspicious activity with a designated contact to fact-check, can all contribute toward reducing the impact of deepfaked cybercriminal activity.

Mitigating the risk of deepfake scams and cybercrime

At present, regulation and legalities around deepfakes remain a rather light-touch approach and therefore the act of creating a deepfake in itself is not punishable, unless in an intimate context under the UK Online Safety Act.

In other contexts, with little application in the legal system, companies must take preventative measures into their own hands.

- Empower your employees and brand partners to spot unusual activity
- Educate your staff and stakeholders on the risks of deepfakes and encourage them to question communications that seem suspicious, even when they appear to come from management
- Provide e-learning or company-wide training on cyber security best practices, and revisit it regularly
- Strengthen verification and authentication tools when there is a risk of someone's data being compromised for fraudulent purposes
- Prepare statements and press release templates to ensure that if something does happen, it can be acted on quickly

We hope the above helps you create your very own crisis communications strategy in your organisation. Utilising channels such as an employee intranet and employee engagement platform will allow you to communicate with your people more effectively. In times of uncertainty, clear and timely communication is the cornerstone of maintaining trust and stability within your team.

At Oak Engage, we understand the significance of staying connected, especially in challenging times. Leveraging the right tools and strategies ensures that your messages reach the right people at the right time, reducing potential misunderstandings and panic.

Remember, in the face of a crisis, preparedness and efficient communication can make all the difference. Stay connected, stay informed, and always prioritise the wellbeing of your team.

Recommended reading

Internal storytelling: A guide for internal comms [with video guides]

Internal audiences: how to create them for IC (free audience persona template)

Top 3 Priorities for Internal Comms Professionals & How an Intranet Can Help Top

10 Comms Books That Will Help Nail your Internal Communications Strategy

oakengage

If you would like to learn more about how to use our platform to support your crisis comms and wider internal comms strategy, arrange a demo with our experts

Book a demo