



Incident Response Communications

IN PARTNERSHIP WITH



Clark
tech



Incident Response Communications

When an unexpected incident happens, implementing a fast and co-ordinated response is vital in reducing potential reputational damage and minimise lost income. To do so successfully, there are three stages you need to consider: before, during and after the incident occurs.

Below are outlined the core questions you need to address when planning and dealing with a crisis. A more detailed approach for handling your crisis communications can be found in the [Reputation Management Framework](#).

Before an incident occurs

The first (and most important) step of dealing with an incident is planning for it before it even occurs. Taking time to consider what people and processes you need to have in place can help make your incident response more successful and mitigate reputational damage. When the incident hits there are going to be a lot of questions, the biggest of which will be: Who? What? How? Having answers to these questions is a must.

Who: Who do you need in your response team, and who are they communicating to? Having a small core cross-departmental team is likely the best option. Ensure this group is clear on their roles and responsibilities and where possible test the efficiency of the team using a specific scenario on an annual basis. This will confirm whether your processes work and if the right people are in place to respond accurately and quickly.

What: What are the immediate actions you will need to take? When responding to an incident, especially to have any hope of getting ahead of it, several actions need to happen almost simultaneously. A crisis response plan should be created which includes pre-drafted statements and information, as well as contact details for key contacts like board members, shareholders or known media to help those responsible activate an immediate response. Include social media access passwords too. This should be available in hard copy or independent to your network to mitigate any IT failures/access issues.

How: How are you going to continue communicating? If your critical infrastructure is taken offline, then ensuring key staff know how to communicate with each other and externally is crucial. Consider that you may not have access to email or virtual meetings. If possible, opt for a physical response centre at the office or conference calls on mobile phone and set up an encrypted messaging channel (e.g. WhatsApp) to quickly disseminate information.

During an incident

In the eye of the storm, things can move very quickly. Having your core response team dealing with all incoming and outgoing information will help to coordinate activity, but there are some other things to consider.

The CEO must be front and centre: To generate a sense of control, and leadership throughout the period of uncertainty and concern a senior spokesperson is essential. Being accessible to staff, stakeholders, and media contacts allows you to prevent accusations of 'avoiding the problem'. Ensure that your CEO is comfortable with this and has attended regular media training sessions to ensure they are clear on how to communicate to various audiences, including the media.

Information is your shield during a crisis:

Be armed with prepared briefings on data structures, encryption levels and organisational details which could support you, especially through the first 48 hours – essentially, make sure you have the access to the information that you may be questioned about; or at the very least know who to call on for this information. As part of planning, your response document should include the copy for webpages such as an FAQ or confirmation of hotlines for customers or stakeholders to call in case of emergency. These can also be published as dark pages on your website which are only updated and made live when needed.

Act quickly: Time is of the essence when it comes to incident response. Bring your team together, activate your plan and inform key stakeholders, customers and the media (where relevant) quickly. This will demonstrate to external parties that the organisation is on top of the issue and is proactively working to resolve it.

Accept responsibility and avoid blaming others: If data loss occurs, you will be expected to shoulder some of the responsibility (even if through a ransomware attack). Clear and honest communication is central to limiting fall out from the incident or contributing to rebuilding the reputation of the company – particularly with customers if they have been impacted directly by the cyber incident.



After an incident

No leader would wish a crisis on their business, but it does present an opportunity for learning and can help to improve your crisis response. While many may overlook this stage, its value cannot be more underlined; this phase brings you full circle, by considering what went well, what didn't, and what needs to change for next time.

- **Timing:** what information was shared, when and to whom (internally and externally)?
- **Tone of voice:** how did your organisation come across?
- **Spokespeople:** did the team work well together? What training do team members need for taking on this role in future?
- **Processes:** any gaps or misunderstandings?
- **Employee engagement:** were staff supported throughout and reassured where possible?
- **Customers and clients:** did they feel reassured, protected?

Five key things to improve your incident response:

- Prepare and share a hard copy of key information pack and content.
- Choose your core response team then delegate the roles and responsibilities.
- Hold annual incident response training sessions.
- Have a backup communications channel e.g., phone numbers, intranet, social media.
- Draft a FAQ page for your answering likely questions you will face.

This document was produced with support by Clark.Tech. For more information on reputation management during an incident response then please contact Kirsten Paul at Clark.Tech on:

kirsten@clarkcommunications.co.uk

or **07814 487 663**

This document references guidance from Richard Knight and Jason R.C. Nurse, "Effective Communications and Public Relations after a Cyber Security Incident" available from <https://doi.org/10.1016/j.cose.2020.102036> and <https://jasonnurse.github.io/comms.pdf>




IN PARTNERSHIP WITH



Clark.
tech



 Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

 01786 447 441

 enquiries@cyberfraudcentre.com

 www.cyberfraudcentre.com

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27