National Cyber Security Centre
a part of GCHQ

Guidance on effective communications in a cyber incident

Context to this guidance

Cyber security incidents affect UK organisations every week, so it's important to be prepared for them.

During an incident, organisations often prioritise their technical response and relegate communication to a secondary consideration. But effective communication to staff, stakeholders, customers and the media is **crucial** for shaping how an organisation is perceived.

Who is it for?

This guidance supports organisations of all sizes to manage their communications strategy before, during and after a cyber security incident.

Even if your organisation doesn't have a specialist communications team, this guidance will still be useful to help you prepare a strategy to put in place if an incident happens.

The principles

The guidance outlines three core principles to follow:

1. **Prepare your communications strategy in advance**
2. **Communicate clearly with different parties, and tailor your messaging where necessary**
3. **Manage the aftermath in the medium and long term**

1. Prepare your communications strategy in advance

Although you can't predict the timing and nature of a cyber incident, effective preparation will help your communications team lessen the harmful impact.

Outline roles, responsibilities and communication protocols

› Draft pre-approved templates for various communication scenarios, including media requests, internal updates and customer notifications. Templates should be adaptable to different types and attack severity.

› Define clear procedures for notifying internal stakeholders, both employees and board members, as well as external parties such as customers and stakeholders.

› Identify individuals in your organisation to act as official spokespeople if an incident happens. Make sure they are trained in crisis communication and that they understand your incident messaging strategy.

External outreach

- Identify the key stakeholders you would need to inform of an incident and any disruption it causes.
- Understand the communications channels you have available to help you reach stakeholders. This could include mailing lists, internal newsletters, social media channels and journalist contacts.
- To help you stay informed about public perceptions, set up systems to monitor media and social media coverage. This will also help you respond promptly to misinformation or rumours.

Test and review your plan

- Conduct regular tabletop exercises and simulations to test the effectiveness of your strategy and to identify areas for improvement. This also helps everyone understand their roles and responsibilities in a crisis.
- Regularly review and update your communications strategy to incorporate lessons learned from tabletop exercises, changes in the threat landscape and any changes in regulatory requirements.

Set up alternative communications

- During a cyber incident, your usual communications channels may not be available. You may need to establish alternative ways to keep in touch with staff, stakeholders and customers, using phone lines, messaging apps or social media platforms.
- If a large number of people could be impacted, it may be worth establishing a dedicated customer support line, email address or platform where customers can ask questions, get help and receive updates.

2. Communicate clearly with different parties, and tailor your messaging where necessary

In an incident, it is best practice to provide clear information that stakeholders, customers and the media need to know, while also being careful not to disclose information that may heighten the risk to your organisation or customers.

An organisation typically has a number of different groups to consider, which will probably include staff, customers, stakeholders and the media. Your communications should address the specific concerns and needs of each group, while also ensuring that the core points are consistent across them.

It may be useful to establish regular internal meetings with key staff and invite a member of the communications team to these meetings where possible, or at least have communications as a standing agenda item, to provide input and situational awareness updates.

Managing your own communications

- Your communications should be clear, consistent, authoritative, accessible and timely. Where possible, provide reassurance that you are taking the right steps to respond to an attack.
- Transparency helps build trust and credibility with stakeholders. Commit to transparent communication with your stakeholders, and provide timely updates on the incident, its impact and your response.
- Provide accurate information about the impact and avoid hyperbole.
- Avoid saying anything that may have to be retracted later. For example, there may be internal pressure from some parts of the business to provide assurance that everything is in hand, but be careful not to misrepresent or downplay the incident in a way that creates future difficulties. For example, stating that there is no known impact on staff or personal data can be problematic later down the line if this understanding changes in later investigations.

- Make use of available resources. If you need customers or partners to take action in some way, signpost appropriately, for example, by directing customers to the NCSC guidance on managing the impact of a data breach.

- If individuals could be directly impacted, reflect this in your communications. For example, an attack on a healthcare provider should acknowledge the real-world impact on service users, such as cancelled appointments, and not just the technical aspects of the incident.

Managing external factors

- Manage speculative media coverage with care, such as inaccurate reporting about the impact or suggestions that personal data has been compromised when it hasn't. By managing communications proactively, you can control the narrative around the incident. Highlight your response efforts, the steps you are taking to prevent future incidents, and your commitment to safeguarding stakeholder interests.

- Avoid compromising the integrity of future investigations by regulatory bodies or law enforcement agencies. You can still provide updates that are factual and consistent with the progress of the investigation, without revealing sensitive details. You should also avoid speculation or premature conclusions about the cause or extent of the incident, or who is behind it.

- While some groups require more detailed information about the incident than others, you should be aware of the risk that this information could be leaked to the media.

Prepare answers and a statement in advance

As well as preparing an on-the-record media statement, you could also develop a questions and answers document which considers what a journalist might ask if an incident becomes public. This will help you maintain trust with stakeholders and counter potential reputational damage. Example questions might include:

- Which services are affected?

- When will services be restored?

- Who is behind the attack?

- Is this a ransomware attack?

- Have the appropriate regulators been informed, for example, the Information Commissioner's Office?

3. Manage the aftermath in the medium to long term

A cyber incident can resemble an earthquake in its impact. When it first happens, there is often an immediate shockwave as the victim organisation rushes to identify the technical causes, and address operational impact in communications to staff, stakeholders and the media.

Depending on the incident, recovery time can vary from only a few days to several months. You should consider this in your communications response.

When you develop messaging and communicating in the medium to long term, consider:

- **Providing regular updates** on the progress of incident response efforts, including any milestones achieved and anticipated timelines for resolution. After the initial phase, external factors, such as stolen data leaked on the dark web or a regulator issuing a penalty, may resurface the story so you should prepare for these possibilities.

- **Communicating updates on your assessment of the impact**, including the extent of potential data compromise, the status of recovery and remediation efforts.

- **Continuing to engage** with key stakeholders to provide updates, address concerns and maintain transparency throughout the recovery process. This can also help rebuild trust and credibility with stakeholders.

- **Maintaining open communication channels with the media**, providing updates and responding to enquiries in a timely and transparent manner to counter negative publicity and misinformation.

- **Sharing insights and lessons learned** from the incident response process and actions taken to strengthen resilience and preparedness for future incidents. The NCSC encourages transparency as a way to build collective resilience across the UK. For example, the British Library published a 'lessons learned' report following a ransomware attack in October 2023. While not all organisations will be comfortable sharing this level of detail, it is an excellent example of what can be done to support the resilience and understanding of others.

After an incident, you should review your communications response and update your strategy to reflect any changes that need to be made. This can include speaking to stakeholders, both internal and external, to see how the message was received and what could be improved.

Additional resources

- NCSC guidance for CEOs in public and private sector organisations on how to manage a cyber incident
- The free NCSC Exercise in a Box resource, designed to help organisations test their plans and preparedness against realistic scenarios
- NCSC 'Top Tips for Staff' for non-technical readers, which explains why cyber security is important and how attacks can happen, with tips to complement existing organisational policies and procedures
- NCSC guidance about managing staff welfare during an incident.
- NCSC guidance for organisations considering payment in ransomware incidents

NCSC.GOV.UK @NCSC @CYBERHQ @CYBERHQ National Cyber Security Centre