AR-IN-A-BOX

CYBER CRISIS COMMUNICATION GUIDE

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu
website: www.enisa.europa.eu

LEGAL NOTICE

COPYRIGHT NOTICE

Project Number: 2023.5729 Title: CYBER CRISIS COMMUNICATION GUIDE
Linguistic version: EN PDF Media/Volume: PDF/Volume_01 Catalogue number: TP-03-23-469-EN-N
ISBN: 978-92-9204-656-9 DOI: 10.2824/802357

Authors: Peter Biro, Alexandros Zacharis, Georgia Bafoutsou, Dimitra Liveri (ENISA)

ACKNOWLEDGEMENTS

Special thanks to ENISA’s Awareness Raising Ad Hoc Working group for their support.

The Cyber Crisis Communication Guide is a comprehensive resource designed to help enterprises prepare for and respond to a cyber crisis. The guide provides practical guidance on how to create an internal and external cyber crisis communication plan, assess cybersecurity risks, and evaluate organisational size and complexity. It also outlines best practices for consulting with cybersecurity and communication experts during a cyber crisis.

The guide emphasises the importance of proactive planning and preparation, including conducting regular risk assessments, establishing clear communication protocols, and training employees on cybersecurity best practices. It also provides guidance on how to respond to a cyber crisis, including how to manage media inquiries, communicate with stakeholders, and coordinate with law enforcement and other relevant authorities.

Overall, the Cyber Crisis Communication Guide is an essential resource for all organisations looking to protect their reputation, retain the trust of their customers and partners, and minimise the financial and operational damage caused by a cyber crisis.

This document focuses on the steps to create an Internal & External cyber crisis communications plan.

HOW TO USE THE DOCUMENT

These guidelines have been created with the best interests of any organisation in mind (whether the reader is and SME or a large corporation the steps to follow remain the same), and we encourage you to utilise them in a way that suits your organisations unique requirements. Any organisation can adapt the recommendations provided to perfectly align with its goals and aspirations.

Every individual and organisation are different, and therefore, flexibility and customisation are crucial. Feel free to make any necessary adjustments, add supplementary information, or reformat the document to suit your preferred style or branding. Our intention is to provide you with a solid foundation upon which you can build, ensuring that the guidelines become an integral part of your success. It would be beneficial for the community and for the evolution of this guide to share your experiences and success stories with us.

PURPOSE OF THE GUIDE

Remember, this document is a tool for you to leverage in your journey towards excellence. We are excited to witness the unique ways in which you adapt and utilise these guidelines, and we encourage you to. Your feedback is invaluable and will contribute to the ongoing refinement and improvement of this resource. Our ultimate goal is to support you in achieving your desired outcomes, and we wholeheartedly believe that your individual touch and customization will play a pivotal role in making these guidelines truly impactful for your specific context.

DETERMINING THE NEED AND SCALE OF A CYBER CRISIS COMMUNICATION PLAN

1

Determining the need for a cyber crisis communication plan and assessing its scale and depth involves evaluating various factors related to an organisation's cybersecurity posture, industry, and potential risks.

- Assess cybersecurity risks
- Review regulatory requirements
- Evaluate organisational size and complexity
- Identify key stakeholders
- Analyse reputation and brand risk
- Conduct a gap analysis
- Consult with cybersecurity and communication experts
- Consider Lessons learned and best practices

In a nutshell:

- The more sensitive data the organisation handles, or the more critical the infrastructure it operates is, greater is the need for a comprehensive cyber crisis communication plan
- Compliance requirements can help determine the scale and depth of the cyber crisis communication plan

- The broader the impact to stakeholders in case of a cyber incident, the more comprehensive and detailed the plan should be.
- Consider the impact of negative publicity, customer trust erosion, and loss of business. A strong communication and reputation management plan can effectively mitigate their impact.
- Size and complexity of the organisation, influence the cyber crisis communication plan and need to address necessary communication aspects.
- Additional planning, coordination, or training might be needed to ensure effective communication during a crisis.
- Learn from the experiences of other organisations that have faced similar incidents.

By considering these factors and conducting a thorough assessment, one can determine whether a cyber crisis communication plan is necessary for the organisation and the level of detail required to address the specific risks and stakeholders. Remember to regularly review and update this plan as the cybersecurity landscape evolves and the organisation's needs change.

When a disaster strikes, it is essential that an organisation be able to communicate internally and also with the outside world

- if an organisation is unable to keep the outside world informed of its recovery status, the public is likely to fear the worst and assume that the organisation is unable to recover
- it is also necessary that the organisation communicates about disaster internally so that employees know what steps they are expected to take in that situation

PREPARING THE COMMUNICATION PLAN

2

2.1 IDENTIFYING OBJECTIVES

The first step in this process is to set the objectives of the cyber crisis communications plan. These derive from the overall organisation goals, in terms of awareness raising and education. Those will, in turn, determine the selection of the specific tools and methods to be used.

Every organisation might set different objectives for its own cyber crisis communications plan, yet some generic ones that are always applicable are the following:

2.1.1 Protect the organisation's reputation

A cyber crisis can damage an organisation’s reputation, causing long-term harm to the business. The first objective of a cyber crisis communications plan should be to protect the organisation's reputation by communicating quickly, transparently, and effectively with stakeholders. This objective involves carefully crafting key messages, controlling media interactions, and addressing stakeholder concerns in a way that mitigates negative perceptions and preserves the organisation's reputation.

2.1.2 Provide timely and accurate information

The crisis communication plan aims to ensure that accurate and up-to-date information regarding the cyber incident is communicated to stakeholders in a timely manner. This objective helps minimise rumours, misinformation, and confusion, and establishes the organisation as a reliable source of information.

2.1.3 Ensure customers or stakeholders are informed

In the event of a cyber crisis, it is critical that all stakeholders are kept informed of the situation. This includes employees, customers, partners, suppliers, and regulatory authorities. The crisis communication plan should outline how and when each stakeholder group will be notified of the incident, and what information will be shared. It should also aim to instil confidence in stakeholders by demonstrating transparency, empathy, and a proactive approach to resolving the cyber incident. Maintaining trust is essential for preserving the organisation's reputation and relationships with stakeholders.

2.1.4 Mitigate the impact of the crisis

A cyber crisis can have significant financial and operational impacts on an organisation. The crisis communication plan should include strategies for mitigating these impacts, such as developing contingency plans, prioritising business-critical functions, and communicating with other, potentially affected parties.

2.1.5 Manage media relations

The crisis communication plan should outline strategies for managing media relations during a cyber crisis. This objective involves providing accurate and timely information to the media, coordinating media interactions, and proactively managing the organisation's public image through effective media engagement.

2.1.6 Coordinate crisis response efforts

In order to effectively respond to a cyber crisis, it is important that all internal and external stakeholders are coordinated and working together. The crisis communication plan should outline how different departments within the organisation will collaborate, and how external partners and vendors will be involved in the response effort.

2.1.7 Learn from the crisis

Finally, a cyber crisis can be an opportunity for an o to learn and improve its cyber resilience. The crisis communication plan should include strategies for gathering feedback and data after the crisis has been resolved, in order to identify areas for improvement and make changes to prevent future incidents. Among others it should outline processes for gathering feedback, conducting post-incident assessments, and using the insights gained to refine the communication strategies and enhance future crisis response capabilities.

2.2 CHOOSING TARGET GROUP

The targeted audience for a cyber crisis communications plan for any organisation includes all stakeholders who may be affected by a cyber incident, such as employees, customers, partners, suppliers, regulatory authorities, and the media. The choice of which stakeholders to include in the plan will depend on the nature of the business operations, the types of sensitive data the organisation handles, and the regulatory requirements for the industry in which it operates.

When choosing the audience for a cyber crisis communications plan, it is important to consider each group's specific needs and concerns. For example, employees may require detailed information about how the incident occurred and what steps are being taken to mitigate it, while customers may be more concerned about the safety of their personal information and what steps they can take to protect themselves. Regulatory authorities will likely be interested in showing compliance with relevant data protection regulations, while the media may focus on the impact of the incident on the broader community.

It is also important to consider the best channels for communicating with each stakeholder group. For example, employees may be best reached through internal messaging systems, while customers may prefer to receive updates via email or social media. In some cases, it may be necessary to provide targeted messaging for specific stakeholder groups, such as language-specific communications for non-native speaking customers or simplified messaging for those with limited technical knowledge.

Table 1. Employee (Internal) target groups and channels

Audience groups	Channels
Generic Employees	Communicating with employees is essential during a cyber crisis. They need to be well-informed about the incident, its impact on the organisation, and any measures being taken to address it. **Recommended channels to reach employees include internal email communications, company-wide meetings or town halls, intranet portals, and employee communication platforms or apps.**
Executives and Management	Keeping executives and management informed is vital for effective decision-making and coordination during a cyber crisis. Regular updates and briefings should be provided to this group. **Channels to reach executives and management can include targeted email communications, leadership meetings or conference calls, dedicated executive communication channels, and secure messaging platforms.**
IT and Security Teams	These teams play a critical role in incident response and remediation efforts. Close coordination and communication with IT and security teams are necessary to address the technical aspects of the cyber crisis. **Channels such as dedicated incident response platforms, secure collaboration tools, and direct communication channels should be utilised to reach these teams.**
Internal Stakeholders	Depending on the organisation, there may be specific internal stakeholders, such as department heads, project managers, or other key personnel, who need to be included in the communication plan. These stakeholders may have unique responsibilities or requirements during a cyber crisis. **Tailored communication channels, including targeted email communications, team meetings, or designated communication liaisons, should be utilised to reach them effectively.**

By carefully considering the needs of each stakeholder group and choosing the most effective channels for communication, organisations can ensure that their cyber crisis communications plan is tailored to the needs of their audience and is most likely to be effective in mitigating the impacts of a cyber incident.

Same applies for external target groups; these refer to the individuals, organisations, or entities outside the organisation who may be impacted by or have an interest in the cyber incident. These groups are key stakeholders who need to be informed, engaged, and provided with relevant information during a cyber crisis

Table 2. External stakeholder target group

Audience groups	Channels
Customers	The organisation's customer base is a crucial external target group. They may be directly affected by the cyber incident, such as through data breaches or service disruptions. Customers rely on timely and accurate communication to understand the impact on their personal information, accounts, or services, and to receive guidance on any necessary actions. **Recommended channels to reach to stakeholders is through a direct communication line via email or SMS, few hours after the incident have been identified. In some cases, the IT can contact them directly to provide advice or mitigation measures.**
Partners and Suppliers	External organisations that the business collaborates with or rely on for business operations, such as suppliers, vendors, or business partners, should be considered as an external target group. Informing them about the cyber incident is essential for managing potential disruptions to supply chains, shared systems, or data exchange. **Channels to reach partners and suppliers can include targeted email communications, designated communication liaisons and in some cases direct communication channels between IT and Security Teams (point of contact – PoC).**
Regulatory Authorities	Depending on the industry the organisation is operating, various regulatory authorities, such as data protection agencies or industry-specific cybersecurity bodies, may require notification and cooperation in the event of a cyber incident. Compliance with legal and regulatory obligations is vital, and these authorities need to be informed in a timely manner. This time is set by the competent authority and usually is between 24 and 72 hours. **Channels to reach regulatory authorities are set by national legislation and might be through a dedicated platform, or via email or direct phone call. The organisation must be informed and hold this information in the incident response policy.**
Media	The media plays a significant role in shaping public perception and disseminating information during a crisis. Journalists, reporters, and media outlets are external target groups that need to be provided with accurate and consistent information. Proactive engagement with the media can help manage the narrative surrounding the cyber incident. **Designated communication liaisons or communication lead should reach targeted channels or media with tailor made statements and messages.**

Audience groups	Channels
Investors and Shareholders	Organisations with publicly traded stocks or investors have a responsibility to keep their stakeholders informed about the potential impact of a cyber incident on the company's operations, financials, and reputation. Shareholders, institutional investors, and analysts may need to be updated on the incident's ramifications and the steps being taken to address it. **Tailored communication channels, including targeted email communications, shareholders meetings, or designated communication liaisons, should be utilised to reach them effectively.**
General public	Depending on the nature and scope of the cyber incident, the local community or the general public may be indirectly affected or have an interest in understanding the implications. Providing accurate and transparent communication can help mitigate any concerns or potential reputational damage. **Communication via the mass media can have great outreach to the local community and general public. Tailor made messages to ensure mitigation measures are important.**

2.3 SITUATION ASSESSMENT

When faced with a cyber crisis, it is crucial to begin by defining the nature and extent of the incident. This involves gathering comprehensive information about the root cause, scope, and severity of the cyber event. This exercise is performed by the designated incident response team, but final result should take into account communication related aspects such as:

- Affecting safety and wellbeing of people
- Affecting the reputation of the organisation
- Possible political implications
- Affecting the establishment of the organisation
- Legal implications or lack of compliance with current regulation
- Affecting the confidence of the organisation towards stakeholders

The assessment process may require the involvement of cybersecurity experts, forensic analysts, legal counsel, and other relevant professionals, depending on the scale and complexity of the incident.

The Governing board or C-level executives would also need to provide their view and eventually approve the communications plan built on this information. Collaboration and coordination among experts can enhance the accuracy and depth of the assessment, enabling a more informed response to the cyber incident.

Severity levels can be high, medium or low, and below some communication techniques based on each level.

High Severity

1. **Immediate Notification:** In the event of a high-severity cyber incident, the crisis communication plan should prioritise immediate notification of key stakeholders, including executive leadership, IT/security teams, legal, and relevant departments. Communication channels should be established in advance for rapid dissemination of information.

2. **Impact Assessment:** Quickly assess the potential impact on the organisation's critical systems, data, and operations. Determine the extent of data breaches, system compromises, and potential financial or reputational damage.

3. **Escalation and Decision-Making:** Establish a clear chain of command for decision-making and escalation. Key executives should be informed and involved in determining the course of action, which may include activating the incident response team, engaging external experts, and coordinating with law enforcement if necessary.

4. **External Communication:** Coordinate with legal and public relations teams to develop external communication strategies. While the initial focus is on containing the incident, prepare for potential regulatory reporting, customer notifications, and media engagement if the incident escalates.

5. **Internal Communication:** Communicate clearly and concisely with employees about the incident's severity, potential impact on their work, and any immediate actions they need to take. Provide guidance on how to avoid spreading misinformation and emphasise the importance of reporting any suspicious activity.

Medium Severity

1. **Stakeholder Notification:** Notify relevant stakeholders, including IT/security teams, department heads, and legal, about the incident. Share initial information about the incident's potential impact and ongoing assessment.

2. **Impact Assessment:** Conduct a thorough impact assessment to understand the extent of the incident and potential risks. Determine if critical systems are affected and whether data breaches have occurred.

3. **Incident Response Activation:** Activate the incident response team and begin containment and remediation efforts. Communicate internally with the team about their roles and responsibilities during the incident response.

4. **External Communication:** Prepare to provide updates to external parties as the situation evolves. Develop messaging that acknowledges the incident, reassures customers and partners, and conveys that the organisation is taking appropriate action.

5. **Internal Communication:** Inform employees about the incident's potential impact on their work and any precautionary measures they should take. Provide regular updates to keep them informed about the organisation's response efforts.

Low Severity

1. **Internal Notification:** Notify relevant internal teams, particularly IT/security staff, about the incident. Begin gathering information to assess the incident's scope and impact.

2. **Impact Assessment:** Assess the incident's impact on non-critical systems and data. Determine whether any sensitive information has been compromised.

3. **Remediation:** Initiate appropriate remediation measures to contain and mitigate the incident. Update internal teams on the progress of containment efforts.

4. **Limited External Communication**: If necessary, prepare to provide limited updates to external parties, focusing on transparency and reassurance. Avoid unnecessary alarm while keeping stakeholders informed.

5. Internal Communication: Communicate to employees about the incident's low severity, the actions being taken, and any precautions they should be aware of. Emphasise the organisation's commitment to cybersecurity.

By tailoring your crisis communication plan to these severity levels and focusing on potential impacts, your organisation can effectively respond to cyber incidents while maintaining transparency, minimising disruption, and safeguarding its reputation.

2.4 CREATING A CRISIS COMMUNICATIONS TEAM

Creating a cyber crisis communications team is an essential component of any cyber crisis communications plan for SMEs. The team should consist of individuals with specific roles and responsibilities for managing communications both internally and externally. When creating the Team, it is advised to include representatives from relevant departments, such as IT, legal, public relations, and executive management. Below are some of the key roles and functions that should be considered for the team.

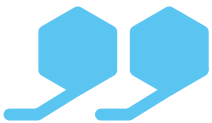
The Incident Manager is ultimately responsible for all communications related decisions during a crisis.

The incident manager is responsible for coordinating the overall response effort and ensuring that all members of the team are working together effectively. This individual should have strong leadership skills and be able to make decisions quickly in a high-pressure environment. The incident manager acts as the head of the Crisis Communications Team.

The Spokesperson or Communications coordinator plays a crucial role as the primary point of contact and official representative of the organisation during a cyber crisis. Their core activities revolve around effective communication, reputation management, and stakeholder engagement.

Firstly, the spokesperson is responsible for delivering clear, consistent, and accurate messages that align with the organisation's communication strategy. They serve as the voice of the organisation, conveying key messages to the media, stakeholders, and the public. Their role involves developing and delivering messages that address the concerns and needs of different stakeholder groups, ensuring the information is tailored appropriately.

It is importamnt to keep the contact details of some key audiences offline, in case systems become unavailable (e.g.: local emergency services, security service provider, potentially top clients and suppliers, regulators, differenrt stakeholders)



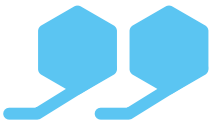
Secondly, the spokesperson acts as the main interface for media interactions. They handle interviews, press conferences, and media inquiries, responding to questions, concerns, and providing timely and accurate information. Their ability to engage with journalists professionally, while staying aligned with the organisation's messaging, is critical in shaping public perception and managing the narrative surrounding the cyber incident.

Furthermore, the spokesperson plays a pivotal role in reputation management. They convey a sense of empathy, transparency, and accountability, working to maintain stakeholders' trust and confidence. By addressing reputational risks proactively and handling external communication with integrity, the spokesperson helps protect the organisation's brand and image throughout the crisis.

Lastly, the spokesperson engages with external stakeholders, such as customers, partners, regulatory authorities, and the public. They provide updates, address concerns, and offer guidance to these groups. This engagement is crucial in maintaining open lines of communication, managing expectations, and building trust. The spokesperson ensures timely and accurate information flow, helping stakeholders navigate the crisis and providing reassurance during a challenging time.

Technical Expert: The technical expert should have deep knowledge of the SME's IT infrastructure and be able to provide guidance on technical issues related to the incident. This individual should also be able to advise on technical solutions for mitigating the incident and preventing future occurrences. Keep in mind that at the beginning of an incident technical experts are busy with the remediation and investigation. Therefore, make sure to gather the relevant questions in advance and occupy the technical expert as shortly as possible in rapid sync-up meetings.

Externally, the team is responsible for managing communications with customers, partners, suppliers, regulatory authorities, and the media. This may include drafting and disseminating public statements, coordinating with the legal team to ensure compliance with data protection regulations, and managing media relations. The team should also be responsible for monitoring social media channels and responding to inquiries from stakeholders.



Legal Advisor: The legal advisor is responsible for ensuring that all communications related to the incident are compliant with relevant data protection regulations and other legal requirements. This individual should have strong knowledge of data protection law and be able to provide guidance on legal issues related to the incident.

Human Resources Representative: The human resources representative should be responsible for communicating with employees and ensuring that their needs are met in the aftermath of the incident. This individual should be able to provide guidance on employee communication and support.

An example table of possible roles and associated responsibilities are to be found in Annex I.

2.5 DEVELOP KEY MESSAGES

When developing key messages during the activation of a cyber crisis communication plan, there are several main points to consider. First and foremost, accuracy and transparency should be prioritised. It is crucial to provide information that is verified, factually correct, and free from speculation. By sharing accurate and transparent messages, the organisation can establish credibility and trust among stakeholders.

Clear and concise language is another important aspect of key message development. Messages should be formulated in a manner that is easily understood by diverse stakeholders, avoiding technical jargon or complex terminology. Using simple and straightforward language ensures that the messages can be easily comprehended and remembered, enabling effective communication during a time of crisis.

Stakeholder relevance is another key consideration. Different stakeholder groups have specific concerns and interests, and messages should be tailored accordingly. By addressing the unique needs of each group, organisations can provide information that is meaningful and impactful to the recipients. Customising the messages to resonate with the stakeholders enhances their understanding and engagement.

Lastly, empathy and assurance should be incorporated into the key messages. Demonstrating empathy towards those affected by the cyber incident and acknowledging their concerns helps establish a compassionate tone. Additionally, providing assurances regarding the organisation's commitment to resolving the issue, protecting affected

individuals, and preventing future incidents instils a sense of trust and confidence. Empathy and assurance can help alleviate anxiety and foster a positive perception of the organisation's response to the crisis.

In summary, when developing key messages for a cyber crisis, organisations should **focus on accuracy, transparency, clear language, stakeholder relevance, empathy, and assurance.** By considering these main points, organisations can effectively communicate with stakeholders, build trust, and navigate the crisis with transparency and confidence.

2.6 ESTABLISH INTERNAL COMMUNICATION PROTOCOLS

To facilitate effective internal communication during a cyber crisis, it is crucial to develop clear and well-defined procedures. These procedures should outline the steps and protocols for sharing information within the organisation, ensuring that messaging remains consistent and accurate across all departments and teams. By establishing a structured framework for internal communication, organisations can minimise confusion, prevent the spread of misinformation, and maintain a unified approach in addressing the crisis.

In addition to defining procedures, it is essential to clearly assign roles and responsibilities for communication during a crisis. Designate specific individuals or teams who will be responsible for managing and disseminating information within the organisation. Each role should have well-defined responsibilities and understand their authority when it comes to sharing information. Furthermore, it is important to provide guidelines regarding the types of information that can be shared internally and externally, as well as establish approval processes for sensitive or strategic messages. By implementing clear guidelines and approval mechanisms, organisations can ensure that only appropriate and authorised information is communicated, minimising the risk of unintended consequences or misrepresentation during a cyber crisis.

It is also crucial to inform all employees about the main points of the crisis communication plan, let them familiar with the plan, the roles and goals. Employees must also be informed about their roles and responsibilities with regard cyber crisis communication e.g.: how to use their social media, what information they can and what information they can’t share about the unfolding situation.

2.7 EXTERNAL STAKEHOLDER COMMUNICATION

During a cyber crisis, proactive communication with external stakeholders is crucial in managing the situation effectively. It is essential to provide timely updates to keep stakeholders informed about the incident, its impact, and the steps being taken to address it. This includes addressing their concerns and managing their expectations regarding the resolution and recovery process. It is important to prioritise communication with various external stakeholders, such as affected individuals, regulatory authorities, customers, partners, and the media. Each stakeholder group may have unique concerns and information needs, and tailoring the communication approach accordingly helps maintain trust, transparency, and open lines of communication.

In the age of social media and online platforms, **monitoring discussions and sentiment related to the cyber incident is vital.** Organisations should actively track social media channels, forums, and other relevant online platforms to identify emerging issues, rumours, or misinformation circulating about the incident. By promptly addressing any inaccuracies, clarifying information, and responding to concerns raised by the online community, organisations can help mitigate the potential negative impact and maintain a positive reputation. Monitoring social media also provides an opportunity to gauge public sentiment and adapt communication strategies as necessary to address emerging trends or issues. Being attentive and responsive in online spaces can contribute to effective stakeholder engagement and help shape the narrative surrounding the cyber crisis.

At the beginning and during the incidents there might not be 100% certainty of the technical factors. Keep your messages as simple as possible.

2.8 MEDIA RELATIONS

To effectively manage media interactions during a cyber crisis, it is crucial to prepare designated spokespersons who will represent the organisation. These spokespersons should undergo comprehensive media training to ensure they are equipped with the necessary skills and knowledge to handle interviews, press conferences, and other media engagements. Media training helps spokespersons deliver consistent, accurate, and professional messages while effectively managing the dynamics of media interactions. By honing their communication skills and becoming familiar with techniques for conveying key messages and responding to challenging questions, spokespersons can effectively represent the organisation and uphold its reputation during media engagements.

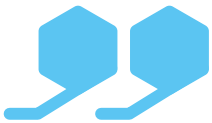
In addition to media training, organisations should develop press materials to support media interactions. These materials serve as valuable resources for spokespersons and journalists, providing them with accurate and relevant information about the cyber incident. Press materials may include press releases, which succinctly summarise the incident, its impact, and the organisation's response efforts. Q&A documents can anticipate common questions from the media and provide well-crafted answers to ensure consistent messaging. Fact sheets can offer additional background information, statistics, or technical details about the incident. Developing these press materials in advance helps streamline communication, ensures accuracy and consistency, and enables spokespersons to provide timely and reliable information to the media during a cyber crisis.

2.9 MONITORING AND EVALUATION

To ensure ongoing improvement and effectiveness of the cyber crisis communication efforts, it is crucial to establish a system for continuous monitoring and evaluation. This involves analysing feedback from stakeholders, monitoring sentiment in the media and online platforms, and assessing media coverage. By actively monitoring these factors, organisations can gauge the impact of their communication efforts, identify any gaps or areas for improvement, and make necessary adjustments in real-time. **This ongoing evaluation allows for agile decision-making and the ability to adapt communication strategies as the cyber crisis unfolds.**

In addition to continuous monitoring, conducting post-incident reviews is essential for capturing lessons learned and refining the cyber crisis communication plan. These reviews involve a thorough assessment of the organisation's response to the cyber incident, including the effectiveness of the communication strategies employed. By analysing the strengths and weaknesses of the communication plan, organisations can identify areas that performed well and areas that need improvement. Lessons learned from the incident can be used to update and enhance the crisis communication plan, ensuring that it remains relevant and robust for future incidents. Regular post-incident reviews foster a culture of continuous improvement, enabling organisations to continually enhance their crisis communication capabilities and better prepare for future cyber crises.

In some countries local governments provide guidance and templates to create documents related to cyber crisis communciation. always consult with your local regulator or competent authorities for further guidances.



2.10 STRATEGIES

A clear and well-structured strategy is crucial when developing a cyber crisis communication plan. Consider the following main points when creating such a plan. Organisations may consider expanding their existing communication strategies, if available.

2.10.1 Spokesperson Response

When a company makes a mistake, the best course of action is to apologise and demonstrate genuine humanity. Assigning a spokesperson to represent the brand is the most effective way to achieve this. One person can connect with stakeholders more easily than a group of lawyers, fostering a sense of relatability and empathy.

The spokesperson can be the CEO, a company executive, or an individual considered well-suited to represent the organisation. It is crucial to choose someone who possesses strong communication skills as their actions will have a significant impact on how key stakeholders respond to the situation. The ability of the spokesperson to humanise the company and present the mistakes as manageable plays a pivotal role in maintaining support from stakeholders.

By having a designated spokesperson who can convey the human side of the company and address the mistakes with sincerity, the organisation showcases its accountability and willingness to learn from the situation. This approach cultivates transparency and builds trust with stakeholders, demonstrating the company's commitment to rectify any errors. It is an opportunity to exhibit the brand's integrity and strengthen relationships with the audience during challenging times.

2.10.2 Proactive Damage Control

When developing a cyber crisis communication plan, proactive damage control should be a cornerstone of the cyber crisis communication strategy. It involves taking pre-emptive measures to minimise the impact of a crisis and mitigate potential risks. By adopting a proactive approach, the organisation can effectively address vulnerabilities and enhance the organisation's resilience to cyber threats.

One essential aspect of proactive damage control is conducting a comprehensive risk assessment. This assessment helps identify potential cyber threats and vulnerabilities specific to the

organisation. It involves evaluating the already existing cybersecurity measures, conducting penetration testing, and staying informed about emerging threats. By understanding these risks, the company can implement robust security measures that help prevent or mitigate the impact of a crisis.

In addition to risk assessment, developing a thorough incident response plan is vital for proactive damage control. This plan outlines the necessary steps to be taken in the event of a cyber incident. It includes defining roles and responsibilities, establishing communication channels, and providing a framework for decision-making and escalation. By having a well-defined plan in place, the organisation can respond swiftly and effectively, minimising the impact on the organisation and stakeholders.

Training and awareness programs also play a significant role in proactive damage control. Regularly educating employees about cybersecurity best practices empowers them to identify and report potential threats, practice good password hygiene, and adopt safe browsing habits. By fostering a culture of cybersecurity awareness within the organisation, one can create a proactive line of defence against cyber threats.

Having a predefined list of companies those can assist in proactive damage control might come handy in case of cyber crisis wight significantly reducing response time.

2.10.3 Case Escalation

Sometimes crises can be resolved on the individual level before they reach a viral tipping point. For these cases, it helps to create an escalation system within the organisation's customer service team that can diffuse the issue before it gets out of hand.

When creating a cyber crisis communication plan, it is crucial to address and prevent the escalation of the situation. This requires a proactive and strategic approach to mitigate the potential damage and maintain control over the incident. First and foremost, a swift response and efficient incident management process are essential. Establish clear roles and responsibilities, along with defined escalation paths, to ensure that the incident is addressed promptly and effectively.

Transparent and timely communication is another critical aspect. Keep stakeholders informed about the incident, its impact, and the steps being taken to mitigate it. Transparency helps build trust and reduces the likelihood of speculation and misinformation. Timely updates are crucial to prevent the situation from escalating due to a lack of information.

Effective coordination and collaboration among internal teams, external partners, and stakeholders are vital in preventing escalation. Establish channels for communication and information sharing to facilitate a coordinated response. Leveraging the expertise, resources, and support of all relevant parties, the organisation can address the incident comprehensively and minimise the chances of it spiralling into a larger crisis.

2.10.4 Social Media Response

Social media is a wonderful marketing tool that allows companies to reach audiences across the globe. But this reach works both ways, as customers can share stories, post pictures, and upload videos for the world to see. One viral video painting the company in the wrong light can lead to millions of people developing a negative perception of the brand.

Crises are battled both in-person and online. In order to cope with the challenges derived from the social media, the company needs a social media plan that can manage the digital buzz around the business or company. This may include assigning more representatives to monitor the company's social channels or updating followers with new information. However, it is utilised, social media cannot be disregarded when a company is navigating through a crisis.

2.10.5 Customer Feedback Collection and Analysis

At times, companies may encounter a crisis that lacks public attention or social media virality. Instead, it silently impacts the company's customers and leads to churn, often due to insufficient feedback collection. Without gathering enough feedback from customers, the company may remain unaware of the issue's impact on the customer base.

To address this challenge, it is crucial to prioritise customer feedback collection and analysis during a crisis. Actively seek feedback through various channels such as surveys, customer support interactions, and online platforms. Encourage customers to share their experiences and concerns openly, ensuring that their voices are heard.

Once customer feedback is gathered, it is essential to analyse it effectively. Look for patterns, common themes, and emerging issues that could indicate the extent of the crisis's impact on customers. This analysis can provide valuable insights into the specific areas that need immediate attention and mitigation efforts. By identifying and addressing customer concerns promptly, the organisation can mitigate further churn and demonstrate the commitment to resolving the crisis.

EXECUTION OF THE PLAN

3

PRINCIPLES FOR CRISIS COMMUNICATIONS

Acknowledge the crisis: Do not try to hide if/when there is an incident developing, but be careful not to take ownership or responsibility for a crisis that is not the organisation's responsibility.

Act swiftly and decisively: As soon as the incident is identified, activate the crisis communication plan, delays lead to speculation, misinformation and reputational damage.

Communicate what the organisation knows: Provide factual information only, without judgment, emotion or guessing.

Clear and Transparent: Responses should be timely, accurate and consistency, despite the likely external media and stakeholder pressure.

Show empathy: It is important to express concern for any affected parties, whether internal or external; take responsibility and apologise if it is demonstrably at fault.

Action-oriented: Detail the steps being taken to remedy the situation and avoid it happening again in order to reassure key stakeholders.

Provide perspective: Place the situation into context.

Tailor messages to different stakeholders: provide each group with necessary information, guidance and support.

Establish clear lines of communication: Provide contact information, such as dedicated hotlines or email addresses, to facilitate communication and ensure that queries and concerns are addressed promptly.

Leverage social media and online platforms: Monitor relevant hashtags and keywords to stay aware of public sentiment and address any emerging issues or misinformation proactively.

Manage media effectively: Maintain a proactive approach in managing media inquiries, providing accurate information, and promptly correcting any inaccuracies or misleading reports.

Provide ongoing updates: Acknowledge the need for ongoing communication to maintain engagement and reassure stakeholders that the issue is being addressed.

Conduct "Hot wash/ Cold wash" exercises after the crisis is resolved to capture findings and comments.

SOME PRACTICAL EXAMPLES

Below is an example of a practical use case for cyber crisis communication management and the actions that could be taken for internal and external mitigation.

Use Case: A small manufacturing company's servers have been compromised by a ransomware attack, resulting in significant data loss and production downtime.

Internal Mitigation Actions:

1. Activate the cyber crisis communication team and establish a clear chain of command.
2. Assess the severity of the incident and prioritise the response effort.
3. Notify employees of the incident and provide guidance on how to respond.
4. Work with the IT team to isolate infected machines and restore data from backups.
5. Assess the impact on production and develop a plan to resume operations.
6. Conduct an internal investigation to determine the cause of the incident and identify any vulnerabilities in the company's IT infrastructure.
7. Provide regular updates to employees and stakeholders as the situation evolves.

External Mitigation Actions:

1. Notify customers and suppliers of the incident and provide guidance on any impact on their operations.
2. Contact law enforcement and report the incident.
3. Work with legal counsel to ensure compliance with data protection regulations and other legal requirements.
4. Draft and disseminate public statements to media outlets and manage media relations.
5. Monitor social media channels and respond to inquiries from stakeholders.
6. Notify insurance providers and work with them to file a claim.
7. Conduct a post-incident review to identify areas for improvement in the response plan.

By following these internal and external mitigation actions, the small manufacturing company can effectively manage the impact of the ransomware attack on their operations and reputation.

Internal Communication Email Example:

Subject: Cyber Incident Update

Dear Employees,

As you may be aware, we recently experienced a cyber incident that has impacted our systems and operations. Our IT team is actively working to restore systems and data and minimise the impact of the incident.

We want to assure you that the safety and security of our employees, customers, and stakeholders is our top priority, and we are taking all necessary steps to address this incident. We have activated our cyber crisis communication team and are working closely with IT and other stakeholders to manage the incident.

We will provide regular updates as the situation evolves and appreciate your patience and understanding during this challenging time.
Sincerely,
[Your Name]

External Communication Website News Post Example:

Subject: Important Update: Cyber Incident Notification

We want to inform our customers and stakeholders that we have experienced a cyber incident that has impacted our operations. We are actively working to restore systems and data and minimise the impact of the incident. Our cyber crisis communication team is working closely with IT and other stakeholders to manage the incident. The safety and security of our customers, employees, and stakeholders is our top priority. We will provide regular updates as the situation evolves. Thank you for your understanding and support

External communication tweet example:

Important Update: We have experienced a cyber incident impacting our operations. We're working to restore systems & data with the safety & security of our customers, employees, and stakeholders as our top priority. Regular updates to follow.
#cybersecurity #incidentresponse

By using these communication channels and templates, SMEs can effectively communicate with their stakeholders during a cyber crisis and help minimise the impact of the incident.

EXERCISING THE PLAN

To effectively exercise a cyber crisis communication plan, organisations may consider the following types of exercises that vary in scale and stakeholder involvement.

Tabletop Exercises: Tabletop exercises are discussion-based exercises that simulate a crisis scenario in a controlled environment. They involve key stakeholders, such as members of the crisis communication team, senior management, IT personnel, and legal representatives. Participants discuss and analyse hypothetical scenarios, review the communication plan, and practice making decisions and coordinating communication efforts.

Functional Exercises: Functional exercises involve more active participation and simulate the operational response to a cyber crisis. They typically include a wider range of participants (internal and external). The exercise scenario unfolds gradually, allowing participants to engage in real-time decision-making, communication, and coordination activities.

Full-Scale Exercises: Full-scale exercises involve a comprehensive simulation of a cyber crisis scenario, often conducted in a realistic setting and with a broader range of participants. This may include representatives from multiple departments within the organisation, external partners, vendors, and relevant authorities. Full-scale exercises aim to replicate a real-life crisis situation as closely as possible, including aspects such as media engagement, public response, and stakeholder interaction.

In the event that the organisation already possesses a well-established framework for conducting cyber incident management exercises, it is advisable to broaden the scope of these exercises **to incorporate scenarios related to communication planning**. This inclusion allows participants to gain a comprehensive understanding of the overall incident management process, including the activation of the crisis communication plan.

It is considered as a good practice to **invite external observers** to oversee the conduct of the exercise. An observer can assist in evaluating the performance, assessing gaps and point to the areas that would require fine-tunning. This observer is not necessarily a consultant, but rather a communication expert or someone with experience in the area of crisis management.

Possible exercise scenarios

1. The email service is not accessible or untrusted, compromised

Objective: To practice effective communication and collaboration within the team when the company's email system is not accessible.

Simulation: Exercise participants simulate a scenario where an important announcement needs to be communicated to the public during the email outage. Each expert should apply their chosen communication methods and strategy to effectively convey the message.

2. The Organisation's general communication channels (teams, slack, yammer) are not available

Objective: To practice effective communication and teamwork when the organisation's general communication channels (e.g., Teams, Slack, Yammer) are not available.

Simulation: Exercise participants simulate a scenario where a cyber crisis is ongoing, and critical information promptly needs to be discussed, disseminated within the team and shared to stakeholders. Each expert should apply their chosen communication methods and strategy to effectively convey the information.

3. Incident happens in the middle of holiday period

Objective: To exercise the backup and alternate system

Simulation: Exercise participants simulate a scenario where a cyber crisis is ongoing during a holyday period and some of the key stakeholders and members of the crisis communication team are on vacation and unavailable.

4. Organisation's assets (network, laptop, communication channels) are inaccessible

Objective: To find alternative ways of communication and information sharing.

Simulation: Exercise participants simulate a scenario where due to a cyber crisis the organisation's assets are not available for use. Exercise participants must find a common agreement which alternative means of communication to be used and how to disseminate important information internally and externally in a timely manner.

LESSONS LEARNT AND LINES TO TAKE

After executing the cyber crisis communication plan, it is crucial to conduct a thorough review and gather feedback to learn valuable lessons and make necessary adjustments. Below there are some steps an organisation can take to gather feedback, analyse it, and adapt the cyber crisis communication plan accordingly.

Conduct Post-Incident Review

As soon as the cyber crisis has been resolved, gather the crisis communication team and other relevant stakeholders to conduct a post-incident review. This review should assess the effectiveness of the communication efforts and identify areas for improvement.

Gather Feedback from Internal Stakeholders

Collect feedback from the internal stakeholders, including members of the crisis communication team, IT department, executive management, and other relevant departments. Their insights can provide valuable perspectives on what worked well and what could be improved.

Seek Feedback from External Stakeholders

Engage with external stakeholders, such as customers, partners, regulatory authorities, and the media, to gather their feedback. This can be done through surveys, interviews, or focus groups. Their feedback will help to understand their perception of the company's communication efforts and identify any gaps or areas that need attention.

Analyse Media Coverage

Monitor media coverage of the cyber incident and the organisation's response. Analyse how the incident was portrayed, the accuracy of information, and any criticisms or concerns raised. This analysis will help to identify areas where the applied communication can be strengthened or clarified.

Monitor Social Media and Online Platforms

Keep an eye on social media platforms, online forums, and other relevant online spaces where discussions about the cyber incident may have taken place. Analyse sentiment, identify misinformation, and respond to any emerging issues or concerns. This feedback can provide insights into public perception and areas where communication can be enhanced.

Review Metrics and Analytics

Assess the performance metrics and analytics associated with the applied communication efforts. This includes evaluating the reach and engagement of the communication channels, such as website traffic, social media metrics, email open rates, and click-through rates. Analyse these data points to understand how the intended messages were received and whether adjustments are needed.

Update the Cyber Crisis Communication Plan

Incorporate the lessons learned and feedback into the existing cyber crisis communication plan. Revise and update the plan, ensuring that it reflects the new information gathered and addresses any identified areas for improvement. This may involve updating key messages, communication channels, internal procedures, or protocols.

Provide Training and Awareness

Communicate the updates and revisions to the cyber crisis communication plan to the relevant stakeholders within the organisation. Conduct training sessions, workshops, or awareness campaigns to ensure that everyone involved understands the changes and their roles in implementing them.

Continuously Review and Improve

Treat the updated cyber crisis communication plan as a living document. Regularly review and evaluate its effectiveness, taking into account emerging threats, changes in the cybersecurity landscape, and new best practices. Iterate and refine the plan to ensure its ongoing relevance and effectiveness.

ANNEXES

ANNEX I. CRISIS COMMUNICATIONS TEAM ROLES AND RESPONSIBILITIES

Role	Team	Responsibilities
Incident Manager	**Mandatory**	The incident manager is ultimately responsible for all communications related decisions during a crisis. The incident manager is responsible for coordinating the overall response effort and ensuring that all members of the team are working together effectively. This individual should have strong leadership skills and be able to make decisions quickly in a high-pressure environment.
Communications Coordinator	**Mandatory**	The communication manager will: • devise a communications strategy • together with the coordinator establish the crisis communication team in order to co-ordinate the dissemination of all information • liaise with the spokesperson or nominate spokespersons according to the magnitude/type of crisis • monitor and report on what is said about the crisis in media and on social media • draft key messages and clear them with the crisis manager • arrange for key messages to be distributed to all relevant audiences • update key messages when new decisions are made or new information becomes available • liaise with the communicators in other organisations/countries/partners and at other levels, where appropriate • lead the communications team • coordinate media management • coordinate internal communications • align on public communication matters with other relevant stakeholders

Role	Team	Responsibilities
IT / CISO	**Mandatory**	IT assesses the impact of the crisis on the organisation's IT systems and ensures continuity measures regarding business-critical IT systems. The IT/CISO have also to understand the incident and lead the planning of the remediation on the technical side.
Spokesperson	**Optional**	The spokesperson will be responsible for the content of all external communications. He/she is also the person in charge of communicating the organisation's official messages to the media during a crisis situation. The spokesperson will: • ensure that the organisation's messages get accurately and effectively communicated to the media during a crisis. • protect the organisation's reputation. • spokesperson is responsible for delivering clear, consistent, and accurate messages that align with the organisation's communication strategy and values. • acts as the main interface for media interactions. • the spokesperson helps protect the organisation's brand and image throughout the crisis. • the spokesperson ensures timely and accurate information flow, helping stakeholders navigate the crisis and providing reassurance during a challenging time.
Legal counsel	**Optional**	• The legal counsel is responsible for providing legal advice on the specific situation. • The legal counsel will ensure that the actions of the CMT comply with local regulations. • The legal advisor is responsible for ensuring that all communications related to the incident are compliant with relevant data protection regulations and other legal requirements.
Human Resources Representative	**Optional**	The Human Resources Representative will advise on how the crisis will impact on and be perceived by internal audiences, and the HR implications of the crisis. • the human resources representative should be responsible for communicating with employees and ensuring that their needs are met in the aftermath of the incident • will be part of the core team for any issues related to social relations and employees • will co-supervise the internal communications from a human resources perspective

Role	Team	Responsibilities
Operations	**Optional**	The head of operations works in close coordination with the CMT lead and coordinates the restarting of critical business processes, activating different organisation units or departments as required. The head of operations will advise on how the crisis will impact the business processes.
Finance	**Optional**	The head of finance will advise on all financial and insurance matters and: • will provide broad order costings for all options the CMT considers and will put in place any special accounting arrangements that are needed and will ensure that the costs associated with the crisis are accurately tracked and recorded • advises the CMT leader on insurances/claims issues, based on the existing policies
(Technical) Experts	**Optional**	The experts are responsible for providing input on the technical aspects of the crisis response. This will ensure that the crisis communications team is sharing the correct information with stakeholders and the media. • the experts are providing guidance on technical issues related to the incident • the experts are be able advice on technical solutions for mitigating the incident and preventing future occurrences Keep in mind that at the beginning of an incident technical experts are busy with the remediation and investigation. Therefore, make sure to gather the relevant questions in advance and occupy the technical expert as shortly as possible in rapid sync-up meetings.
Assistant	**Optional**	The crisis team assistant is: • dedicated to the CMT • responsible for office/administrative management • responsible for outfitting the crisis management office • responsible for reception of media and other visitors • responsible for minutes (extremely important to keep log of events & decisions for later possible legal issues) • responsible for collecting, filing and distributing log sheets and all other written materials (e.g., press releases, letters) • responsible for organising administrative support (including after hours if needed)

ANNEX II. CRISIS COMMUNICATIONS LOGBOOK FORM

A copy should be printed whenever necessary. Keep meticulous archives of all these forms.

Date: / / Time:	To be completed by the person in charge of the Log Book Mr/Mrs/Ms:		
CMT MEmbers:			
Time	**Decisions & Action plan**	**Person in charge**	**Deadline**

ANNEX III. CRISIS COMMUNICATIONS MEDIA ENQUIRY LOG FORM

Name of person taking enquiry	
Journalist name	Phone
Date	Mobile
Time	Email
Deadline	Twitter
Media/social media outlet and country	
Purpose of call/enquiry	
General attitude and tone of voice	
Links to any previous coverage on the subject	
Action taken (if any)	
Next steps (including person responsible)	

ANNEX IV. SOCIAL MEDIA COMMENTS LOG FORM

Date	Time	Social media comment and location (include hyperlink)	Response (if any)

ANNEX V. STAKEHOLDER & EMERGENCY CONTACT DETAILS

Contact details of all the relevant people or organisations should always be included in the crisis communication management plan to help with the process. This information must both be readily available and be kept up to date.

Crisis management team

CMT Role	Name	Position	Office Tel	Email	Mobile
Crisis manager					
Coordinator					
Communication manager					
Spokesperson					
Legal Counsel					
Finance					
Operations					
IT / CISO					
HR					
Experts					
Assistant					

Security, IT and Technical support

Role	Name	Position	Office Tel	Email	Mobile

ANNEX VI. KEY TAKEAWAYS

Cybersecurity threats are a growing concern for small and medium-sized enterprises (SMEs). The Cyber Crisis Communication Guide provides practical guidance on how to prepare for and respond to a cyber crisis. Here are the most important takeaways:

How to Prepare:

- Conduct **regular risk assessments** to identify potential vulnerabilities and threats.
- Establish clear communication protocols and **designate** a crisis management **team**.
- **Train** employees on cybersecurity best practices and **establish** incident response **procedures**.
- **Develop** an internal and external cyber crisis communication **plan**.

How to React:

- **Activate** the crisis management **team** and **follow** established incident response **procedures**.
- Communicate **clearly and transparently** with stakeholders, including customers, partners, and employees.
- Manage media inquiries and coordinate with law enforcement and other relevant authorities.
- Take steps to mitigate the impact of the cyber crisis and prevent further damage.

How to Learn from Crisis:

- **Review** case studies, industry reports, and best practices in cyber crisis communication.
- Conduct a **thorough assessment** of the cyber crisis communication plan and identify areas for improvement.
- Regularly review and **update the plan** as the cybersecurity landscape evolves and the organisation's needs change.
- **Use lessons learned** to enhance the organisation's preparedness and effectiveness in managing cyber incidents.

By following these steps, SMEs can better protect their reputation, retain the trust of their customers and partners, and minimise the financial and operational damage caused by a cyber crisis.

ANNEX VII. DOS AND DON'TS

Key Dos

1. Do conduct regular risk assessments to identify potential vulnerabilities and threats.
2. Do establish clear communication protocols and designate a crisis management team.
3. Do communicate clearly and transparently with stakeholders, including customers, partners, and employees.

Key Don'ts

1. Don't ignore potential cybersecurity threats or assume that your organisation is immune to cyber-attacks.
2. Don't delay in responding to a cyber crisis or fail to communicate with stakeholders in a timely and transparent manner.
3. Don't rely solely on technology to protect your organisation from cyber threats - employee training and incident response planning are also critical components of a comprehensive cybersecurity strategy.

ANNEX VIII. REAL-LIFE EXAMPLES OF CYBER CRISIS COMMUNICATIONS

Equifax: In 2017, Equifax, a credit reporting agency, suffered a massive data breach that exposed sensitive personal information of millions of consumers. Equifax's crisis communication response was swift and proactive. The company established a dedicated website to provide clear and timely information about the breach, including details on the incident, steps to check if one's data was affected, and instructions on how to enrol in credit monitoring. Equifax's CEO issued a public statement acknowledging the breach, and the company offered free credit monitoring and identity theft protection services to affected individuals. The communication was transparent, informative, and included consistent updates.

Link: Equifax Data Breach Response

Maersk: In 2017, global shipping company Maersk fell victim to the NotPetya ransomware attack, causing significant disruptions to its operations. Maersk's crisis communication was effective in conveying the severity of the situation, without disclosing sensitive details. The company utilised social media platforms to share updates on its response efforts, openly acknowledging the impact on its operations, while reassuring customers about its commitment to resolving the issue. Maersk's CEO communicated directly with stakeholders through video messages, providing a human touch to the crisis response.

Link: Maersk Twitter Updates

Yahoo: In 2016, Yahoo experienced a series of data breaches that affected billions of user accounts. The company's crisis communication response was criticised for its delayed disclosure of the breaches. Yahoo faced backlash for not promptly notifying affected users, which led to a loss of trust. The lack of timely communication and transparency damaged Yahoo's reputation and raised concerns about user data protection.

Link: Yahoo Data Breaches and analysis

Sony Pictures: In 2014, Sony Pictures experienced a cyber-attack that resulted in the leak of sensitive emails, employee data, and unreleased movies. Sony's crisis communication was criticised for downplaying the severity of the breach initially and not adequately informing employees about the situation. The leaked emails revealed internal discussions that were damaging to the company's reputation. Sony's communication lacked transparency and failed to effectively manage the crisis.

Link: Sony Pictures Cyber Attack

SMEs

Cracker Barrel: In 2017, an individual by the name of Bradley Reid raised an inquiry through Cracker Barrel's official corporate website. His query pertained to the circumstances surrounding his wife's departure from her 11-year managerial role at one of Cracker Barrel's establishments in Indiana. In response, Cracker Barrel opted for a restrained approach, refraining from providing a public statement. This decision was influenced by considerations surrounding matters of personal privacy and the potential for the company to become engaged in a defensive stance. Rather than engaging in immediate communication, the company opted for a strategy of allowing the situation to naturally dissipate over time.

Link: 10 Crisis Communication Plan Examples and Examples of effective crisis management and communication

TalkTalk: TalkTalk, a UK-based telecommunications company, experienced a cyber-attack in 2015 that exposed customer data. TalkTalk's crisis communication response involved swift acknowledgment of the breach and transparent communication with customers. The CEO appeared in media interviews, addressing the issue directly and reassuring customers about the steps being taken. The company also offered support to affected customers and took measures to enhance its cybersecurity. While TalkTalk faced criticism for the breach, its proactive communication helped mitigate the damage to its reputation.

Link: TalkTalk Data Breach Response

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu