|  |  |
| --- | --- |
| **Title:** Incident response communication plan | |
| **Approved by:** | **Approval date:** |
| **Senior management approval:** | |
| **Effective date:** | **Last updated:** |
| **Author:** | |
| **Communication point person:** | |
| **Purpose:** The purpose of this document is to provide a sample communications plan in the event of a cybersecurity incident. | |
| **Location:** This document should be accessible by all members of the incident response team, even if all communications systems and the main corporate network are offline. It should be stored in multiple locations, including the following:   |  |  | | --- | --- | | **Location** | **Access notes/instructions** | |  |  | |  |  | |  |  | |  |  | | |
| **Incident response team members and responsibilities:**   |  |  |  |  | | --- | --- | --- | --- | | **Name** | **Responsibility** | **Telephone** | **Email address** | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | |
| **Notification responsibilities**   |  |  |  |  | | --- | --- | --- | --- | | **Stakeholder** | **When to notify** | **Who gives final notification approval** | **Notification channel** | | **Cyber insurance** | [e.g., Once incident is confirmed] | [e.g., CEO and general counsel] | [e.g., email and/or telephone] | | **Law enforcement** | [e.g., Once incident is confirmed] | [e.g., CEO and general counsel] | [e.g., telephone] | | **Internal staff members** | [e.g., Once incident is confirmed] | [e.g., CEO, general counsel and HR] | [e.g., email and/or SMS] | | **Regulatory** **bodies** | [e.g., Within 72 hours of confirming incident] | [e.g., CEO and general counsel] | [e.g., email] | | **Customers/clients** | [e.g., Once details of the incident have been confirmed, especially if customer data is affected] | [e.g, CEO, general counsel and PR] | [e.g., social media and email] | | **Partners/suppliers** | [e.g., Once details of the incident have been confirmed, especially if partner/supplier data is affected] | [e.g., CEO and general counsel] | [e.g., email and/or telephone] | | |
| **Sample internal email**   |  |  | | --- | --- | | **Sender** | CEO | | **Subject** | Cybersecurity incident | | **Body** | Colleagues,  I regret to inform you that we are currently investigating a cybersecurity incident. Our IT systems appear to have been infiltrated by an unknown attacker, and as a result, some of our confidential data may have been compromised.  Our IT team is currently investigating the extent of the incident and is taking all necessary steps to mitigate the impact of the attack. At this time, however, we believe unauthorized individuals may have accessed some of our internal systems and data.  We take this matter very seriously and are working diligently to address the issue. We are also engaging with external security experts to conduct a thorough investigation to determine the extent of the attack and prevent any further compromise of our data.  I want to assure you we are doing everything in our power to safeguard our systems and data. We have already implemented additional security measures, and we will continue to take all necessary steps to prevent future incidents.  In the meantime, we ask that you remain vigilant and report any suspicious activity or emails to our IT department immediately. Please also be extra cautious when opening emails or attachments from unknown sources -- through email, text message, WhatsApp or social media.  We understand this incident may cause concern, and we want to assure you we are committed to providing updates as we learn more. If you have any questions or concerns, please do not hesitate to reach out to our IT team or myself.  Thank you for your understanding and cooperation during this time.  Kind regards,  [CEO name] | | |
| **Sample external email**   |  |  | | --- | --- | | **Sender** | CEO | | **Subject** | Cybersecurity incident | | **Body** | Dear valued customers,  We respect the privacy of your personal information and are, therefore, contacting you to advise you of a cybersecurity incident that resulted in the possible disclosure of your personal data by unauthorized parties.  **What happened?**  [Enter known details of incident here, including how the breach occurred (e.g., phishing attack); date that you became aware of the incident; and what data was accessed.]  For example:  On March 24, 2023, we became aware that our systems had been accessed by unauthorized parties. A staff member clicked a link within a phishing email and then divulged their username, password and second-factor authentication code. The attacker then used this information to access internal systems, including databases containing names, addresses and order details of our customers.  **How did we respond?**  [Enter details of steps you have taken to contain and investigate the incident. Provide reassurance that the incident is being handled professionally.]  For example:  The staff member reported the incident shortly after divulging their credentials, and our security team took steps to revoke access and isolate any affected IT systems. We are continuing to monitor the situation closely and are engaging with third-party experts to continue the investigation.  I want to assure you we are doing everything in our power to safeguard our systems and data. We have already implemented additional security measures, and we will continue to take all necessary steps to prevent future incidents.  **What should you do?**  In line with good practice, we are advising you to change your password on our website and any other website where you may have been using the same password. We ask that you remain vigilant to any suspicious activity or emails.  We are very sorry for the inconvenience and concern this may cause. We have contacted the police and relevant regulatory authorities and will be assisting them in their investigations.  Kind regards,  [CEO name]  For further information, please contact us at [phone number] or [email address]. | | |