# Develop an Incident Response Communication Plan

Project by: **D. James Chrishan**

## 1. Purpose and Objectives

The purpose of this Communication Plan is to ensure that accurate, timely information is provided to all relevant stakeholders in the event of a cybersecurity incident. By coordinating communication efforts, this plan seeks to:

- Limit misinformation and prevent reputational damage.
- Support efficient incident response and recovery.
- Comply with legal and regulatory obligations.

The primary objectives are:

- To deliver clear, accurate information to stakeholders promptly.
- To coordinate internal and external communication effectively.
- To maintain trust by transparently sharing updates and incident resolutions.

## 2. Stakeholders and Communication Channels

**Internal Stakeholders**

1. **Executive Management**
   - **Purpose**: High-level updates and decision-making support.
   - **Channel**: Email, conference calls, dedicated incident response app.
2. **Incident Response Team**
   - **Purpose**: Real-time updates, actions, and coordination.
   - **Channel**: Secure chat (e.g., Slack), video calls, email.
3. **IT & Security Staff**
   - **Purpose**: Technical details and instructions.
   - **Channel**: Internal communication tools, SMS for urgent alerts.
4. **Employees**
   - **Purpose**: Inform about impact and behavioral guidelines.
   - **Channel**: Email, intranet, secure employee portal.

**External Stakeholders**

1. **Customers**
   - **Purpose**: Transparency about data integrity, reassurance.
   - **Channel**: Email, website announcements, customer support line.
2. **Partners and Vendors**
   - **Purpose**: Notify about impacts on shared systems or data.
   - **Channel**: Email, phone calls, secure portals.
3. **Regulatory Bodies**
   - **Purpose**: Comply with mandatory breach notifications.
   - **Channel**: Email, secure online portals, official documentation.
4. **Media and Public**
   - **Purpose**: Manage reputation and provide public updates.
   - **Channel**: Press releases, social media, website updates.

## 3. Communication Protocols

**Initial Notification Protocol**

- **Trigger**: Incident identification and preliminary assessment.
- **Content**: Nature of the incident, potential impact, and initial response steps.
- **Responsibility**: Incident Response Lead.
- **Timeframe**: Within 1 hour of detection for critical incidents, within 4 hours for others.

**Status Update Protocol**

- **Frequency**: Every 4 hours for critical incidents, daily for ongoing low-impact incidents.
- **Content**: Status, actions taken, new developments, anticipated next steps.
- **Responsibility**: Incident Response Coordinator.
- **Channels**: Adjusted per stakeholder group as mentioned above.

**Incident Resolution Communication**

- **Content**: Summary of the incident, actions taken, impact assessment, preventive measures.
- **Responsibility**: Chief Information Security Officer (CISO).
- **Timeframe**: Within 24 hours of resolution for critical incidents, within 48 hours for others.

- **Escalation**: If an incident intensifies, escalate notifications to the Executive Management Team and initiate regulatory body notifications if required.

**Escalation Procedures**

- **Low Impact Incidents**: Incident Response Team manages communication internally, with periodic updates to Executive Management.
- **Moderate Impact Incidents**: Notify all internal stakeholders, begin preliminary communications with regulatory bodies if data exposure is detected.
- **High Impact Incidents**: All stakeholders notified, escalation to external communication with customers, partners, media, and regulatory bodies.

## 4. Message Templates

**Template 1: Initial Notification**
*Subject: Important Notice: [Incident Type] Detected*

Dear [Employee/Customer/Partner],

We want to inform you that a cybersecurity incident involving [general description of data/system] was detected on [date and time]. Our team is actively investigating and taking steps to resolve the situation. At this time, we recommend [guidance, e.g., changing passwords, disconnecting affected devices, etc.].

Please rest assured we are committed to addressing this matter swiftly and will keep you informed of further developments.

Best regards,
[Incident Response Lead’s Name & Position]

**Template 2: Status Update**
*Subject: Update on [Incident Type] Incident*

Dear [Employee/Customer/Partner],

We are reaching out to update you on the cybersecurity incident reported on [date]. We have [describe actions taken, e.g., isolated affected systems, begun forensic analysis, etc.]. Our response efforts are ongoing, and we are working diligently to protect your information and restore normal operations.

We will provide another update by [next update time]. Thank you for your patience and understanding.

Best regards,
[Incident Response Coordinator’s Name & Position]

**Template 3: Incident Resolution Notification**
*Subject: Incident Resolved: [Incident Type] on [Date]*

Dear [Employee/Customer/Partner],

We are pleased to inform you that the recent cybersecurity incident has been resolved. After thorough investigation and remediation, we have [describe actions taken and safeguards implemented]. We do not anticipate further impact. We are committed to preventing future incidents and continuously enhancing our security.

If you have any questions or concerns, please contact us at [support contact information].

Thank you for your cooperation.

Sincerely,
[Chief Information Security Officer’s Name & Position]