Template # 1 (CISO - Internal Communication)

## Subject: CISO Alert - Immediate Incident Response Update

**Incident Status: High Severity**

Team,

A critical cybersecurity incident has been identified. Our security systems detected unauthorized network access originating from a sophisticated phishing campaign. An employee's compromised credentials allowed the attacker to move laterally and access several databases. Our security team detected the activity and initiated containment protocols immediately.

**What Was Affected:** Our forensic analysis indicates the breach impacted:

- **Customer Database:** A subset of customer information, including names, email addresses, and encrypted passwords. **No financial information was accessed.**
- **Employee Records System:** Employee names and company email addresses. **No personal data was accessed.**
- **Internal Source Code Repository:** Limited access to some repositories, with the full scope still under investigation.

**Actions We Are Taking:** Our incident response team, supported by external cybersecurity experts from [External Firm Name], is working around the clock. Immediate actions include:

- **Containment:** Compromised accounts are disabled and affected servers are isolated.
- **Eradication:** We are removing the threat and patching vulnerabilities.
- **Forensic Investigation:** A full investigation is underway to determine the complete scope of the breach.

**Next Steps & Your Role:**

- **All employees must change their passwords immediately** via the password portal at [Internal Password Reset URL]. Do not reuse old passwords.
- **IT and Engineering teams, refer to the Incident Response Plan (IRP)** at [Document Link]. Stay alert and report suspicious activity to [Internal Security Email].
- We will provide updates every [Frequency, e.g., 2 hours] via [Communication Channel].

This is a difficult moment, but our coordinated efforts will ensure a swift and thorough recovery. Thank you for your professionalism and focus during this time.

Sincerely,

[CISO Name] Chief Information Security Officer

Template # 2 (CEO - Internal Communication)

## Subject: An Important Message from [Company Name] CEO

Team,

I am writing to you today to confirm that [Company Name] has experienced a cybersecurity incident involving unauthorized access to our network. I want to be upfront and transparent with you about this situation.

**What Happened:** Our team detected and has been actively responding to a security breach. We believe the incident began with a phishing attack that compromised an employee's credentials. This led to unauthorized access to a portion of our data. I want to assure you that our team took immediate action to contain the threat.

**Who Was Affected:** The incident affects certain internal and customer data. Please be aware that a subset of customer information and some internal employee details were accessed. We are working diligently with leading cybersecurity experts to determine the full scope.

**Actions We Are Taking:** The security and privacy of our data is our top priority. We have taken the following immediate steps:

- **Containment:** The threat has been contained, and the compromised systems have been isolated.
- **Investigation:** We have engaged a team of world-class forensic experts to conduct a comprehensive investigation.
- **Restoration:** We are working to restore any affected systems and enhance our security protocols to prevent future incidents.

**Our Commitment to You:** We understand that this news is concerning. Our teams are working tirelessly to resolve this issue, and we will keep you informed with regular updates. In the coming days, you will receive more specific guidance from the CISO and CIO on your role in this recovery.

Thank you for your cooperation and for your commitment to our company's security. It is in moments like these that our collective strength and resolve truly shine.

Sincerely,

[CEO Name] Chief Executive Officer

Template # 3 (CIO - Internal Communication)

## Subject: CIO Update: Incident Recovery Plan & IT Status

IT Team,

Following the CISO's update, here is our roadmap for recovery. Your work is critical to getting our systems back online securely and efficiently.

**Operational Impact:** Due to containment protocols, the following systems are offline or have limited functionality:

- [System 1]: [Reason for outage, e.g., "for forensic imaging and cleaning"]
- [System 2]: [Reason for outage, e.g., "access disabled to prevent further compromise"]
- [System 3]: [Reason for outage]

**Recovery Actions & Timeline:** We are executing a phased recovery plan. Your team leads will assign tasks based on these priorities:

1. **Immediate (24-48 hours):** Complete forensic imaging of affected servers and begin phased restoration of core infrastructure.
2. **Short-Term (3-5 days):** Restore essential business applications, with a focus on enhanced authentication and access controls.
3. **Mid-Term (1-2 weeks):** Restore all non-critical systems, finalize post-mortem analysis, and implement long-term security enhancements.

**New Security Protocols:** During this phase, we are implementing new security protocols:

- **Multi-Factor Authentication (MFA) is now mandatory for all systems.**
- **All administrator accounts must be audited and reset.**
- **Increased logging and monitoring of critical systems.**

Your expertise is essential. Refer to the detailed recovery plan at [Document Link] for assignments. Report any roadblocks to your team lead immediately.

We will hold a daily stand-up at [Time] to review progress.

Thank you for your hard work and dedication. Let's get our systems secure and our company back to full strength.

Best,

[CIO Name] Chief Information Officer

Template # 4 (CEO - External Communication)

## Subject: An Important Message Regarding a Data Security Incident at [Company Name]

To Our Valued Business Partners and Clients,

I am writing to you today with an important update regarding a data security incident at [Company Name]. We recently detected and took immediate action to address unauthorized access to a portion of our systems.

**What Happened:** Our team discovered that an unauthorized third party gained access to our network. Upon this discovery, we immediately took steps to contain the incident, including isolating the affected systems. We have also engaged a leading cybersecurity forensics firm to conduct a thorough investigation and fully understand the scope of the incident.

**Who Was Affected:** While our investigation is ongoing, we can confirm that the unauthorized access resulted in the potential exposure of a limited set of client data. This may include business contact names and email addresses. We can confirm that no sensitive financial data, such as credit card numbers or bank account information, was compromised, and our core business operations were not impacted.

**Actions We Are Taking:** The security of the data you have entrusted to us is our highest priority. We are treating this matter with the utmost seriousness. In addition to our ongoing investigation, we are taking the following steps to protect your data and prevent this from happening again:

- We have notified law enforcement and relevant regulatory bodies.
- We are enhancing our security infrastructure and access controls.
- We are providing a direct communication channel between our security teams to ensure full transparency and coordination.

We will continue to post updates on this matter on our dedicated page at [Public-facing URL]. We apologize for any concern this may cause and appreciate your partnership as we work to resolve this issue.

Sincerely,

[CEO Name] Chief Executive Officer

Template # 5 (Chief Customer Officer - External Communication)

## Subject: Important: An Update from the Chief Customer Officer at [Company Name]

To Our Valued Partners and Clients,

As our Chief Customer Officer, I am reaching out to you directly to provide more information about the security incident at [Company Name] and to tell you what steps we are taking to protect your business and data.

**Our commitment to you is clear: The security of your data is our priority.**

As the CEO's message explained, our company has been the subject of a security incident. We can now confirm that a limited set of shared business data may have been affected, specifically your company's business contact names and email addresses. We want to be perfectly clear: your financial information or operational data was not compromised.

**What We Are Doing to Help You:** We are working diligently to protect you and your business. We recommend the following immediate actions and a path for coordination:

- **Internal Review:** As a best practice, please conduct an internal review of your systems for any unusual activity.
- **Be Vigilant:** Advise your team to monitor for any suspicious emails or communications.
- **Contact Us:** We have set up a direct line for our security teams to communicate with yours. If you have any questions or require more technical details, please contact us at [Dedicated Phone Number] or [Dedicated Email Address].

We know that this situation is concerning, and we sincerely apologize for any worry this may cause. We are working around the clock to ensure our systems are secure and your information is protected. We will continue to be transparent and provide updates as they become available at [Public-facing URL].

Thank you for your understanding.

Warmly,

[CCO Name] Chief Customer Officer