# Security Incident Response Interdepartmental Communications Template

Use this template to help streamline internal communication between Security Incident Response Communications Team members. It can be used as an aid during face-to-face interaction or as a means to facilitate communications between team members when they cannot all be in the same place.

# Introduction: How to Use This Template

To use this template, simply replace the text in dark gray with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Overview

|  |  |
| --- | --- |
| Incident type | [e.g. ransomware, DDoS attack, stolen data, etc.] |
| Date and time incident was discovered | [e.g. 06/06/18 at 1430] |
| Date incident was reported | [e.g. 06/09/18]  **Reason for delay: [e.g. email not working]** |
| Security Incident Response Communications Team Members (SIRCT) | [e.g. John Jones, IT Advisor  Yoko Young, IT Deputy  Paul Pauls, Legal Council  George Georges, HR Representative  Ringo Rings, Communications Coordinator  Pete Peters, Communications Deputy]  [Be sure to note if one or more member is an alternate] |
| Primary contact methods for SIRCT members | [e.g. John Jones: jjones@beatlecorp.com / 555-555-5000 ext. 500, etc.] |
| Secondary contact methods for SIRCT members | [e.g. John Jones: SIRCT1@free-email.org, etc.] |

# Status Report (to be completed by the IT Advisor)

Use this section to report on the remediation effort during the incident. This is not meant to be a comprehensive report, so include only the most essential details that the Security Incident Response Communications Team (SIRCT) members and executives will need to know to understand where the organization presently stands in the remediation process.

E.g.

* Ransomware has been contained.
* 56 computers are still infected.
* All employees advised not to turn on computers.
* Required regulatory reporting complete.

# Challenges Ongoing (to be completed by the IT Advisor)

Use this section to track the challenges your organization faces during the remediation effort. Be sure to track each challenge and the date it is resolved, as this information can be used during the SIRCT’s post-incident review to better anticipate the kinds of challenges they may face in the future.

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Impact | Recommendations | Resolved |
| Phones offline | Communication difficulties | Employees to use cell phones |  |
| Email unavailable | Communication difficulties | SIRCT to use alternate communications method |  |
| Files encrypted | No access to company data | Consult third-party specialist to help remediation |  |
| Regulatory reporting | Legal liability | Have SIRCT report ASAP | 06/10/18 |

# SIRCT Members’ Reports (to be completed by one member from each department)

Use this section to communicate, in plain language, the essential details of the incident that each branch of the SIRCT should be aware of. (See examples below.)

### IT Report

Data breach of approximately 1,200 users’ personal data, including names, addresses, email addresses, and payment card information. All of this data was encrypted, but a flaw is suspected in our encryption protocol, so the true extent of the breach is not yet known. It also appears employees with last names beginning with the letters L through R have had personal data exposed.

**Updates:**

* 08/10/18 encryption flaw confirmed for approximately half of the breached accounts.

### Legal Report

Our company holds data on European Union citizens; it is therefore required to report the incident to the appropriate supervisory authority within 72 hours, and we must notify affected stakeholders without undue delay in order to comply with the GDPR. Legal exposure is high, given the encryption failure.

**Updates:**

* 08/12/18 State law requires us to make a media statement regarding the issue, as per HIPAA.

### PR Report

Holding statement confirming that an incident occurred has been drafted and is pending approval by the SIRCT. Recommended action: make a public statement expressing accountability and empathy. Even if few details are available, a press release should be drafted to outline what we know so far and what we are doing to address the issue. PR presently needs more information to make a proper press release.

**Updates:**

### HR Report

The potentially affected employees have been notified and advised that HR can answer any additional questions and that the company will support them through any difficulties that arise due to the breach.

**Updates:**

### Points to Clarify

Use this section to request clarification or to ask questions about any of the SIRCT members’ reports above.

E.g.

**08/12/18 – Legal to IT:** Were we at fault for the encryption flaw?

**08/13/18 – IT to Legal:** It appears to be a flaw in the encryption software we use, but the investigation is not complete.

### Communications Series

|  |  |  |
| --- | --- | --- |
| Date of update | Date of next update | Reviewed by |
| [e.g. 06/09/18] | [e.g. 06/14/18] | [signatures of SIRCT members] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Sources:** inspired by Cisco’s Incident Response Communications Template.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.