

WHITE PAPER · OCTOBER 2026

# Internal **crisis** communication

**Be ready before the alert**

Cyberattack, accident, severe weather, labor or media crisis: the plan, channels, message templates and checklist to inform every employee within minutes.

---

**6 scenarios**

of crisis to anticipate

---

**5 templates**

of messages ready to adapt

---

**20 points**

to be ready before the alert

# In a crisis, you communicate only as well as you prepared.

A crisis gives no warning. A cyberattack on a Monday morning, an incident on site on a Friday evening, a storm the night before a new hire starts: in the first minutes, the question is always the same. How do you reach everyone, fast, with the right message?

Employees are the first affected. They need to know what is happening, what is expected of them, and whether they are safe. They are also the first to talk: to family, to customers, on social media. If the company stays silent, rumor fills the gap.

Good internal crisis communication is never improvised. It relies on **a simple plan, channels that keep working even when IT systems go down, and messages prepared in advance**. This white paper gives you what you need to build all of this, and shows how the We Advocacy platform helps you reach every employee, in the field and in the office.

**Thomas Artiguebaille**

President and Co-founder, We Advocacy

## CONTENTS

|           |                                                        |       |
|-----------|--------------------------------------------------------|-------|
| <b>01</b> | <b>Why internal communication is on the front line</b> | p. 3  |
| <b>02</b> | <b>The internal crisis communication plan</b>          | p. 4  |
| <b>03</b> | <b>The first hours, minute by minute</b>               | p. 5  |
| <b>04</b> | <b>Alert everyone, on the right channel</b>            | p. 6  |
| <b>05</b> | <b>Five message templates</b>                          | p. 7  |
| <b>06</b> | <b>After the crisis: reassure, thank, learn</b>        | p. 8  |
| <b>07</b> | <b>The “ready before the alert” checklist</b>          | p. 9  |
| <b>→</b>  | <b>We Advocacy at a glance</b>                         | p. 10 |

# Why internal communication is on the front line

In a crisis, we think first of the press and customers. Yet everything plays out internally first: team safety, business continuity, and how the company will be seen from the outside.

## PROTECT

Evacuate a site, close off an area, tell people not to come in: some information is a safety matter and must arrive within minutes.

## ORGANIZE

Who works, where, how? Without clear instructions, each team improvises and operations fall apart.

## CONTAIN

A poorly informed employee spreads rumors. An informed employee becomes a reliable messenger, with customers and family alike.

## Six scenarios to anticipate



### Cyberattack

Email and internal tools down, urgent IT security instructions.



### Accident or on-site incident

Evacuation, restricted area, informing teams and families.



### Severe weather

Snow, flood, storm: site access, schedules, remote work.



### Health crisis

Protective measures, work organization, long-term follow-up.



### Media crisis

A story gaining traction in the press or on social media before teams are informed.



### Major outage

Power, network, business tool: instructions for degraded operations.

**The cyberattack trap.** It is the scenario where you most need to communicate, and the one where usual channels fail first: email, on-premise intranet, IP telephony. Your plan must include channels independent of your IT systems.

**"Am I safe?"**

**"What should I do, right now?"**

**"When will I know more?"**

The three questions every employee asks in the first minutes. Every message must answer them.

# The internal crisis communication plan

An effective plan fits in a few pages. It doesn't try to foresee everything: it sets who decides, who speaks, on which channels, and with which starting messages.

1

**A crisis team and roles**

Who triggers, who approves, who writes, who sends. With a backup for each role: crises happen during vacations too.

2

**A short approval chain**

Two people at most to approve an urgent message. Any more, and the news arrives after the rumor.

3

**Up-to-date distribution lists**

By site, job and team, with phone numbers for those without email. An outdated list means forgotten employees.

4

**Backup channels**

At least one channel hosted outside your IT systems, accessible from a phone, and tested.

5

**Pre-written messages**

One template per scenario, completed in minutes rather than written under pressure.

6

**Regular drills**

At least once a year, a real alert drill: it always reveals a missing number or a forgotten access.

## Will your channels survive a cyberattack?

| CHANNEL                              | AVAILABLE IF IT IS DOWN                 | REACHES THE FIELD |
|--------------------------------------|-----------------------------------------|-------------------|
| Internal email                       | No, often the first to go               | No                |
| On-premise intranet                  | No                                      | Rarely            |
| Personal messaging groups            | Yes, but no control or up-to-date lists | Partly            |
| SMS sent from an external platform   | Yes                                     | Yes               |
| Mobile app hosted outside IT systems | Yes                                     | Yes               |

**WITH WE ADVOCACY****A ready-to-use alert system, kept up to date automatically.**

**Directory synced** from Entra ID, Okta, Google Workspace, SAP SuccessFactors or by file: lists are always up to date.

**Platform hosted outside your IT systems**, in Europe on Google Cloud: a channel that stays up if your email goes down.

**Publishing rights by scope:** the crisis team and site directors know who can send what, to whom.

# The first hours, minute by minute

In the first hours, the rule is simple: speak fast, even without all the facts, then give updates at regular intervals.

H0

**TRIGGER****Activate the crisis team**

The designated lead triggers the plan and convenes the team, remotely if needed.

+15

**FIRST MESSAGE****Inform those affected**

A short, targeted message on the fastest channels: what is happening, the immediate instruction, when the next update will come.

+30

**CHECK****Make sure everyone received it**

See who has read it, follow up with the others on another channel, ask those affected to confirm their status.

+1h

**EXPAND****Inform all employees**

Before the news arrives via the press or social media. Give managers what they need to answer questions.

+4h

**KEEP THE PACE****Provide regular updates**

At set times, even with nothing new: silence fuels anxiety.

**THE FOUR-QUESTION RULE**

Every crisis message answers four questions:

- 1 **What we know**, without speculating.
- 2 **What we don't know yet**, and saying so.
- 3 **What we are doing**, and what we expect from you.
- 4 **When the next update will be.**

**✓ Do**

- Short sentences, clear instructions
- One official source, cited everywhere
- Inform teams before the outside world

**✗ Don't**

- Wait until you have all the facts
- Downplay or speculate on causes
- Let each manager improvise their message

## Alert everyone, on the right channel

In a crisis, one channel is never enough. You must reach offices, the field, remote workers and those on leave at the same time, then know who received it.

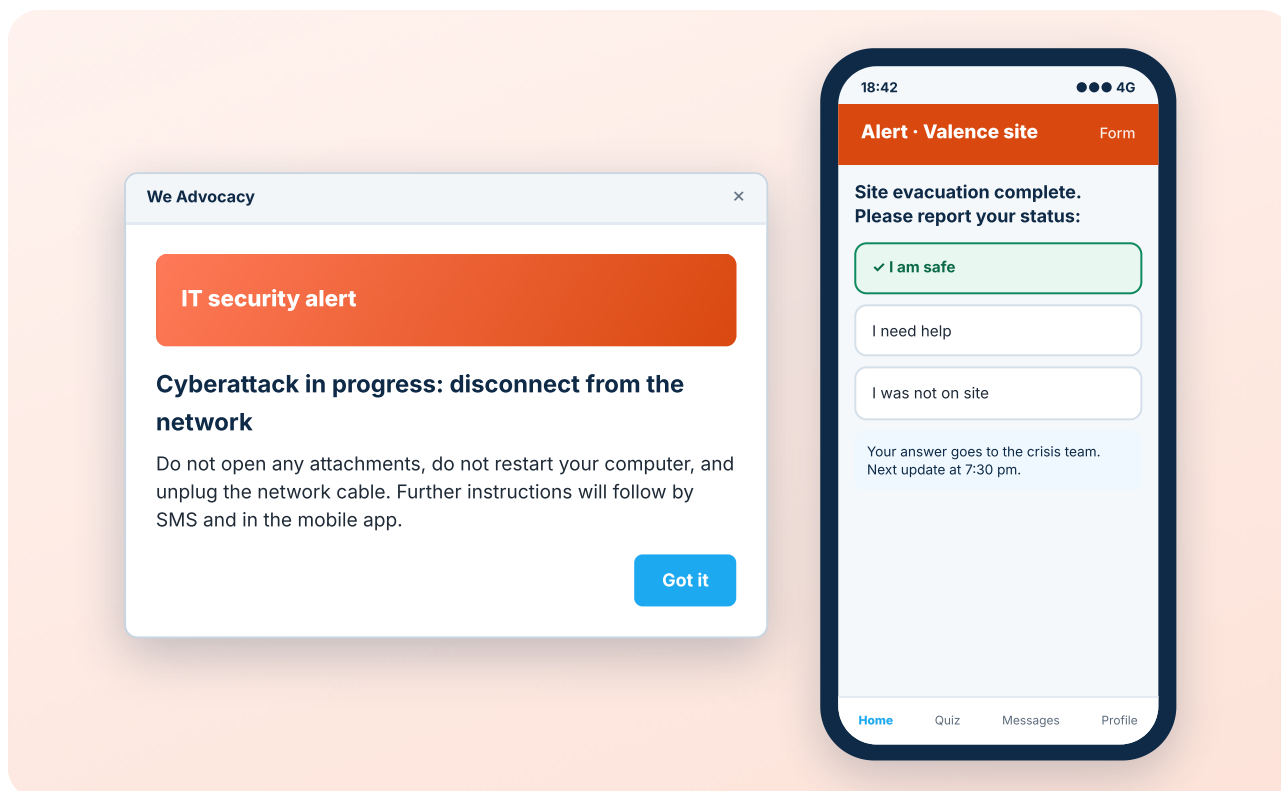


Illustration: a Windows pop-up during a cyberattack, and a status form after an evacuation.

### Channels to combine by scenario

| SCENARIO         | FIRST MESSAGE                       | FOLLOW-UP               |
|------------------|-------------------------------------|-------------------------|
| Cyberattack      | Windows pop-up, then SMS            | Mobile app, SMS         |
| On-site incident | SMS and notification, affected site | Status form, app        |
| Severe weather   | SMS the day before, next-day teams  | App, email              |
| Media crisis     | Email and pop-up, all employees     | Intranet, FAQ, managers |

- One send, five channels: Windows pop-up, mobile notification, SMS, email, intranet.
- The Windows pop-up appears on screen, even if email is closed or unavailable.
- SMS and the mobile app reach frontline teams, remote workers and those who are away.
- Targeting by site, job or entity avoids alarming those not affected.
- Forms collect everyone's status in seconds.
- Statistics show who has read in real time, and reminders go out on another channel.

## Five message templates

Prepare these messages in advance, get them approved ahead of time, and save them as templates. On the day, you'll only need to fill in the bracketed items.

### CYBERATTACK · POP-UP AND SMS

"IT security alert. Our systems are under attack. Right now: do not restart your computer, unplug the network cable, do not open any suspicious email. Email has been shut down as a precaution. Next update by SMS at [time]."

### ON-SITE INCIDENT · SMS AND APP

"Incident at the [site] site. The site has been evacuated and emergency services are on site. Go to assembly point [location] and report your status in the app. Do not post on social media. Next update at [time]."

### SEVERE WEATHER · SMS THE DAY BEFORE

"Weather alert for [area] tomorrow. Morning teams at [sites] start at [time]. If you cannot travel safely, let us know in the app before [time]. Your safety comes first."

### END OF CRISIS · ALL CHANNELS

"The situation is back to normal at [scope]. [What resumes, and when.] Thank you all for your quick response. A full update will be shared on [date]. Questions: [contact]."

### MEDIA CRISIS · EMAIL AND POP-UP, BEFORE THE PRESS

"You may read or hear news today about [topic]. Here is what we know: [facts]. Here is what we are doing: [actions]. If a journalist contacts you, please refer them to [press contact]. You will hear from us first, before any external communication."

## Writing rules in a crisis

### SHORT

The key message must fit in an SMS. Details follow in the app or on the intranet.

### ACTIONABLE

Lead with the instruction: what everyone must do, now.

### HUMAN

A calm, direct tone. People's safety comes before everything else.

**With We Advocacy:** save your standard messages as templates, ready to complete and send in a few clicks on the channels and to the audience of your choice.

## After the crisis: reassure, thank, learn

A crisis doesn't end when the emergency subsides. How the company comes out of it, explains, thanks and learns lessons has a lasting impact on team trust.

### REASSURE

Clearly announce the return to normal, what has changed, and who to ask questions.

### THANK

Recognize the teams' efforts, by name when possible, in the newsletter and from leadership.

### LEARN

Ask employees: did the information arrive in time, was it clear?

#### Post-incident review · Cyber alert

Report

**96%**

reached in 30 min

**12 min**

median time to read

**4.1 / 5**

perceived clarity

#### SHARE OF EMPLOYEES REACHED IN 30 MINUTES

|                    |                        |     |
|--------------------|------------------------|-----|
| Head office        | <div><div></div></div> | 99% |
| Production sites   | <div><div></div></div> | 95% |
| Branches           | <div><div></div></div> | 93% |
| Employees on leave | <div><div></div></div> | 61% |

✦ **AI analysis:** the pop-up was the fastest channel at head office, SMS on sites. Employees on leave were the least reached: add their phone numbers to the directory before the next drill.

Illustration with fictitious data: the report serves as the basis for the post-incident review.

**With We Advocacy:** statistics by channel and population, **AI reports** for the post-incident review, a post-crisis **survey** in minutes, and an AI-assisted thank-you **newsletter**.

# The “ready before the alert” checklist

Twenty points to check today. If you can tick them all, you're ready.

## ORGANIZATION

- ☐ The crisis team and its backups are designated
- ☐ The approval chain has two people at most
- ☐ Site directors know what they can send on their own
- ☐ The plan fits in a few pages and is accessible offline
- ☐ Managers know what to tell their teams

## CONTACTS

- ☐ The directory is synced automatically
- ☐ Phone numbers are on file for everyone, frontline included
- ☐ Temp workers and contractors on site can be reached
- ☐ Lists by site, job and team are ready
- ☐ Consent and data use are documented

## CHANNELS

- ☐ At least one channel is independent of your IT systems
- ☐ SMS, mobile and pop-up are enabled and tested
- ☐ The crisis team can send from a phone
- ☐ A backup login method is in place
- ☐ You can measure who received it and remind the rest

## MESSAGES AND DRILLS

- ☐ A message template exists for each scenario
- ☐ Templates are approved by leadership and legal
- ☐ A status form is ready to use
- ☐ An alert drill took place in the last twelve months
- ☐ The last post-incident review led to actions

### ANNUAL DRILL

Once a year, send a drill message to all employees, on all channels, with a “Received” form. In one morning, We Advocacy tells you who can be reached, on which channel, how fast, and who is missing.

#### 9 AM

Drill message sent on all channels, with the “Received” form.

#### 10 AM

Automatic reminder to non-respondents on another channel.

#### 12 PM

AI report: reach rate by population and list of contacts to complete.

# The multichannel internal communication platform. Designed in France, hosted in Europe.

**200+**

client companies since 2018

**100,000**

users every day

**5 channels**

from a single send

- ◉ **Integrated with your environment:** Google Workspace, Microsoft 365, SSO, directory sync from Entra ID, Okta, Google Workspace or SAP SuccessFactors.
- ◉ **Modular:** start with the modules you need today, add others with no migration.
- ◉ **Secure and GDPR-compliant:** Hosted in Europe on Google Cloud, data encrypted in transit and at rest.
- ◉ **Supported:** guided rollout, France-based support, unlimited number of communicators.

*"We Advocacy has helped us unify our communications for several years. We particularly appreciate their responsiveness and efficiency."*

Mary Pifer, VP Marketing, 3SI

## See what the platform can do for you.

In 30 minutes, we start from your audiences and tools to show you the modules that matter, and only those.

**Book a demo →**

weadvocacy.fr · contact@weadvocacy.com · +33 7 82 72 97 28 · 10 chemin du Renevier, 38700 Corenc

### Sources

We Advocacy, platform feature descriptions. Message templates should be adapted and approved within your organization; screen mockups are illustrations and the data shown is fictitious.