Public communications for cyber security incidents

A framework for organizations

Created and published by the FIRST Cybersecurity Communications Special Interest Group.

Contents

Acknowledgements

***"Effective communication following a cyber security incident forms a critical element of the activities needed to protect your company's customers, stakeholders, and reputation more generally."* – Richard Knight and Jason Nurse.**

The original version of this framework was based on the work of Richard Knight (University of Warwick) and Jason Nurse (University of Kent) [1].

It was refined by CERT NZ using information from interviews conducted with New Zealand-based organizations that had been the target of cyber security incidents. I would like to thank them again for sharing their experiences.

The report was internationalized for FIRST using examples taken from various national CSIRTs. It was then edited and refined by the FIRST Cybersecurity Communications Special Interest Group (SIG).

[1] *A Framework for Effective Corporate Communication after Cyber Security Incidents*, Richard Knight and Jason R. C. Nurse, 2020

About this Framework

This is a guide for an organization to create a plan for public-facing communications in the event of a cyber incident.

The Framework gives a way of formalising and constructing decision-making on when to communicate, with whom and at what level, as part of an overall incident response plan.

International version

The first version of this framework was created for New Zealand as part of CERT NZ's advice for organizations. Subsequently it has been adopted by many international organizations and, as such, an internationalized version was required.

This is a living document, which means it will be updated and adapted as required for various audiences. Each major revision will be given a new version number. (See Appendices for revision changes.)

This document is written in US English.

Basic structure

The framework follows this construction.

- Roles and responsibilities of responders.
- Decisions on the type of incident and how to respond.
- How to create and disseminate communications for greatest effect.
- Post-incident work.

Examples are given throughout and supplementary materials – such as templates and exercises – can be found in the Appendices.

Examples are formatted like this to distinguish them from body text.

Roles and Responsibilities

This section covers the steps to take when an incident has started or you receive a report of an incident[2] that you are in control of. The roles and responsibilities of team members should be determined well ahead of time and listed in your overall incident response plan.

Communications lead

The **Communications Lead** (Comms Lead) will be aware of all communications between internal teams or out to external stakeholders. This includes executive teams, government officials, media, the public and any other stakeholders.

This role is essential to ensure a clear understanding of which groups have which pieces of information.

Choosing a Comms Lead

- **The Comms Lead does not have to be a communications expert.**
- **You can have two leads for internal and external communications.**

While it is preferable for the Comms Lead to have some communications skills, it is not a necessity. However, the creation of clear, pre-agreed response plans means the Comms Lead can be from any area. External incident response teams (including national CSIRTs) should be able to offer communications assistance for the creation of messages.

The Comms Lead does not necessarily need to be making decisions about the content of the communications or see every email or text message but they will need to know the communication has happened.

Depending on organizational structure, the Comms Lead may not be the final sign-off for certain communications. For example, a formal letter to a government Minister may require CEO or executive level sign-off. However, the Comms Lead will ensure all required edits and changes are made before sending to that final level.

Similarly the role can be split across functions. For example, external communications could be run by a communications expert while internal communications could be run by HR.

In terms of incident response chain of command, the Comms Lead usually sits at the same level as technical response and logistics leads, reporting directly to the Incident Response Coordinator.

Comms Lead responsibilities *before* the incident

- Understanding all of the formally required communications should an incident occur[3].
- Managing a list of known stakeholders and the preferred method of contact.

[2] In this context an “incident” means any cyber security issue that requires a response.
[3] See section on Responsibilities

- Managing a secondary mode of wide-band communication for internal staff should normal communications be unavailable (such as a Signal group or text messages).
- Maintaining a set of 'standing lines' that can be sent to stakeholders and internal staff, if required[4].
- Managing the members of the organization who will be spokespeople, should the need arise – this includes ensuring they have adequate training and support for that responsibility.

Comms Lead responsibilities *during* the incident

- Clear knowledge of which stakeholders have which pieces of information.
- Altering the communications approach as the incident changes over time.
- Sign off on wide communications to stakeholders (for example, an email to all customers).
- Reporting to Incident Response Coordinator.
- Managing incoming communications.
- Monitoring media and social media (if required).

Who are your stakeholders?

Stakeholders is the term we use to refer to anyone with a connection to the organization.

An example of a basic list of stakeholders.

Internal stakeholders

- Staff
- Contractors
- Vendors
- Shareholders

External stakeholders

- Customers/members
- Government agencies (including law enforcement)
- Governing bodies or regulators.

The list of stakeholders will be determined what type of incident has occurred. It can be as broad as everyone who has contact with the organization or as few as internal staff.

As part of creating your communications response framework we recommend doing an audience mapping exercise to determine who your audiences are on a normal basis and the best ways to communicate with them.

A guide for this exercise can be found in the appendices.

Decisions

The Comms Lead needs to make the following decisions throughout the incident.

[4] Standing lines are explained further into the document.

- **What information needs to be communicated and when?**
- **What regulatory disclosures need to be made?**
- **Which audiences need which pieces of information?**

They may not be able to answer these immediately and as such will require information updates during the incident.

Info gathering

The Comms Lead needs the following information as soon as possible. This can come from the wider Incident Response (IR) team or as part of the Comms Lead's monitoring role.

- What type of incident is it?
- Who is affected? (Clients, public, specific agencies etc)
- How widespread is the incident? (Localized, industry specific, regional, national, international etc)
- Is there an immediate impact on clients, agencies or the public?
- Is the risk level increasing over time? / Has the incident been contained?
- Is the incident being reported by the public/journalists/experts in media/social media?
- Are reports being made from clients/users to your organization?
- Has the organization been contacted by the attacker? / Has the attacker made themselves known publicly?

What you don't know is sometimes as important as what you do.

At the start of an incident, it is likely some of these pieces of information will be unknown, and that should be noted as well. As the incident progresses more information may be added that will affect your decisions.

What information needs to be communicated and when?

The matrix below is used to determine a communications response to an incident. Each of the four quadrants – based on risk to stakeholders vs visibility – has a different communications approach. These quadrants and how best to approach each one, are outlined in the Order of communications section below.

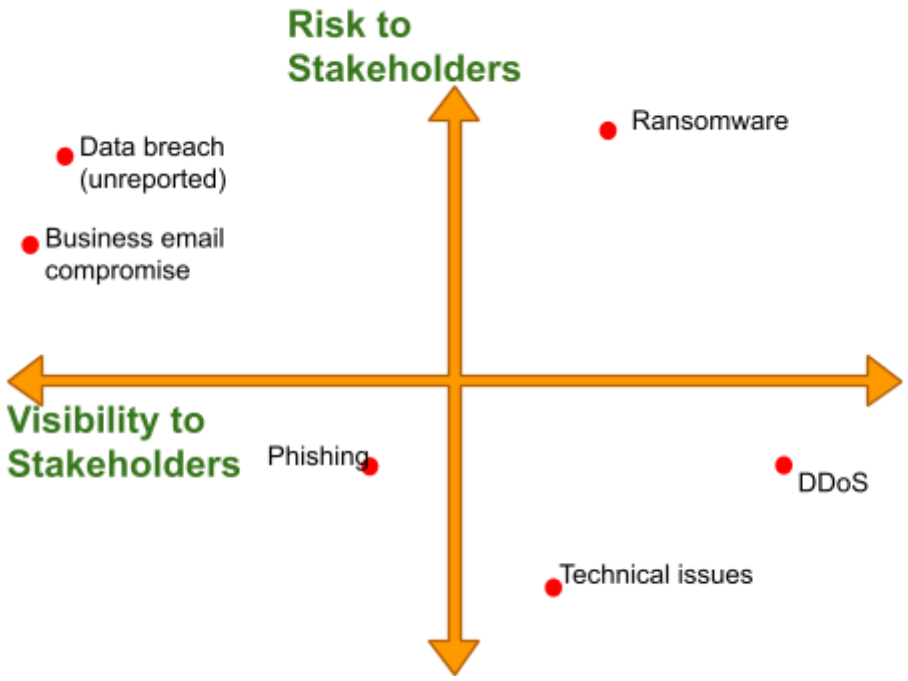

Figure 1: Stakeholder risk vs visibility matrix for cyber incidents with example incidents

The information gathered by the Comms Lead in the initial stages of incident response allows them to place the incident into the matrix. This is not an exact science and it's a good idea for the Comms Lead to agree on the placement with other response team leads.

Responsibilities

Disclosures to Police, financial organizations, government agencies, and oversight groups may need to be done immediately.

These steps could already be part of the standard incident response plan and may not require your communications team. However, the Comms Lead should be aware of what has been reported and where. This information may be used in communications with stakeholders.

Applicable laws

There will be laws and policies that your organization or the affected organization will have to comply with during an incident. This may include mandatory reporting to government or law enforcement.

The Comms Lead should have contacts at all of the organizations with applicable laws.

Privacy:

Many countries have laws covering data protection and information privacy. If you are involved in a data breach or other incident where data has been exposed, then you need to be aware of the exact wording of these.

This is an example of the New Zealand government's Privacy Act.

"Under the Privacy Act 2020, if your organization or business has a privacy breach that either has caused or is likely to cause anyone serious harm, you must notify the Privacy Commissioner and any affected people as soon as you are practically able."[5]

The phrase "serious harm" can seem ambiguous, so the Commission gives examples including:

- physical, psychological or emotional harm or intimidation; and
- financial fraud including unauthorized credit card transactions or credit fraud.

The Privacy Commission expects to be notified of breaches no later than 72 hours after your organization becomes aware of it.

Some considerations need to be taken as transmitting any sensitive information to an external party can lead to this information being made public – either inadvertently or as part of the legal process.

However, it is good practice to report any breach or potential breach, regardless of the level of severity, even if you are not sure if it meets the criteria of the law. Doing so, gives greater reassurance to your stakeholders. You can work with your contacts at the relevant agency to discuss the details of formal reporting.

Financial laws:

Your organization may be legally obligated to report to the stock exchange, shareholders or other authorities depending on the incident type.

Criminal and anti-terrorism laws:

You may be based in a country that has laws about funding criminal or terrorist activities. As such, advice about paying ransoms need to take this into consideration.

Applicable international laws and agreements

It's rare, but possible, that your organization may be bound by international agreements or laws. This can include information sharing agreements between organizations. It's a good idea to be proactively aware of these.

[5] https://www.privacy.org.nz/responsibilities/privacy-breaches/

Internal policies

Your organization may have agreements in place regarding communications about significant incidents with suppliers, distributors, unions, etc. These can be helpful in framing your message, as you should have clear parameters of disclosure.

Voluntary disclosure:

There is a growing practice of organizations choosing to communicate beyond what's required by law. This can be a good way to build credibility and trust with your stakeholders.

The core argument behind this idea is that voluntary transparency is harder to fake and therefore more persuasive. Organizations that communicate proactively, consistently – and before they're forced to by legal requirements – build a different kind of stakeholder relationship than those that don't. This also follows an operating principle of "communicating by default".

This can be a difficult practice to implement as the response is usually “why say something if I don’t have to?” The answer, as with most communications, is that it raises trust levels. Again, the communications need to be balanced to ensure no personal information is given out or anything that could hinder the response, however, “getting out in front of the story” is a well-known communications tactic.

Note: this does not mean to immediately report an incident to the public when affected parties are still unaware, but to be proactive and open with your disclosures.

Cyber Insurance

If you have cyber insurance, you will have reporting responsibilities to your insurer. They may also offer specific help with external communications and reporting.

How to create a message

“organizations that take responsibility and are seen to be proactively trying to address the problem are perceived in a positive light.” **– Richard Knight and Jason Nurse**[6]

This is the part of the process that can be intimidating to those without a background in communications. However, by following the steps outlined in this framework and preparing standing lines and mapping your audiences, this can be a smooth process with few worries and you will see the preparation pay off.

These messages are a chance for your organization to demonstrate competence, reinforce stakeholder trust, and shape the narrative via well-crafted disclosures.

---

[6] *A Framework for Effective Corporate Communication after Cyber Security Incidents*, Richard Knight and Jason R. C. Nurse, 2020

Things to consider

Internal and external stakeholders will get different messages, simply because they need to know different pieces of information.

When creating the messaging for external communications, you need to cover a lot of points while also being easy to understand and clear about what the next steps are.

- Create a balance between clear information that stakeholders need to know, while also keeping specific information confidential to not entice further attacks.
- Do not say anything you may have to retract later.
- Anything you say to stakeholders has a chance to be reported in the media, consider everything to be public messaging.
- Media may come to you with queries before you have a chance to communicate with stakeholders.
- If your external stakeholders receive information about the incident via third parties, such as the media, before hearing from you, they are more likely to be negative towards your message.
- In certain cases your organisation may be obliged to provide up to date information about the availability of your services (see example below).

Example:

Under the NIS 2 Directive[7], entities must notify the recipients of their services (customers, business partners, et al.) "without undue delay" if a significant incident is likely to adversely affect the provision of those services.

AI use

Just like learning any new skill, creating messages will take practice. Resist the urge to use AI if possible, especially if you're starting out. While AI can be a helpful tool in incident response, learning with AI or giving it full control over your messaging can lead to an overly generic tone and voice from your organization.

People are getting better at recognizing AI-generated text, and it can come across as less personal and even potentially uncaring or insensitive. For example if you are a stakeholder who has had information stolen, you might take exception to a message generated by a computer.

For more generic communications, such as warnings of new threats or vulnerabilities, AI generated messages can speed up your processes.

[7] The NIS 2 (Directive (EU) 2022/2555), Article 23(1) and 23(2), https://www.nis-2-directive.com/

Availability heuristic

The availability heuristic is people's tendency to act off information that easily comes to mind. In this context, we know that people start taking cyber security more seriously when they hear of an incident[8].

This can impact your communications as recipients are:

- more likely to take actions on cyber security
- less likely to click links
- more suspicious if the email doesn't come from a usual source
- likely to try to corroborate via another source.

Resist the urge to create a bespoke email address for the incident. While the message can come from your CEO (or similar), it should be sent out via usual channels.

Balancing the message

While you need to communicate clearly about what happened and will be happening, there is a very real risk that the attacker may use your communications as a signal to start a new phase of the attack or double down on their efforts.

This is where being linked into the technical side of the incident response becomes incredibly important. Early information gathering allows you to craft the proper messages for the situation.

- What type of incident has occurred.
    - Gives you a good idea on what the future timeline will look like in terms of resolution and impact on stakeholders. Also you can decide what level of information to release about the incident.
- If the incident is ongoing[9].
    - You may not be able to say much, and what you can say will need to be more cautious.
- What steps have been taken to mitigate or solve the incident.
    - Giving clear examples to stakeholders of what has happened gives them greater trust in you. However, revealing too much information will tip off the attacker.
- What other organizations are involved in the response.
    - Explaining that other experts are involved, especially government, gives higher levels of trust to your communications. In general a National CSIRT will not say publicly if it is involved, however, asking them to do so can help take pressure off your organization.

Example:

[8] 25% of respondents said they are more likely to implement online security after hearing a cyber attack story – *Cyber Change: Behavioural insights for being secure online*, CERT NZ, 2022, pg42-43

[9] If it is uncertain if the incident is ongoing, treat it as such.

You have discovered that an attacker has exfiltrated data and has run ransomware software. Your IR team has managed to isolate one of your servers and is cleaning them of any potential malware. They are also about to test and then restore the two affected servers from a back-up. A ransom demand has been received.

Your message should contain some, but not all, of that information and detail.

"Our incident response team is working to contain the incident and secure any unaffected systems. We are aware that some data may have been stolen and are working to ascertain the extent of that. We have notified the Privacy Commission and will keep them updated as the situation progresses."

Keeping control of the message

You are not required to respond to any media queries, however, while it can seem like a good idea to decline them or otherwise downplay an incident, you run the real risk of losing the message to other commentators.

Having a set of pre-prepared statements for media queries is a good start. Even placeholder statements are better than silence.

Example:

"We are aware of a disruption with our systems and we are looking into the cause."

"We are aware that some of our online services are currently down, we are working at getting them back up as soon as possible."

While these seem cliché, they show that you are aware of the problem. They are a temporary solution; you won't get away with these a few days into the incident. Resist the temptation to describe a cyber attack as an unexpected technology failure or glitch, or something easily fixed.

Any update on the situation is better than nothing. With no official comment journalists will go to other sources; this can lead to speculation and incorrect statements about the situation. Updates can be sent either as a full press release or via social media.

Order of communications

The type of incident will direct who you communicate with and when. The more serious and public facing the incident is, the sooner you will need to go out with some kind of message.

Using the diagram of risk vs visibility, you can sort incidents into four categories, which are listed in increasing risk and urgency for communications.

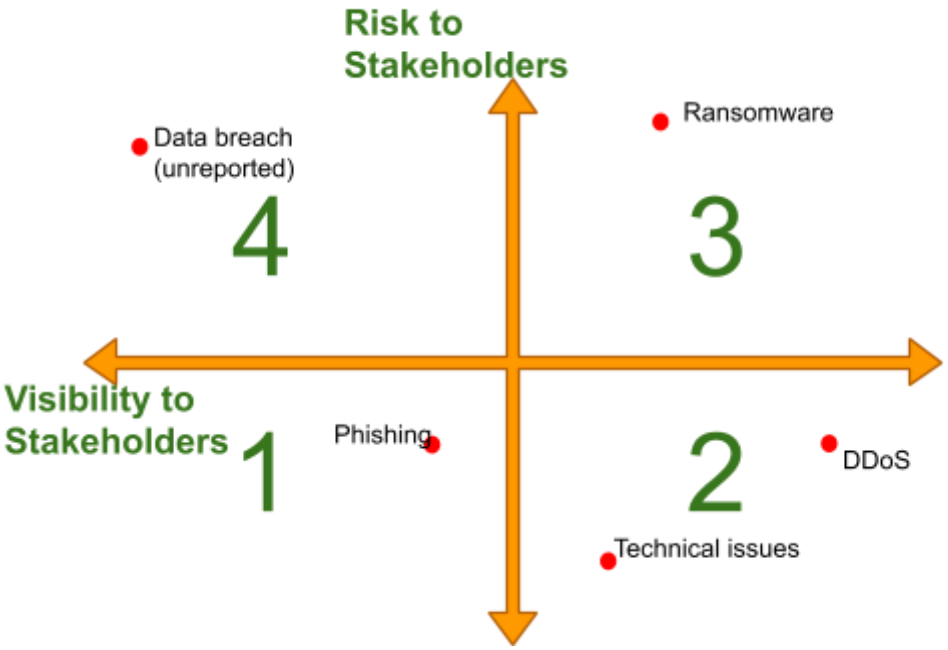

Figure 2: Stakeholder risk vs visibility matrix putting cyber incidents into quadrants

1. **Low risk *and* less visible to the public.**
   Direct communications may not be needed. Can be addressed via social media or website.

2. **Low risk but visible to the public.**
   These can usually be communicated via a written statement or media release. The scale of the outage may determine the timing, but these can usually go out without needing to delay.

3. **High risk but low visibility to public.**
   Initial communication directly to stakeholders should occur as soon as possible after discovery. A public disclosure must follow but can be done at a later date. Monitoring should be kept up to measure public visibility.

4. **High risk *and* visible to the public.**
   You will need to communicate quickly but cautiously. This can mean a short message to stakeholders to start, followed by messages over a longer timeframe. Media releases/responses will need to be short on details. Standing lines should be a priority.

Remembering that every message you send has the chance to be made public, so even internal communications should be cautious with details.

Internal communications

Internal stakeholders will need to know what is happening. This will usually occur directly after the Incident Response team is stood up.

Depending on the event, this message will need to explain:

- what internal systems have changed (eg. email),
- how to engage with external stakeholders,
- what staff data may be at risk, and
- what systems are in place to support affected staff.

External stakeholders

If external stakeholders are affected, they should be contacted as soon as possible, determined by the scale of the incident.

Depending on the event, this message will need to explain:

- what external facing systems are available,
- what data may be at risk,
- what systems are in place to support stakeholders and where they can go for more information.

The messaging will be pared back, however, as mentioned above in the section on balance. As part of this process, it may be necessary to stand up a call centre or provide extra staffing for your existing contact portal.

Remember that after hearing about a cyber incident, some people will prefer to phone an official help line.

This communication is usually done in the form of email, however, physical letters can be sent as well, depending on the audience.

Media release/queries

The more public facing the incident, the more likely you will need to put out a press release or respond to inquiries from media.

For more detailed descriptions on dealing with media, please see the Cybersecurity Communications SIG Media Guide[10]

Any direct communication with media should always be done at least a day after communications have been sent to any affected stakeholder groups, to allow for delays in delivery. While it can be difficult, direct media queries should be put off with prepared statements.

Example: “We are aware of a disruption with our systems and we are currently contacting affected customers. We are happy to provide a broader response once this step is completed.”

[10] link will be available soon

It is totally acceptable to **not** do a press release. If the story hasn't already been picked up, then there is no need to further spread the message.

Social media/website

These can go out at the same time as press releases or in lieu of one. For incidents with lower risk to stakeholders these can be used as a vehicle for your main message.

What should the message say?

This is the crucial part. Your message needs to be clear and concise but also empathetic. Some of this section may seem basic but others have fallen into these traps.

A good message will provide the information stakeholders need to protect themselves and will demonstrate that you are doing your best to address the situation.

The subject line

If you are contacting stakeholders directly via email, you need to ensure they read your message. This is tough because you need to create a subject line that sounds urgent without scaremongering or sounding generic.

Remember that people can receive dozens of emails every day from various organizations, yours may get lost.

Remember to avoid language used by threat actors and phishing emails. For example, do NOT say:

- "Urgent message regarding your account"
- "Take immediate action now…"

If you're able to give someone more personal information that will be useful.

- "Regarding your [company] account – [account number]"

Or give information about the situation.

- "[Company name] has suffered a [incident type]

There is no easy solution for this, sadly. There will always be those that ignore the message in their inbox. For this reason you should consider other paths for your message, such as social media.

Accept responsibility

You are the caretaker of your stakeholders' data. This means you will need to offer an apology. The form of the apology will differ from country to country and with different audiences.

While it feels like you have been attacked by an external party or let down by a flaw in a piece of software, your stakeholders will want to hear an apology from you.

Apologies can feel insincere if they are framed incorrectly. Where possible apologize directly to "people" rather than vaguely about the situation.

Do not say: "We are sorry that this incident makes you feel vulnerable."
Say: "We apologize to those who feel vulnerable in light of this news."

Do not say: "We are sorry to say that there was a data breach."
Say: "We have discovered a data breach and apologize immediately to all affected."

Even when stakeholder or customer is at fault (for example through password reuse) you will be expected to have mitigated through monitoring or another control.

Avoid downplaying

This may be perceived as not taking the incident seriously. While you do not need to give the exact extent of the incident, it is unwise to use words like "only" or "just".

Do not say: "The incident only affected 100 people."
Say: "The incident was limited to 100 affected people."

This will also help you if the incident is larger than initially thought.

Address feelings of vulnerability

Depending on the type of incident your stakeholders may feel vulnerable and worried for their security. This is especially so in cases where they could be individually identified.

It is a good idea to list steps that stakeholders can take to protect themselves in the wake of the incident, the more people can do for themselves the more they feel secure. This can include:

- contacting other agencies (such as the national CSIRT, their banks, or the government's Privacy agency),
- changing passwords on their accounts, or
- enabling two-factor authentication.

If the incident involves finances, you can offer credit monitoring or other services for free.

Remember that the recipients may be reluctant to click links.

Avoid blaming others

Blaming other parties can be seen as an attempt to dodge accountability. This includes cases of employee error. While a single person may be the cause of the incident, blaming them will be seen as poor organizational culture.

If the incident was caused by a known hacking group, do not name them or mention this at all. Doing so gives the group media coverage that they will use to gain notoriety and advertise their abilities.

If the incident was due to a service partner, refrain from apportioning blame to them publicly. You can sort out issues behind the scenes, as any public disagreements will result in damaged reputation for both parties.

Keep the message clear and easy to understand

Chunking the information into smaller pieces makes it easier to understand but also lessens the chances that the recipient becomes overwhelmed with the information.[11]

Avoid jargon and keep everything simple. Don't use a multi-syllabic word when a shorter one will do (for example, "utilize" instead of "use"). Longer, and more formal words can seem like you are trying to hide something.

For explaining aspects of the incident, you may need to dip into technical terms, however, keep these to a minimum and instead refer to other spaces (such as an explainer on your main website).

Avoid the message damaging your credibility

While this may seem obvious, too many times a message can inadvertently cause damage to your reputation down the track.

Often this is due to an underselling of the severity of the issue, an omission of key information or a falsehood that must be retracted.

Never say anything you may need to take back. This covers saying things you know are untrue or things that may change over time.

For example, saying you have a "technical issue" when you're aware it's a DDoS attack or saying that "no data has been breached" before the investigation has been completed.

You can omit incident response steps in your message in order to simplify the message and keep information out of the hands of threat actors. But conversely it can make it sound as though your organization is not doing a thorough job or has an incomplete plan. If you can say everything without compromising the message's balance, then it is better to do so.

Consider stakeholder characteristics

Depending on who your stakeholders are, you may need to alter your message, both in content and format. For example, some people are less likely to read emails and may prefer receiving a text message (from a legitimate source).

Similarly different groups of people may ignore calls to change passwords or take other steps to boost their own security. They may see it as a hassle or even as your responsibility.

Adding a "why" element to the steps can help this.

[11] *Cyber Change: Behavioural insights for being secure online*, CERT NZ, 2022, pg31-32

For example: “As your email address and password have been taken, it is likely the culprits will try to gain access to other accounts. You can protect yourself by changing your password and turning on multi-factor authentication”.

Other organizations

It may be that many organizations in your area are being affected by the same incident. You may consider doing a joint statement with them to show that you are not the sole target. This also allows you to pool resources.

Beyond the message

Remember that the message will likely generate questions from stakeholders – even if you think you’ve covered them all, they will still come up with new ones.

Ensure your staff, especially those who deal with external stakeholders, are across the message and know what to say. This can include a list of key messages and answers for obvious questions that can be quickly responded to.

Updates

Depending on the incident, “after the event” may not be after a month or two, it may, in some instances, be ongoing. This means you may need to send updates for a long time. These should be short and kept to essential communications only. If an investigation is continuing, then stakeholders can expect to be updated.

No news is good news.

You can add into your initial message that further communication will only happen if the investigation turns up more information. So you don’t have to follow up unless there’s something to say. This depends heavily on the type of incident.

There is also a chance the incident could flare up again (for example, a DDoS attack) or another incident could happen if attackers think you may be vulnerable. So be prepared to cover that scenario.

After the event

This is the section of your communications planning that can be the most important. The goal is to help your organization use the incident as a capability-building event, not just something to close out and forget about. This is a chance to review and evaluate your previous preparations and to improve your ability to respond in the future.

Debrief and review

As with any part of an incident response, a debrief on how the communications went is essential. Part of this is to review your process, updating as required and pinpointing areas that can be improved on.

Some questions to consider as part of the review:

- Was your stakeholder or audience mapping accurate?
- Did your standing lines work?
- Which lines did you use and do you need to take them out of the rotation or change them?
- Did your Comms Lead have all the information they needed?
- Did the sequence of communications match the incident or how you planned it?

In some cases this may mean re-running some of the exercises, such as audience mapping, with any new information or lessons you have learned. This can also be a chance to refocus efforts, for example, if you spent a lot of time checking FAQs for the helpdesk but noone called through, then you can deprioritize that in the future.

You may want to talk to stakeholders, internal and external, to see how the message was received and what could be done better next time. If you use analytics on your emails you could look to see how many emails were opened, you can look at traffic statistics for any webpages you may have set up for the response. We would **not** recommend using social media comments as a reliable measure for feedback.

Admin tasks

After an incident a lot of things need updating. For communications we recommend checking this list and making changes as necessary.

- **Stakeholder contact details:** update with current information, including changes of staff and notes about if and how they may have been affected during the incident.
- **Standing lines:** change to be better aligned to any audience changes, and refresh any you have used so you don't repeat the same messages for every incident.
- **Website:** update your website as necessary with relevant information. If you have added information regarding the incident, review and decide if it needs to stay up.
- **Processes:** ensure any changes made as part of the review are reflected in internal policy documents, especially reporting lines and responsibilities. This allows for better business continuity should there be staff turnover.

You may wish to create reminders to check these periodically or to update them when you do the regular review of your overall incident response plan.

Appendices

1. Version history.
2. Audience mapping exercise.
3. Standing lines.
4. Real examples.

Version history:

Version	Date	Notes on changes
1.0	02/2024	First finalized version of the template.
1.5	01/2025	First draft with international content.
2.0	05/2026	Finalized international version with full appendices and examples. Changed to US English.

Audience mapping exercise

This can be used to create a greater understanding of your audiences. We have added examples into the template.

1. Use the Audience column to list every audience you communicate with. Resist the idea of condensing groups, in the initial steps it's best to have more entries. You can sort them by categories to help organize and summarize especially for the final step.
2. The Medium column lists all the way your organization communicates with those audiences.
3. Voice and Tone are the ways you write or construct your messages and are descriptive of the type of language you use.
    a. Voice is how you *always* communicate. This means you will likely want to use words such as "professional" or possibly "official". This is also where you list the ways you should avoid. This likely includes being rude or blunt, but depending on your organization may also include things like "humorous" or "condescending".
    b. Tone is how you *sometimes* communicate. For example, you might always be professional, however, in some cases you might be friendly, in others you might be technical. Think about the difference in talking to teachers and students – your voice and message will be the same to both parties but your tone will be very different.
4. The final step is to map across the columns. Linking each audience to the mediums and tones you will use.

Audience	Medium	Voice (always)	Tone (varies)

• Board
• Regulators
  ○ Government
  ○ Financial
  ○ Shareholders
• Customers
• Vendors
• Contractors
	• Email
	• In-person
	• Text messages
	• Website
	• Social
	• Reports
		• Professional (but not formal)
		• Expert (intelligence)
		• Knowledgeable (wisdom)
		
		NEVER
		• Condescending
		• Overly technical
		• Distant
		• Scary
			• Friendly
			• Technical
			• Succinct
			• Human – talking to a real person
			• Informal
			• Simplistic
			• Empathetic

These are examples only and it is a good idea to fill out this table with as many team members as possible.

Standing lines

The following are examples to use to answer certain questions. We do not recommend using these exactly as written but change them to suit your own style, tone and language.

In general it is best to avoid using words like “hacker” or “attack” as they can cause some audiences to panic or raise further questions you may not be able to answer at the time.

What is happening? (if you do not have any information)

Note: the use of “attack” is fine, but can cause some audiences to panic unnecessarily.

- We are currently experiencing an outage and are investigating the cause.
- We are aware that there has been a technical incident and our response team is working on it.
- At this time we are unsure of what is affecting our systems, however, our teams are working hard to resolve the issue and we will update you when we know more.
- We are aware that there has been a cybersecurity incident and we are working on resolving it as soon as we can.
- We are aware of a disruption to our systems, we believe it may be a cybersecurity incident. We have contacted the [national CSIRT] are currently working to resolve the issue and will update you as soon as we know more.
- [specific example] Our systems are currently experiencing a DDoS attack. While this is keeping our [website/app/etc] offline, we are working to ascertain if any client data has been affected.

When did this happen?

Note: the exact time of the incident doesn’t need to be shared, you can simply use the day or month if it occurred a long time before discovery.

- We believe the incident began on [day]. Our security team began investigating and restoring services from back-ups. We are reaching out to you now as we have a greater understanding of what has occurred.
- [specific example] A data breach of our systems was discovered on [day], we are currently investigating and determining what data has been compromised. We will advise you as soon as we know more. In the meantime we recommend you… [information from national CSIRT or other trusted source].

What kind of attack is it? (if known)

Explain the type of attack broadly speaking without specifics and link to a trusted official site for more information.

Who did this?

Your audience will, in general, not get any useful information from knowing who is behind an incident. Moreover, naming a threat actor can make them more likely to continue their attack for future influence.

- At this time we are solely focussed on restoring your data and protecting it for the future. We are working with law enforcement and they will deal with attribution of the attack.

How did the attackers gain access?

Note: again do not give too much away.

- The investigation into the attack is ongoing and we will be conducting a thorough assessment of the potential access points for the attackers.

What data was accessed? (in the case of a data breach)

Remember the rule to not say anything you may need to retract.

- At this time we are working through our systems to determine what information the attackers may have been able to access. We will notify affected people when we learn more.
- We know the attackers were able to access [list of data types]. Because of this we recommend affected users take the following steps…

Real Examples:

Communications strategy

This was created for an international company that suffered a ransomware attack. It has been anonymized.

Communications strategy
This is a draft with basic steps listed out.

1. Get advice on steps internal and external stakeholders will need to or can follow.
    a. Do they need passport renewals?
    b. Do they need to talk to their banks?
2. Prepare standing lines in case of queries
    a. FAQs
    b. Call centre?
    c. Manager for client interaction
3. Contact internal staff
4. Contact external stakeholders

Getting advice.
Due to the nature of the data, you will need advice on the response and what actions your stakeholders need to take.
Passports:

- Do the individuals whose passport details have been stolen need to renew their passport?
- Is this different for the ex-pats whose information was stolen?

Bank account details:

- Was this only account information or was there further identifying information?
- Do people need to contact their bank to halt any transactions?

General Data Protection Regulations (GDPR)

- GDPR covers people from EU members.
- This includes ex-pats.
- You may be required to report or follow rules set out by the EU if you are holding information of their citizens.

Local Laws (where applicable):

- Report to law enforcement as they may need the information for a criminal investigation.
- Report to Privacy or Data or Human Rights Commission (even if not a legal requirement it is good practice)
- Report to NatCSIRT (even if not a legal requirement it is good practice)
- Stock market
- Does negotiating or paying attackers breach any international conventions signed by the Government on funding criminal or terrorist activities?

FAQs and answers/Standing lines.

These are not in order

- When did this happen?
  - We believe the attack began in late May. We brought in a security team and began the investigation and restoration of services from back-ups. We are reaching out to you now as we have a greater understanding of what may have been taken.
- What kind of attack is it?
  - This is known as a ransomware attack. Criminals access your system and encrypt files so you no longer have access to them.
- Who did this?
  - At this time we are solely focussed on restoring your data and protecting it for the future. We are working with law enforcement and they will deal with attribution of the attack.
- How did the attackers gain access?
  - The investigation into the attack is ongoing and we will be conducting a thorough assessment of the potential access points for the attackers.
- Is our data still on your system?
  - We are rebuilding parts of our systems and, at this time, the data we hold is now secured.
- Was the information backed up?
  - Our systems are backed up regularly and we are still working at restoring some parts. We apologize that this is a slow process to ensure the attackers no longer have access.
- What data was being stored and why?
  - Our current investigation has revealed that the affected data contained:
    - Personally identifiable information (PII), including some passport information.
    - Bank account information.
    - Invoices.
    - Contracts.
    - Audits.
  - This information is regularly collected for us to do business in this country and with international clients.
  - We are working diligently to ensure this data is fully protected and backed up for the future.
- What are you doing to fix this?
  - As soon as the attack was noticed, we immediately called in our IT service provider to run the recovery. We apologize that this is a slow process to ensure the attackers no longer have access.

- We have engaged the government's cybersecurity response team and are working with them, and international experts, to work towards future solutions.
- We will be updating all those affected as we learn more during the course of the investigation.

- What do I need to do?
  - While nothing is required from you at this stage, the government's cybersecurity incident response team recommends you take the following steps to be extra secure:
    - Check your bank account for unusual transactions.
    - Where possible, turn on two-factor authentication (2FA) on your financial accounts to ensure transactions cannot be made without your explicit consent. For more information about 2FA see [security website].
    - Be wary of any unusual communications to your work or personal email accounts, as the attackers may try to contact you directly.
    - If you do receive anything suspicious, please let us know.
- Has this affected any payments made in the last month?
  - At this stage of the investigation we do not believe that any payments have been diverted or accessed by the attackers.

Initial comms for internal staff.
This goes out first.
Internal staff includes anyone with access to your systems, so this includes any contractors you may have.
Ensure all staff are fully briefed and that managers are prepared for questions that they can pass up to the executive level.

Initial comms for external stakeholders.
This goes out second and shortly after you are certain every staff member has received the first communication (even if they haven't read it yet).
External stakeholders are: anyone whose information you had that isn't employed by SMG Construction. This includes customers, suppliers, logistics and transport companies.
You will need a single communications point for external stakeholders. This person can refer to the standing lines and will need to be ready to give answers quickly.

Message to affected parties (1).

This example is taken from a data breach involving a tertiary education provider. It has been anonymized for this document. The audience is the students whose records were stolen.

Hello

As you may know, our organization was the target of a cyberattack on [DATE]. While we are still investigating the incident, we are concerned that the attackers may have had access to personal information.

We understand how concerning this may be for you. We'd like to assure you that we are doing everything we can to continue to strengthen our security practices and to protect your personal information by improving our information security frameworks.

We have been working with cybersecurity advisors to investigate this situation. Since becoming aware of the issue, we have addressed the vulnerabilities and your personal information on the system has been secured.

What happened

Attackers, using a type of software known as ransomware, were able to lock our staff out of the system. This was first noticed as a system outage, but we quickly realized it was a cyberattack and updated stakeholders as soon as possible.

We are working diligently to restore the systems and investigate what systems and information the attackers may have had access to.

What information was exposed

At this stage we are uncertain exactly what data may be affected but the following is a list of information we keep on individuals.

- Your name.
- Email address.
- Password.
- Date of birth.
- Address.
- Phone number.
- Student number.
- Class records.
- Credit card details.

Please know that keeping your data safe is of the utmost importance to us and we have strengthened our security procedures as quickly as we can.

What should you do

[CREDIT CARD] As credit card numbers may have been stolen as part of the attack, we recommend that you contact your bank to get their advice on what to do next. You may only need to put a temporary hold on your card.

[PASSWORDS] Passwords used to access our systems may have been exposed. We recommend you update this password as soon as possible. We recommend that if you use the same password across multiple sites that you update your password on these sites. It is also a good idea to use a password manager application on your phone or computer to help you create strong passwords that are unique to each site you use, and store these securely.

[TWO-FACTOR AUTHENTICATION] You may also want to turn on two-factor authentication on the online platforms you use. Doing this adds another layer of security to your accounts and uses a code sent to your phone – either via text message or app.

Note that different apps call it different things, but it can usually be found inside the security settings.

[FURTHER CYBER ATTACKS] As the information we hold includes personal information there is a risk of further attacks, including phishing and other scams. This can include scammers claiming to be from our organization.

Remember to be safe online and do not respond to any emails, text/chat messages, or social media communications that you consider suspicious or calls from numbers you don't recognize. University staff will never ask you to share extra personal information, and we will not be asking for any payments in response to this attack.

You can report any suspected fraudulent activity to [NatCSIRT or relevant authority].

For more information

If you have any further questions, please visit our website, and search for [KEYWORDS] to read the FAQs or you can visit [NatCSIRT website] to understand more about what to do next. If you would prefer to speak to someone, please call [TOLL FREE PHONE NUMBER].

We sincerely apologize for this situation and the stress it has caused.

Message to affected parties (2).

This is the text of a message sent to users of Ticketek in Australia following a data breach. This is an excellently constructed message often used as an example of best practice.

- First paragraph explains the situation. It's a bit long but it gives a good summary.
- Second paragraph explains that your payment information is safe, giving reassurance and setting expectations. Remember that to say this, you must be certain about what data is affected.
- Third paragraph explains what happened but does not blame the provider. Also sets out why you are being contacted.
- Fourth paragraph discusses who the team are working with giving further reassurance.
- Fifth paragraph is placed inside a separated section to show it is important. This gives a clear description what data has been impacted.
- Sixth paragraph also starts with a new section which is what users should be doing. It begins with a clear apology for the incident.
- Seventh paragraph does make one small mistake of linking to a pdf file. The file contained no new information, and asking users to open a pdf is not a good idea if you can simply add more text to your message.
- The final paragraph is important because this is where Ticketek funnels all the queries. They had set up a dedicated phone line and email address for the affected customers. Note: if you do decide to do this your helpdesk operators will need a set of lines to use.

SUBJECT: Important Message
BODY: Dear Ticketek Customer, We are writing to let you know that Ticketek has become aware of a cyber incident impacting Ticketek Australia account holder information, which is stored in a cloud-based platform, hosted by a reputable, global third party supplier. We would like to reassure you that Ticketek has secure encryption methods in place for all passwords and your Ticketek account has not been compromised. In addition, we utilise secure encryption methods to handle credit card information and transactions are processed via a separate payment system which has not been impacted. Ticketek does not hold identity documents for its customers. Since our third party supplier brought this to our attention, over the past few days we have worked diligently to put every resource into completing an investigation, so that we can communicate with

you as quickly as possible. We wanted to notify you early to enable you to take steps to protect your information as a precautionary measure.

We have also notified the Australian Cyber Security Centre (ACSC) and we are liaising with the Office of the Australian Information Commissioner (OAIC) and the National Office of Cyber Security in relation to the incident.

What personal information is involved?

The available evidence at this time indicates that, from a privacy perspective, your name, date of birth and email address may have been impacted.

Next steps

We sincerely apologise to all those who may have been affected by this incident.

We recommend that you review the cyber security guidance available at this link[12], so as to protect your information moving forward and to lower the risk of your information being potentially misused.

We thank you for your understanding and support as we respond to this incident – please don't hesitate to contact our dedicated customer support team relating to this incident on our 24-hour incident hotline XXXXXXX (Australia) or +61 XXXXXXX[13] (International) or email us via XXXXXXX@ticketek.com.au, if you have any questions.

Kind regards,

Ticketek

[12] Link removed for this document.
[13] Phone numbers and email address removed for this document.