certnz

Public communications for cyber security incidents

A framework for organisations

New Zealand Government

Contents

Acknowledgement

The following is based on the work of Richard Knight (University of Warwick) and Jason Nurse (University of Kent)

Introduction

***"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[1].**

This framework is designed to guide an organisation through a plan for public-facing communications in the event of a cyber security event.

This framework aims to help organisations decide when to communicate and at what level as part of an overall incident response plan[2].

Communication can be an after-thought during an incident response, with organisations wanting to nail down the IT response first. However, communications are vital to how the organisation is perceived during and after the incident.

A balance needs to be struck between:

- helping stakeholders, members, customers and the general public understand how they may be affected and any steps they need to take, and
- not giving attackers information that may give them an advantage or make the attack worse.

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

[2] Creating an incident response plan | CERT NZ https://www.cert.govt.nz/business/guides/incident-response-plan/

When an incident occurs

Initial steps

As part of the incident response plan, someone needs to be nominated as **Communications Lead** (Comms Lead). This person will be the single sign-off point for messages to any internal or external stakeholders, including media and the public.

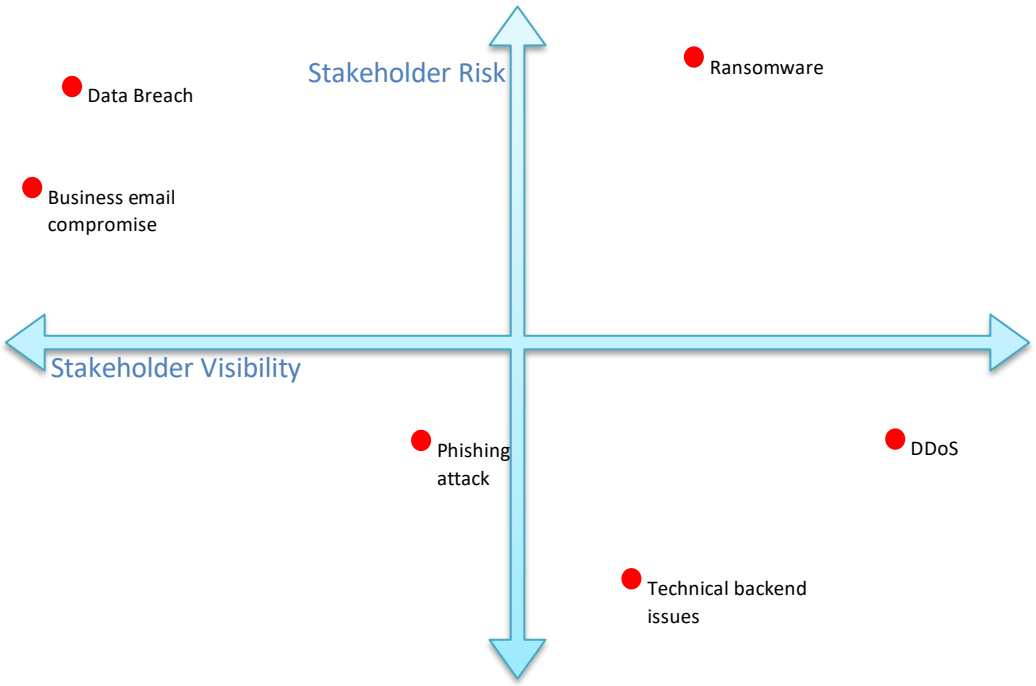
"Stakeholders" will be determined by the organisation or incident. It can be as broad as everyone who has contact with the organisation or as few as internal staff.

Decisions

The Comms Lead needs to make the following decisions.

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

To do this they need to gather information which is part of the regular incident response plan.



Info gathering

The Comms Lead needs the following information from the Incident Response (IR) team as soon as possible. This can be done during the initial briefing and updated as the incident progresses.

- What type of incident is it?
- Who is affected? (Clients, public, specific agencies etc)
- How widespread is the incident? (Localised, 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?

It is also useful if the Comms Lead is aware of the following.

- Is the incident being reported by the public/journalists/experts in media/social media?
- Are reports being made from clients/users to your organisation?
- Has the organisation 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?

While some incidents require disclosures to relevant agencies, some communications with stakeholders can be delayed (depending on the incident). Messages should be created quickly but not hastily.

Responsibilities

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

These steps should be part of a standard incident response 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 New Zealand laws

Privacy Act:

"Under the Privacy Act 2020, if your organisation 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."[3]

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

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

CERT NZ strongly urges you to report any breach or potential breach to the commission regardless of the level of severity. Doing so, gives greater reassurance to your stakeholders, even if the breach was a lower level.

The Privacy Commission expect to be notified of breaches **no later than 72 hours after your organisation becomes aware of it**. Breach notifications can be made via the Commission's website: Office of the Privacy Commissioner | Privacy breach notification form

Financial rules:

Your organisation may be legally obligated to report to NZX, shareholders or other authorities depending on the incident type.

Applicable international laws

It's rare, but possible, that your organisation may be bound by international agreements or laws. It's a good idea to be proactively aware of these.

Internal policies

Your organisation 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.

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.

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

How to create a message

"Organisations 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**[4]

This is the scary part: letting other people know about the incident.

Remember, if your clients, users or stakeholders first receive information about the incident via third parties, such as the media, rather than you, they are more likely to be negative towards your message.

Things to consider

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.

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[5].

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.

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

[5] 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

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.
    - You may not be able to say as 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 organisations are involved in the response.
    - Explaining that other experts are involved, especially government, gives higher levels of trust to your communications. Organisations, like CERT NZ, will not say publicly if they are involved.

Example:

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.”

Controlling 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."

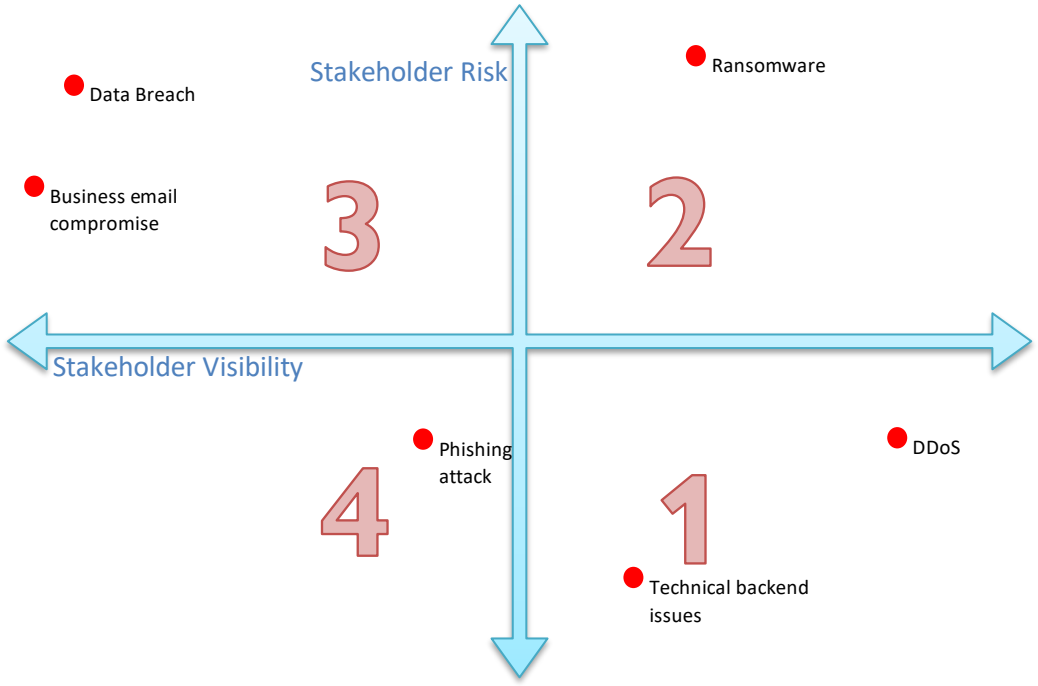
While these seem cliché, they show that you are aware of the problem. They are a temporary solution; you won't get away with these a few days into the incident. Resist the temptation to describe a cyber attack as an unexpected technology failure or glitch, or something easily fixed.

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.



1. **Visible to the public but with a low risk to stakeholder data.**
   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.

2. **Visible to the public and high risk to data.**
   You will need 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.

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

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.

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.

Public perception of an organisation decreases if they hear about an incident through the media first.

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 organisations., yours may get lost.

Accept responsibility

You are the kaitiaki, custodian and caretaker, of your stakeholders' data.

Apologise and apologise again. While you may 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.

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

Do not say: "We are sorry that this incident makes you feel vulnerable."
Say: "We apologise 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 apologise 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. This can include

- contacting other agencies (such as CERT NZ, their banks, or the Privacy Commission),
- 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 dodging 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 organisational 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.

Avoid jargon and keep everything simple. Don't use a multi-syllabic word when a shorter one will do (for example, "utilise" 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.

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.

Omitting steps will shorten and simplify the message, but conversely it can make it sound as though your organisation has an incomplete response plan. If you can say it without compromising the message's balance, then it is better to do so.

Consider stakeholder characteristics

Depending on the demographic make-up of your stakeholders you may need to alter your message, both in content and format. Some demographics are less likely to read emails and will see things on social media sooner.

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. 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 organisations

It may be that many organisations 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.

After the event

Updates

Depending on the incident and how long it continues, you may need to send updates. 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.

Debrief

As with any part of an incident response, a debrief on how the communications went is essential. 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.

Self-assessment

After an event is the best time to go through your systems and processes, highlighting potential risks from a communications perspective. (Your IR team should work on potential tech risks).

This can be as simple as ensuring all stakeholder contact details are up to date. But it can also include complex tasks, such as updating your website or changing internal reporting lines.