A guide to responding to journalists (media) for CSIRTs

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

About the guide

This guide has been created for small teams and those who do not have a built-up communications function. It is an introduction on how to work with media.

It will give your team ideas to create internal processes for both reactive and proactive responses, as well as techniques for creating better written and non-written responses to queries from journalists.

Remember, this is a guide and not something to be rigidly followed. Your team will have slightly different scenarios and relationships with your media environment so you can adapt and change these processes to work for you.

This is also a way of sharing information. Sometimes speaking to the media can get a message out much faster than through other means at your disposal.

Note: this guide uses the 'write', 'create', 'speak' and similar words interchangeably. This is because there are multiple ways of communicating with media.

Quick Notes

The most important things to remember.

- Most media queries coming to you are low risk, the journalists want you to be a source of information rather than a target.
- Most media queries will be for information you already have to hand (for example, "how does a ransomware attack work?", "how can people avoid online scams?")
- Create 'standing lines' (see Technique section) to be better prepared.
- Talk to journalists to get a better idea of what information they want.
- Understand what you are, and *are not*, allowed to talk about to media.
- If you can lean on a communications person to help, do it.
- Do not be scared to ask for help.
- If you can write a technical report, you can write a media response – it will just take time to finesse into something the journalist can use.
- Practice, practice, practice.

Journalists

Journalists are not an adversary. They are a vehicle for getting information out to the public, and you can use this to your advantage.

As an incident response team with access to threat intelligence, you are considered an expert on the subject and a resource. Journalists will come to you to get background information or be a subject matter expert.

Unlike politicians or other public figures, you are not the target for journalist to ask tough questions. Generally, they will want to ask you about the 'what' and 'why' of a situation – what is happening and why is it bad? – rather than the 'how' – "how did this happen?"

You will know exactly when you are able to answer a question or not, how you respond to that is what takes some practice.

For example, you should avoid talking about:

- Threat actors – do not give the bad guy free publicity
- Ransom demands – again this gives publicity to the bad guy but also the public doesn't have a good grasp of ransom and think it is a surefire solution.
- Specific actions being taken to respond to the incident – don't give away information that can be used by threat actors.
- Specific incidents – while there is a little bit of wiggle room here, most incidents should be kept out of the media until it is resolved.

Remember that journalists tend not to understand technology, cybersecurity or statistics[1]. Because of this, journalists will ask about a topic or incident they want to cover without having the idea fully thought out.

This can mean speaking to the journalist ahead of time and discussing what they want to talk about and leading them to something you feel more comfortable talking about. Or you can use it to highlight an issue that you feel is more important.

> Example:
> "I wanted to ask Christmas shopping scams"
> "Well we can cover basic text message scams, but we've also been seeing a lot of scams that use an AI chatbot and it'd be great to focus on those if we can…"

Remember that journalists are under a lot of pressure. Newsrooms are shrinking and a single journalist may be required to file three or more unique stories every day that include

[1] That is a broad generalisation and there are many who have a good understanding of technical topics, especially if they have a specialist area.

interviews and photos and editing, all before a daily deadline. If you have good information for them, especially information they can cut+paste, they will appreciate it.

Finally, don't be afraid to make friends with journalists. This is not about influence but having a rapport with them. Ensuring they come to you for quotes and trust you as experts.

Response processes:

Proactive

A proactive approach is best for teams that have some sort of communications capacity. This requires teams to approach media in advance of getting a request.

It can be as simple as a social media post or article on your website, or it can be more complex with a media release and suggested talking points.

You do not need to follow this approach as it does require more communications expertise to maintain; however, it does lower the overall workload of a communications team compared to the reactive method.

Set-up

You will need the following roles (note that one person can do multiple roles, however, you need a minimum of two people).

- Creator (the person who creates the content).
- Media Point-of-Contact (POC, the person who will send out any releases or posts).
- Subject-matter expert (if required).
- Quoted person (this is often the Sign off or other high-level person, such a director, must be ok with their name used publicly)
- Sign off (the person who approves the response).
- Proofer (a final set of eyes looking for typos and glaring errors).

Media releases

Media releases are what most people think of when it comes to communications with journalists. A media release is a pre-written statement that covers at topic: often it announces something or is in response to an issue.

These releases will be sent to a list of known media outlets that you maintain. It is good practice to have these available in a section on your website.

You can think of a media release as being like an advisory or alert. It will cover what is going on, offer advice and links to further help.

Website updates

Very similar to a media release, but without needing to send it out to a list. Often these are used for journalists to find when they are searching for a topic or to point them to if they ask for a basic statement.

Social media

Most useful for ongoing or developing issues that require updates. These are much shorter but still cover the same type of things as the other two options.

Reactive: journalist wants to learn what the issue is

Instead of going out to media with information, often, CSIRTs will wait and react to queries coming in. This requires less preparation, but can be a larger workload when a query comes in.

This type of process can be run by itself or, preferably, alongside a proactive one. It's good for teams that don't have dedicated communications staff or don't expect many media queries.

Set-up

You will need the following roles (note that one person can do multiple roles, however, you need a minimum of two people).

- Media Point-of-Contact (POC, the person who interacts with the journalist).
- Responder (the person who creates the response, often is also the POC).
- Subject-matter expert (SME, if required).
- Quoted person (this is often the Sign off or other high-level person, such a director, must be ok with their name used publicly)
- Sign off (the person who approves the response).
- Proofer (a final set of eyes looking for typos and glaring errors).

The basic process

This is a very basic process that can be altered as needed for your team.

Step	Person	Action
1	POC	Receive media query (via phone call or email or other method)
2.	POC	Reply to the journalist and ask the following: • What is their deadline? • What format do they want the response in (interview, written, etc)? • Can they clarify what areas they want to cover? (Often journalists do not know about cybersecurity and will ask about things that are irrelevant). Where possible this follow up is done over the phone because it's:

		• faster, • clearer, and • gives you a chance to talk to the journo about the subject and frame some of their questions[2].
3.	POC	Forward query on to • Responder (if that's not you) • Subject-matter expert, • Sign off point, and • Anyone else who might need to know[3]. Include any other info you get from the journalist.
4.	Responder	Plan the response and ensure it works for the journalist, sign off and the SME – including different options if necessary.[4]
5.	Responder	Create the response: • Written • Interview
6.	Proofer	(Written only) Check response for typos and errors
7.	Responder	Send for sign off
8.	POC	Send to journalist (before their deadline)

Deadlines for journalists depend on who they work for. Print journalists tend to have two per day (morning and afternoon). It's good form to get your response back to the journalist well before their stated deadline to allow for any potential follow ups.

Sometimes a journalist may ask for a very quick turnaround, for breaking or important stories. You are ok to say that you cannot make those timeframes. Generally, journalists know they are asking for a 'favor' when they do this, so if you don't have capacity, it is ok to say so.

Reactive: journalist already has the story

When a journalist contacts you because they already have documents, a source, or are calling to say they're about to publish, the dynamic is fundamentally different and you might need a different approach than the standard reactive process.

Here are a few signals that you are in this scenario:

- The journalist mentions specific documents, screenshots, or internal information.
- They give you a very short deadline, usually hours, not days.

[2] See the Technique section, below, on how to do this.

[3] For example, your Minister's office or the communications team from your wider agency.

[4] The journalist may ask for an interview but you can go back with different options if you have no capacity or you deem the request to be too much for the situation.

- They ask you to "confirm or deny" something specific or simply ask you for a comment in response to their conclusions.
- They tell you the story is "going to publish either way."

First step: escalate to your sign-off person and, if you have one, your communications lead before you respond to the journalist at all, even to acknowledge receipt.

When you do respond to the journalist, keep it brief. Acknowledge receipt, ask what specifically they want a comment on, and confirm their deadline. Do not volunteer information, correct assumptions you haven't verified, or confirm details you're uncertain about.

Example: A response of "We are aware of your request and will respond before your deadline," is entirely acceptable as a holding reply.

Some practical points for this scenario:

- **Ask to see the specific claims they intend to publish.** Journalists are not obliged to share them but many will, especially if they want an accurate story. Knowing exactly what they have lets you correct errors of fact without confirming everything they've been told.
- **If information in the story is factually wrong, say so clearly and provide the correct version.** Journalists generally do not want to publish inaccurate information. This is your best lever so long as the issue is factual, not subjective — and you can prove it.
- **If you genuinely can't comment, say so with a reason.** "We are unable to comment on this as it is part of an active investigation" is more useful to a journalist than silence, which will typically be reported as a choice you made.
- **Don't try to talk the journalist out of publishing.** It rarely works and often damages the relationship. Your goal is to ensure what they publish is accurate, not to prevent publication. Once the story runs, it's also worth asking how the story developed in the first place, and whether that points to an organisational gap, a communication failure, or something else that needs fixing internally.

After the story is published, review what ran against what you were told. This helps you calibrate how to handle the same journalist in the future and gives your team useful information about real issues that need to be surfaced and addressed.

Social media DMs and non-email contact

Journalists increasingly make first contact via LinkedIn, X, or other social platforms. This is not a different kind of media inquiry (i.e. the process is the same), but the channel creates practical considerations you should plan for.

The main issues including:

- **Routing.** Messages can go to individuals rather than a shared inbox, which means they're easily missed or not routed to the right person. If you have a public-facing team presence on LinkedIn or X, monitor the DMs on those accounts. Individual staff members who receive journalist DMs should forward them to the POC and not respond independently or ignore them (these messages still count as your organisation being asked for comment and the journalist is allowed to include that in their reporting).
- **No paper trail.** DMs don't create the same record as email. As soon as a journalist makes contact via social media, move the conversation to email before the substantive discussion begins. A simple "Thanks for reaching out — could you send your question through to [media inbox address]?" is sufficient. This protects both parties and keeps the documentation within your standard process.
- **Pressure to respond informally.** Character limits and the casual register of some social platforms create pressure to respond quickly and briefly. Resist this because a short DM reply can be screenshotted and used out of context in a way that a formal written response can't. Don't give substantive answers via DM, move the conversation to your standard process.
- **Personal accounts.** It's worth clarifying with your team whether individual staff members should accept follow requests or connection requests from journalists on personal accounts. There is no universal right answer, but there should be a shared understanding of where the line is between having a professional relationship with a journalist and being a source for them without the rest of the team's knowledge.

Remember that the same process applies regardless of how a request arrives. The specific channel doesn't change what constitutes an appropriate response; only how quickly you need to move the conversation somewhere more appropriate.

Techniques

These are some basic tips on how to respond to media queries or create useful media releases.

Standing lines

These are pre-written lines or statements on specific topics and they are incredibly useful.

The most important standing line is the one you need to send when you can't speak about a topic. This needs to be short and to the point but not rude or dismissive.

Below is a table with examples of lines for queries when you need to say "we can't talk about that".

Topics you can't talk about	Example standing line
Sensitive incidents Foreign interference	"We are unable to discuss specific incidents"

Ransom demands Specific threat actors Criminal investigations Not cyber security.	"That is not part of our jurisdiction, please contact…" "While that is an important part of the investigation, at this point in the response we are focussed on …" "I can't speak to that aspect, but what I can say is that …" "Obviously, we can't talk about specific incidents but in general we find that…" "That is an important matter that is being looked into, but what we want people to focus on right now is…"

You will likely also need standing lines on various types of incidents, such as DDoS, data exfiltration and ransomware. However, as journalists' audience is the general public you will also need to have lines prepared for scams, phishing attacks and other more common incident types.

These are more like explainers, showing how each incident type works and with steps people or businesses can take to be secure in the wake of an attack. This means they can be simple (How phishing works and what to avoid) or more technical (controls that can limit the spread of ransomware in your system).

Even if you aren't able to respond to a query directly, you can use these standing lines to give more information, which is ultimately what the journalist wants.

For example, "We are unable to discuss specific incidents, however, if you are worried that your data may be involved in the breach, here are the steps you can take to protect yourself…"

These descriptive lines can also sit on your website, and for days when you're busy you can point journalists to that. However, do this sparingly because it's not best practice.

Written responses:

Most media queries are for written responses. The journalist will want a paragraph or two on a topic.

If you choose to respond, you must include:

- A clear, accurate answer – this will lower the chances of a follow up question.

- A person in your organisation that can be quoted.

Any response that just comes from a generic spokesperson is less likely to be used and usually will have the journalist asking for a name.

Remember that a quote doesn't have to a be an actual thing the person said. The responder should write lines for the spokesperson and then check with them that it's ok. Usually the person being quoted may make some small changes but it makes the process faster and means your regular standing lines can be converted to quote if need be.

Example: CSIRT Director Jane Doe said, "phishing is the most common type of cybersecurity incident and can lead to much more serious attacks".

Also try to make your response easy to cut+paste into the journalist's article. As mentioned above, journalists are time poor and would rather add full quotes than try to rewrite sentences.

Use your standing lines where you can but also change them around a bit. By doing this it means you're not sending the same line out over and over again.

Finally keep a folder on your system with all your responses (include audio and video as well if possible). This gives you a resource of past responses that you can use to copy into new responses for consistency but also gives you an idea of the type of things that journalists are asking about.

Things to remember

- The key here is speed – getting back to the query quickly with accurate responses and using sentences that can be quoted in full.
- Where possible attribute to a person rather than a generic "spokesperson".
- Refer to the standing lines but rewrite them so you don't sound repetitive.
- Keep a record of responses you have sent.

Non-written responses

Sometimes you will be asked to talk about a subject. There are four types of interview:

1. **A conversation "on background":** this is where the journalist will not use your answers but wants more detail about a topic. For example, they may ask about the ins and outs of phishing. This is usually done for longer pieces where they will talk to someone else later. They may record the interview for note taking.

2. **A conversation that is recorded (audio):** this will form the basis of a written article where the journalist will quote you.
3. **A pre-recorded interview (audio or video):** this will be used in whole or edited down. As it is pre-recorded ("pre-rec" journo terms) if you fumble an answer, it's ok to stop and start again. Sometimes the journalist will repeat the question or ask in a different way because they realise they wanted a different angle.
4. **A live interview (audio or video):** these are very rare and are often done for urgent incidents. They require a lot of prep and training for the spokesperson. Where possible I would *avoid* doing live interviews unless you have complete confidence in the subject.

Preparation is key here.

When discussing an interview with a journalist always:

- Ask what topics will be covered.
- Tell them clearly what topics you will not talk about.
- Ask what type of interview it will be a how long it will take.
- Ask for questions ahead of time to prepare.

Journalists will often share questions or discuss the topics to cover with you because it means a better story for them. The worst thing for them would be an expert who can only "sorry I can't talk about that". If you have to do a TV interview, they are much more likely to give you questions ahead of time.

After you get that information, practice. It is a good idea to:

- Sit down and write out some ideas, then
- Work on responses and bounce them off others in your team.

If they ask to do the interview over Zoom, Teams or a similar platform, make sure you have a strong connection and use a headset as the microphone will better capture your voice. If they are recording video from the platform, try not to have any effects on the camera, including background blurring, it looks awful on a TV screen.

Finally try to get a copy of the published interview

People, media training and photography

Create a list of people who are available to talk to media. There may only be one. If you have more than one, choose who you think is best for the topic.

It's best if the spokespeople get media training of some kind. This can range from a professional course with a trainer, to a session with a communications person who can go over the basics with them. But anything is better than nothing.

There is no substitute for practice. Even if this means running dummy interviews and questions past the spokesperson. You can even take questions from previous interviews and think about ways you might answer them differently.

Also remember that simply because someone is an executive, that doesn't mean they are necessarily the best spokesperson for a cybersecurity topic.

This is an example from a larger organisation with multiple spokespeople at different levels:

Topic	**Person**
Incident response, cybersecurity information and advice	Manager of IR team
High level policy, statistics, annual reports	Director of CSIRT
Policy, international issues	Director of CSIRT, or higher if possible.

Every spokesperson will need good quality photos to share with any written response that includes them. 'Good quality' doesn't mean you need a professional photographer, but it does need to be of a high resolution. Each person needs at least four images:

- a formal photo in portrait and landscape, and
- a more casual option, in portrait and landscape.

This is because you do not want a smiling happy photo next to a headline that reads "Thousands of People Lose Money in Cybersecurity Attack". The different orientations are due to website requirements; some media outlets prefer landscape, some prefer portrait.

Media inbox

If you get a lot of queries, it can be good to create a media email address that is monitored by a few people.

Put an auto reply on it that says something like:

> Thank you for contacting [NAME OF TEAM].
> A member of the team will be in touch with you shortly.
> If your query is urgent or you are contacting us outside of office hours (8:30am-5pm), you can call on [YOUR PHONE NUMBER]. We aim to respond to emails within 60 minutes during office hours.

The '60 minutes' line is obviously up to your team but is a good rule of thumb.