To OOB, or Not to OOB?: Why Out-of-Band Communications are Essential…

Archived: 2026-04-05 18:54:29 UTC

tl;dr

- Out-of-band (OOB) communications are alternative systems or technologies that allow responders to collaborate, coordinate, and inform during an incident.
- OOB should not use any existing, normal infrastructure.
- OOB should provide email, voice, and real-time communications capabilities; mass one-way communications to employees, clients, and the public; and file storage.
- Ensure that your OOB solution meets any internal legal requirements.
- Set up OOB before an incident occurs.
- Test your OOB platforms.

Communications are critical during an incident. If you cannot coordinate, collaborate, and inform actions and information about an incident, the incident response will eventually fail. Normally, this isn't an issue, as organizations have resources like Microsoft 365 email, SharePoint, Slack, and Teams to use to communicate with each other. However, what happens when those technologies are unavailable? That is where OOB communications come in.

OOB communications are alternative technologies that are utilized outside of your normal, existing communications systems to allow response teams to collaborate during an incident. It is important to note that these technologies are **outsideof your existing infrastructure**–they are systems that you do not use daily and are not tied to your current communications systems or infrastructure. In other words, if you use M365 and Active Directory, then Teams is not OOB and neither is anything that uses AD authentication. OOB needs to be completely separate.

When is OOB needed?

OOB communications are commonly used when existing communications are *unavailable,* or they either are, or are suspected to be, *untrustworthy*. Examples of situations that could make systems unavailable include a vendor outage, a severe storm, a ransomware event, or a DDOS attack. During these times, OOB provides a backup to the existing systems' functionality.

Communications are considered untrustworthy if you are no longer confident that their confidentiality or integrity is intact. This often occurs either during an incident where the threat actor has successfully compromised your communications systems (usually email or chat) or when the possibility exists that they may have. Since you should keep your incident response actions confidential, organizations should automatically go OOB once an

incident reaches a high severity level or if they have indicators that their communications systems have been compromised.

It may sound unlikely that an attacker would use your communications systems against you during an incident, but it happens more often than many realize. In 2016, Nick Carr described a case he worked in which the attacker was targeting the external IR team, which the attacker knew about because they were monitoring the victim's email. In September 2022, an attacker who compromised Uber announced it by sending a message through the company's Slack. These are not isolated incidents but serve to highlight why OOB is necessary during an incident.

OOB may also be used when you need to reach many people at once. Some organizations have pager systems to contact all employees in the event of a disaster or outage. They are usually used for weather events but can also be used to let employees know the status of a major IT outage or security event.

What should OOB do?

OOB requirements look different for every organization. To determine yours, look at how you would need to communicate during an incident to organize, inform, and respond effectively. This should include:

- Email
- Real-time chat
- Voice
- Emergency one-way messages to all employees
- File storage
- External websites to communicate with clients, the media, or the public

Understand that you do not need to set up OOB for every employee, except for maybe having employees opt-in for the emergency one-way system. OOB communications should be restricted to only those who need to help the organization respond and recover from the incident. OOB should be looked at as a temporary system that is used while you recover your normal communications systems and ensure that their integrity has not been compromised.

One note on OOB file storage–be sure that whatever you choose has sufficient space to store anything within an incident, such as evidence. Additionally, upload any policies and procedures, such as Incident Response plans or playbooks, to the file storage before an incident occurs.

OOB considerations

For whatever OOB solution you choose, make sure that you meet any requirements from your legal team. Legal teams may require that OOB can log, save, or back up all communications, or that data is stored for a specific length of time. This could be required if a legal hold is put in place on the organization for the incident.

Additionally, examine the security and usage around the solution you use; don't just find something that is convenient. For example, many organizations I have talked to on Tabletop Exercises state that they use SMS texting or a free application, like WhatsApp, on personal devices for OOB. That sounds great until they realize that there may be little security around those applications and that using them on personal devices may also mean

that they could be compelled to turn those devices over during litigation. (It's funny how often requirements change once someone realizes that their personal device may be used in a work litigation.)

When should you set up OOB?

Yesterday.

OOB communications need to be set up **before** an incident occurs. Organizations that wait for an incident to find OOB solutions waste valuable time that could otherwise be spent investigating and recovering and may even find their OOB solution pulled away from them.

A great example of this occurred when the city of Baltimore was responding to their 2019 ransomware attack. They had instructed city employees to create Gmail accounts to continue operations. This not only violated Google's policies for free accounts, but it also set off security alarms when many Gmail accounts were created from the same location. Google subsequently locked or deleted all the new accounts, and Baltimore's OOB email system was no more.

Additionally, don't set up your OOB and forget about it. Test your OOB on a yearly basis (at minimum) to ensure that it works as expected and that everyone can connect. You may also consider having devices, such as tablets, that are preconfigured to connect to OOB platforms. This will ensure that operators can open the tablets and connect without having to remember how to use OOB.

Don't reinvent the wheel!

The good news is that organizations may already have OOB systems. Communications and business continuity teams frequently have OOB systems for disaster recovery or to communicate with employees during events, such as severe weather. Incident Response teams can often piggyback on these solutions to use during a cyber security incident, and if you already have the solution in-house, chances are the procedures to use them have already been written.

OOB communication systems are a reality that organizations need to plan for. Taking the time now to set up OOB for needed communications will save the organization many headaches–both technical and operational. In turn, this allows responders to focus on what matters–getting the organization back up and running.
