

Name: Cristian Barreno

Out-of-Band communications and Cybersecurity.

Out-of-Band (OOB) communications are crucial in an organization during a cyber attack. Some examples that an organization needs to implement OOB communications are ransomware attacks, DDOS attacks, and when internal communications are suspected to be untrustworthy.

Setting up or figuring out how to set up OOB communications during a cyber attack wastes time for the organization. It's better to be proactive and set up OOB communications. It could be something simple or maybe something complex like a cloud base solution. It's important to emphasize that OOB communications are completely separate from the day to day communication infrastructure. Test your OOB communications at least once a year, and conduct training for the people involved in a cyber attack.

Threat actors can monitor and infiltrate the victim's email, and cell phone chats in their personal cell phones. So it's key that staff don't use personal cell phones as OOB communications.

