CYGNVS

# The **CISO’s** guide to **Out-of-Band Incident Response Management**

# Table of Contents

# Major cybersecurity incidents don’t stay within the walls of IT and Security.

They disrupt business operations, trigger regulatory scrutiny, and often unfold under public and board-level pressure. Responding to these incidents requires coordination not just among technical teams, but also across executives, legal, communications, and boards. And in nearly every major incident today, external vendors like forensic firms, outside counsel, and insurance providers also play critical roles.

**Yet some organizations still try to manage this complexity** with disconnected systems, generic collaboration apps, or even consumer messaging apps. That approach breaks down under pressure, especially when core systems are down or compromised.

**This guide is for CISOs** ready to move past that chaos. You’ll learn what out-of-band platforms are and how they create a secure, independent command center for managing cyber incidents, enabling continuous communication, collaboration, and documentation even when your core systems are unavailable.

**You’ll also learn how out-of-band platforms improve resilience** through preparation, practice, and reporting capabilities. Organizations that manage the full incident response lifecycle in a secure out-of-band environment consistently reduce breach costs, accelerate recovery, strengthen regulatory posture, and increase board confidence.

> **Establish secure out-of-band communication channels to ensure the continuity of critical communications during security incidents, data integrity attacks, or in-network communication failures.**
>
> - MITRE ATTACK Mitigations M1060

# Where Incident Response Breaks Down

Most organizations have at least basic incident response plans. Some even run an annual tabletop exercise. But during an actual incident, those plans often fall apart. Not because the threat isn't detected, but because the response breaks down. The weak links aren't always obvious until you're in the midst of a crisis, but they lead to slower response, regulatory missteps, legal exposure, and higher breach costs.

## HERE'S WHAT THAT LOOKS LIKE DURING AN INCIDENT

### Mobilization Stalls

The first minutes and hours are critical. But if SSO, Active Directory, or email is down, even assembling the right people takes too long. Teams scramble to identify and verify responders and spin up alternative channels, losing valuable time.

### Status Pressure

Leadership demands regular updates on impact, progress, and next steps. In fact, 50% of the time in an incident is spent updating others. No live, role-based roll-up means responders stop working to craft one-off communications and updates, and leaders get different versions of the truth.

### Evidence and Reporting Chaos

The disclosure clock is ticking. When artifacts are spread across tickets, chat, and shared drives, this leads to conflicting redlines, lost legal privilege, and delayed disclosures.

### Vendor Coordination Delays

Outside counsel, forensics, insurance, and supply-chain partners need to be brought in, non-disclosure agreements (NDAs) signed, and figuring out what data needs to be shared with whom slows down response, leading to side channels spinning up, loss of chain of custody, and delays.

### No Secure Centralized Workspace

The lack of a secure, central place for everyone to collaborate means teams scatter across channels, leading to decision delays, duplicate work, and conflicting updates.

### Threat Actor Eavesdropping

Teams often keep using in-band channels because "it's faster." But adversaries are known to monitor those communication channels, tipping them to response moves, resulting in proactive countermoves by attackers and delayed containment.

# What Are Out-of-Band Platforms?

Out-of-band platforms are purpose-built for managing cybersecurity incidents when your core systems are compromised, down, or not designed for cross-functional crisis response. They don't replace your security operations center (SOC) or IT tools. They sit alongside them, covering the human side of response: creating a secure command center for communication, coordination, and decision-making across security, IT, business teams, and external providers.

This distinction is at the heart of **cybersecurity incident response management (CIRM)**, the emerging category Gartner has now defined. CIRM reflects what security leaders already know: detection and automation tools aren't enough. Without a secure, organized way to prepare, mobilize the business, and manage response, incidents spiral into chaos. And without out-of-band capabilities, you don't really have CIRM - you just have another tool with the same blind spot.

> **After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods.**
>
> #StopRansomWareGuide-CISA

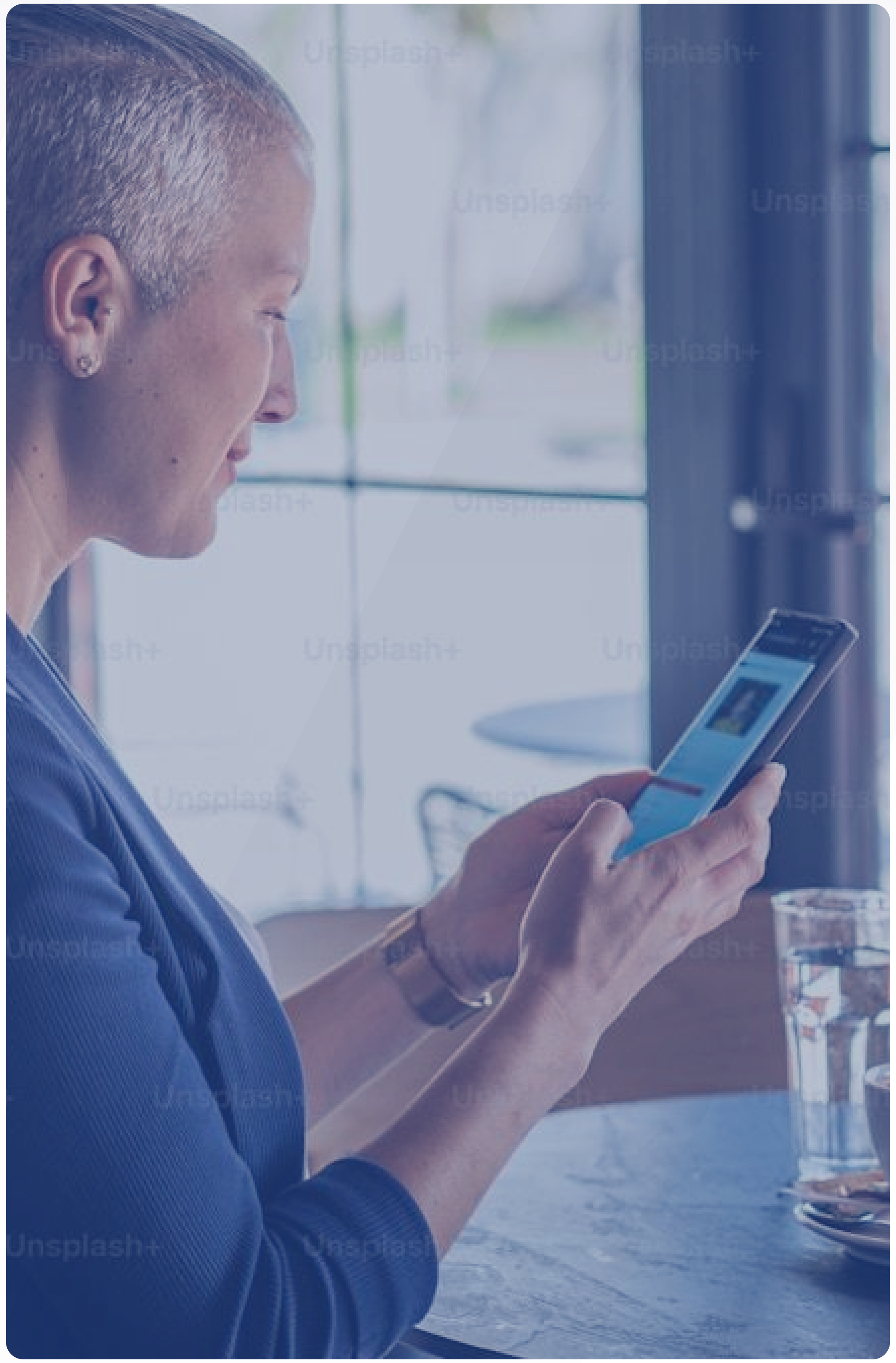
# How Out-of-Band Platforms Differ from **Messaging and Collaboration Apps**

Corporate collaboration apps like Slack, Teams, and Google Docs are essential for daily productivity, but they collapse during an incident. If SSO or corporate networks are down, you're locked out. Even when they are accessible, you can't assume they're safe: attackers often monitor corporate chat and file-sharing systems. These apps also weren't designed to manage playbooks, securely coordinate external vendors, or preserve defensible audit trails.

When corporate tools fail, many teams default to personal messaging apps like WhatsApp and Signal. But these are not managed by the organization and not designed for the specific needs of cyber incidents, creating serious risks:

- No audit trail or chain of custody to defend decisions later.
- No role-based controls – anyone added to a thread sees everything.
- Disappearing or encrypted messages may violate legal hold requirements.
- Screenshots are easily falsified and don't meet evidentiary standards.

An out-of-band platform alleviates both risks. It provides a sanctioned, secure environment purpose-built for incident response that's available even if corporate systems are unavailable.

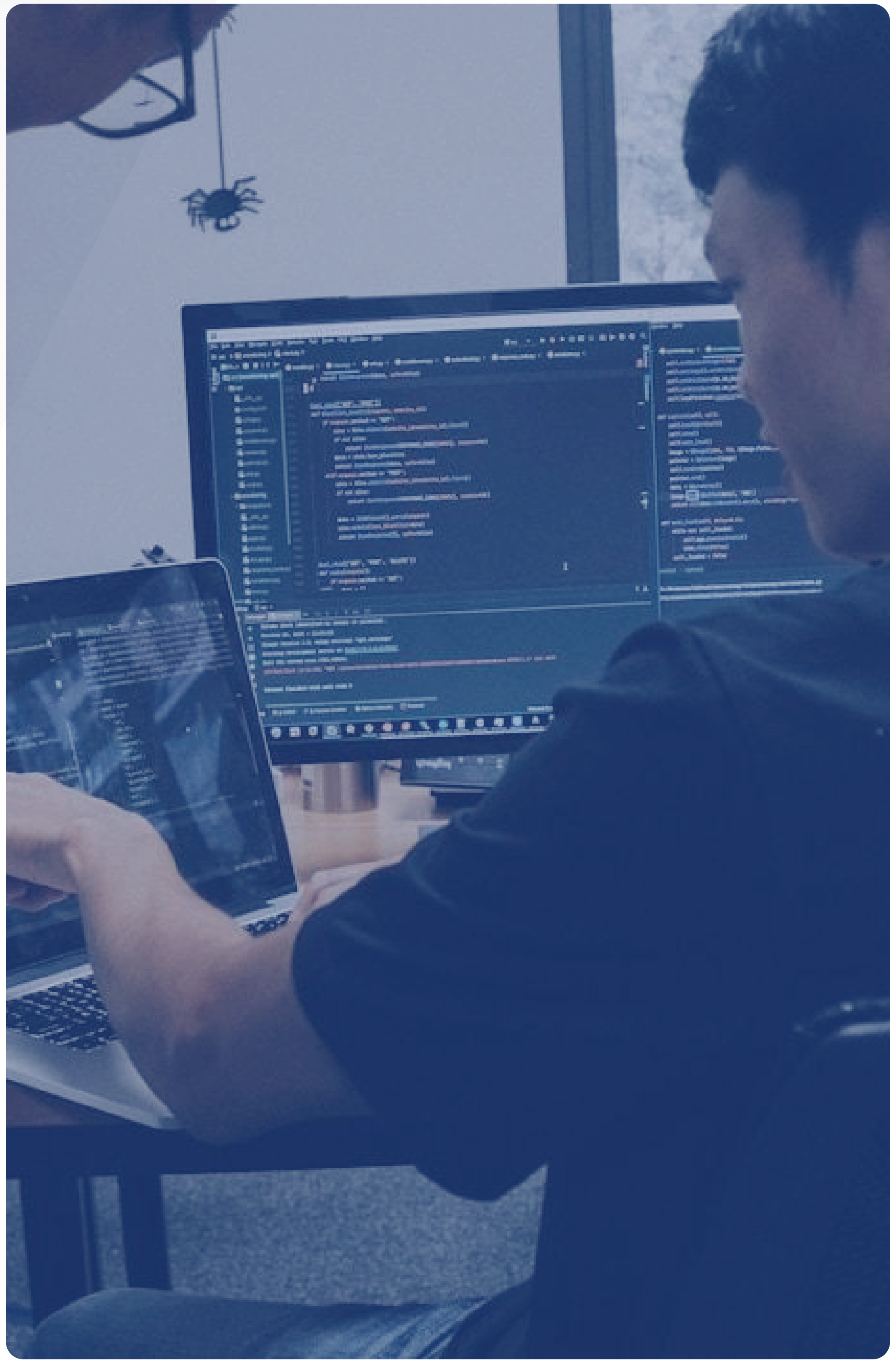


# How Out-of-Band Platforms Differ from **SIEM and SOAR Tools**

Tools like SIEM (Security Incident and Event Management) and SOAR (Security Orchestration, Automation, and Response) are foundational to security operations. SIEM aggregates logs and telemetry to help security teams detect threats, while SOAR, either as part of the SIEM platform or standalone, automates technical response actions based on those alerts.

But alerts don't stop at the SOC. Once an alert escalates to a major incident, the circle expands: executives, legal, corporate communications, HR, insurers, regulators, outside counsel, and more. SIEM and SOAR were never built to coordinate those teams. At best, some SOAR tools had a "war room" for technical teams, but it was not enough when your lawyers, your PR team, even your CEO needed to be in the loop, executing their own tasks.

That's why Gartner created the CIRM category: to capture the need for coordination, visibility, and accountability across the entire business. And this is why out-of-band platforms are foundational. They extend incident response beyond the SOC, mobilizing and orchestrating business teams, executives, and external vendors, tracking actions to resolution, and creating a secure, auditable system of record.



# How Out-of-Band Platforms Differ from **Critical Event Management/Mass Alerting Tools**

Critical Event Management (CEM) platforms like Everbridge and BlackBerry AtHoc are best known for mass alerting during natural disasters, infrastructure outages, or physical safety incidents. However, they weren't designed for cybersecurity incident response and lack essential capabilities for managing cyber incidents:

- Out-of-band identity management for when corporate identity/SSO are compromised or unavailable.
- External provider onboarding/offboarding with data custody controls.
- Collaboration capabilities like video conferencing, screen sharing, and file editing.
- Cyber-specific playbooks either pre-built or generated for common incident types.
- Tabletop exercise environments to rehearse cyber incidents.
- Regulatory reporting libraries covering multiple jurisdictions.
- Full audit trails for legal and forensic defensibility.

Out-of-band platforms should integrate these cyber-focused capabilities while also supporting mass alerting when needed. For example, they can simultaneously notify employees to avoid compromised corporate email while coordinating privileged response discussions among leadership and external partners.

CEM tools are great at notifying large populations of emergencies. Out-of-band platforms orchestrate the cyber incident lifecycle with built-in communication, coordination, and compliance capabilities.

# The Urgency of Resilient Response

## Cyber Threats Are Evolving And Accelerating

Ransomware and data extortion remain persistent and increasingly sophisticated. Ransomware accounted for **28% of malware incidents** in 2024, with dark web data showing a 25% year-over-year rise in activity. At the same time, attackers have rapidly adopted gen AI, fueling a **1,265% surge** in phishing attacks. Out-of-band platforms offer a secure, accessible environment when your primary infrastructure is under siege.

## Regulatory Pressure Is Increasing

Disclosure deadlines are getting shorter, with the **SEC** requiring material incidents to be disclosed within four business days, and the **NIS2 Directive** mandating reporting within 24 hours for critical infrastructure. **NIST CSF 2.0** and **DORA** explicitly emphasize the need for resilient, alternate communication channels to ensure continuity and defensibility in a crisis. Out-of-band platforms address these expectations.

Ransomware accounted for **28% of malware in 2024,** with dark web showing a 25% year-over-year rise in activity.

# The Urgency of Resilient Response

## Cyber Incidents Are Business Continuity Risks

The **average cost of a data breach** in 2025 is $10.22M in the US and $4.44M globally, with 86% of breached businesses experiencing disrupted operations. As **Gartner** notes, “Financial losses due to incidents are often related to incident handling from secondary teams, such as legal,” underscoring that damage is often organizational, not just technical. Out-of-band platforms keep collaboration and decision-making moving during disruption.

## Supply Chain Attacks Require Joint Coordination

Supply chain attacks have surged, with incidents **rising 431%** between 2021 and 2023. In 2024, nearly **1 in 3 reported attacks** originated via third parties. These threats transcend organizational borders, forcing coordination between vendors, security, legal, procurement, and risk teams. Without secure, out-of-band systems to bring everyone together, response slows, and exposure widens.

Supply chain attacks have surged, with incidents **rising 431%** between 2021 and 2023.

The average cost of a data breach in 2025 is **$10.22M** in the US and **$4.44M** globally.

# Why CYGNVS

CYGNVS is the market leader in out-of-band platforms, purpose-built to reduce the time, cost, and business impact of incidents and outages. Security, IT, business teams, and external providers collaborate inside CYGNVS to prepare and store response plans, practice playbooks in tabletop exercises, successfully execute response, and report to regulators and customers. This full lifecycle approach is why customers and insurers trust CYGNVS to turn chaos into peace of mind.

Trusted By

**2,500+**

Organizations

**2,600+**

Major Incidents Managed Annually

Endorsed By

**Top Cyber Insurers**

CYGNVS

**Get Started**

## Insurer Access

Many cyber insurers provide a limited version of CYGNVS to policyholders as part of their coverage.

Check with your insurer to see if you already have access.

## Contact Us

Want to learn more about how CYGNVS can strengthen your resilience strategy?

Visit **CYGNVS.com** or ***contact us*** to speak with our team.