CYGNVS

Solution Brief

Incident Types on CYGNVS

Learnings from 2,500 CYGNVS Customers on when to use CYGNVS

CYGNVS Customers weighed in on the benefits of the platform across a variety of incident types. Customers reported use cases and usage scenarios spanning ransomware, critical incidents, Supplier incidents, privacy investigations, system outages, regulatory compliance, and incident recovery.

Ransomware

Customers shared CYGNVS was their "go to" platform when investigating a potential Ransomware incident. When existing systems including Single Sign On (SSO) or Active Directory are unavailable or compromised, CYGNVS is the out-of-band platform completely isolated from the organization for IT/Security, Business Teams and External Providers to communication and execute the incident response plan and recovery.

Critical Incidents

Customers surveyed are leveraging CYGNVS for managing Severity-1 and Severity-2 level incidents. To quote one Customer, "When you start pulling on that thread, you never know where it might lead – and Legal Privilege once lost cannot be reinstated." By leveraging CYGNVS for critical incidents, Customers ensure that from the beginning, Business Teams and External Providers (like forensic teams and law firms) are engaged, and information is controlled and protected, ensuring legal privilege and chain of custody throughout the investigation.

Supplier Incident Management

Customers report that two thirds of their major incidents emanate from their key Suppliers. In such an event, Customers immediately cut access, email, and integrations to the Supplier. CYGNVS then becomes the platform to securely communicate and collaborate with the Supplier and any third parties throughout the incident. The playbook for Supplier resolution is run inside CYGNVS to ensure that the Customer is satisfied with before reconnecting. Customers reported using CYGNVS to benchmark various Suppliers on their conduct and performance during their respective incidents.

Privacy Investigations

Customers benefit from conducting privacy investigations within CYGNVS. Whether investigating a malicious insider or potential data exposure, CYGNVS is used for conducting privacy investigations completely out-of-band ensuring integrity, fidelity, and auditability. Customers need to protect privacy investigations with Legal Privilege, while maintaining communications and investigation details outside of their systems.

System Outages

With the increasing complexity of technology dependencies, system outages are becoming more frequent. Customers leverage CYGNVS during an outage – even when communications are not impacted. CYGNVS becomes the platform for IT teams to manage the outage and connect with Business Teams, External Providers, and the organization's own Customers.

Regulatory Compliance

With the increasing number of cyber disclosure and regulatory reporting requirements, CYGNVS helps organizations prepare regulatory filings and submit disclosure reports. Customers stated using CYGNVS allows them to securely prepare incident reports with External Providers, demonstrating chain of custody, and maintaining legal privilege throughout the process.

Incident Recovery

To securely recover from a cyberattack, organizations must restore systems to the most recent clean version. Customers use CYGNVS as a secure offline vault to actively sync recovery plans, system configurations, and active directory recovery scripts. This helps accelerate recovery post incident to minimize business interruption.

INFO@CYGNVS.COM
4940 EL CAMINO, SUITE 100, LOS ALTOS, CA 94022 USA