

## Ransomware & Life-Safety

TACTICAL INTELLIGENCE REPORT // 2026

### Beyond Encryption: Total Chaos

Ransomware in 2026 is a public safety issue. Attackers now prioritize 'Life-Safety' systems to ensure the highest possible payout pressure.

### Case Study: OnSolve Emergency Alerts (Nov 2025)

#### THE LIFE-SAFETY PIVOT

The INC Ransomware group targeted OnSolve, a platform used for state-level emergency alerts. By disabling the notification system, they effectively held the safety of millions hostage. The pressure to restore service forced a rapid settlement, proving that the modern blast radius is no longer just digital—it is physical.

### The 3-2-1-1 Resilience Model

Standard backups are dead. You need the **3-2-1-1 Model**: 3 copies, 2 media, 1 offsite, and 1 **IMMUTABLE AIR-GAP**. If your backup admin account is compromised, the air-gap is your only savior.

### Operational Best Practices

#### The Kill Switch

- **Micro-Segmentation:** Ensure that your Accounting department cannot even 'see' the Production server on the network.

- **Canary Files:** Place hidden files in your directories that trigger an immediate network shutdown if modified.