

# The Five Ways Organisations Fail at Incident Readiness

## And What High Performers Do Differently



### Overview

**Format:** Keynote or Conference Session

**Duration:** 45–60 minutes (adaptable to 30 minutes)

**Audience:** Security leaders, incident response teams, executives

Most organisations believe they are prepared for cyber incidents – until they are tested under real conditions.

**The Five Ways Organisations Fail at Incident Readiness** presents a pattern-based analysis of the most common readiness failures observed across real incidents, tabletop exercises, and response engagements. Rather than focusing on tools or maturity models, this session examines how organisational design, decision authority, and assumptions undermine response when it matters most.

The result is a clear, practical view of what actually separates high-performing organisations from those that struggle.

### What This Session Covers

The talk walks through five recurring failure patterns, including unclear authority, untested playbooks, weak evidence handling, poor cross-functional coordination, and unrealistic assumptions about tooling. Each pattern is illustrated with real-world examples and contrasted with how effective organisations design their response capability differently.

The emphasis is on readiness as a lived capability, not a documented one.

### Key Takeaways

Attendees gain a practical framework for assessing their own readiness, identifying the highest-impact gaps, and prioritising improvements that meaningfully change response outcomes. The session avoids large transformation programs in favour of achievable, defensible steps.

### Why This Talk Resonates

This session resonates because it is recognisable. Audiences consistently see their own organisations reflected in the patterns discussed, making the recommendations immediately relevant and actionable.

### Delivery Style & Customisation

Direct, practical, and grounded in experience. Content can be tailored for enterprise, critical infrastructure, or regulated environments, and delivered to technical, leadership, or mixed audiences.

**Presented by Seth Enoka**

Director & Principal Analyst, Lykos Defence

Author, Cybersecurity for Small Networks (No Starch Press)