Cyber Chaos to Organisational Resilience

Our role as Cyber Leaders in Crisis Leadership

Nigel Hedges | **July 2025**

Why This Matters **Now**

⬆️ Cyber incidents escalating into organisational crises

🚫 Gap: Incident responders ≠ Crisis leaders

✅ Goal: Practical methods to bridge this gap

Why Cyber Leaders can drive Proactive Leadership?

🔍 **High Contact experience:** Cyber incidents = High-visibility business crises

🧠 **Defensible Strategy experience:** Mindset shift: From tactical to strategic

🏆 **Business orientation:** Goal - Lead beyond technical resolution

Lots of Different Forms of Crisis

Crisis can manifest from several common critical events.
(not limited to these crises)

| Supply Chain Disruption | Failure of Critical IT Systems | Utility Outage | Cyber Attacks or Threats | Physical or IP Theft | Natural Disaster | Acts of Violence | Pandemic | Customer / Staff Injuries |

Snapshot: When Incident Management Fails

❌ Example: Credential Harvesting / Data Breach

💡 Issue: Poor leadership, chaotic communication, business disarray

✅ Lesson: Leadership mindset reduces crisis impact

5 Benefits of ISO 22361

👥 Drives Leadership accountability

📈 Preparedness culture

🛠️ A flexible structured approach

🤝 Encourages transparency

🔄 Continuous improvement

Differentiating Issue and Crises

- Frequently, *issues* are generally solved through operational management response.

- Poorly managed issues can manifest into *incident(s)*, and if not careful can become crises.

- *Crises* can be the escalation of poorly managed issues & incidents, but they can also come out of left field and escalate quickly without warning.
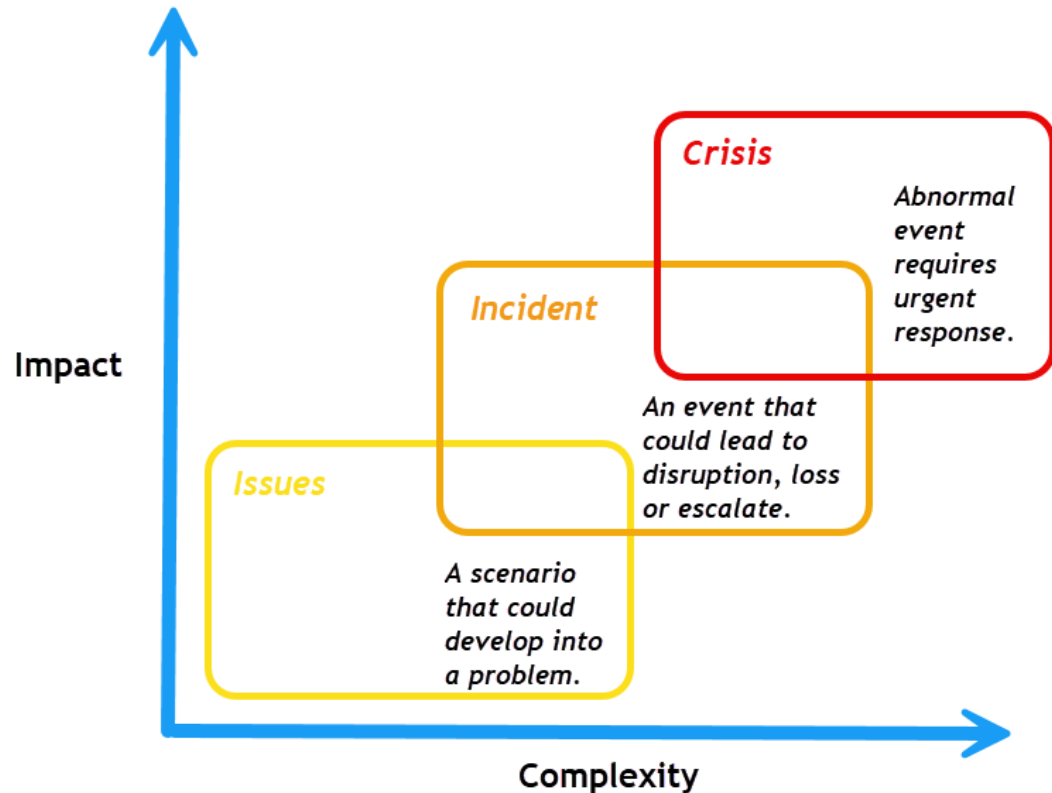
The take-away: **We need to always be clear when something is an issue, an incidents or a crisis.**

Impact

Crisis

Abnormal event requires urgent response.

Incident

An event that could lead to disruption, loss or escalate.

Issues

A scenario that could develop into a problem.

Complexity

Understand the Stages

The Crisis Management Process starts well before a declared crisis starts or ends. It should include pre-crisis planning and post-crisis learnings.

The Process for Crisis Management Response is a means to make decisions during the crisis itself.
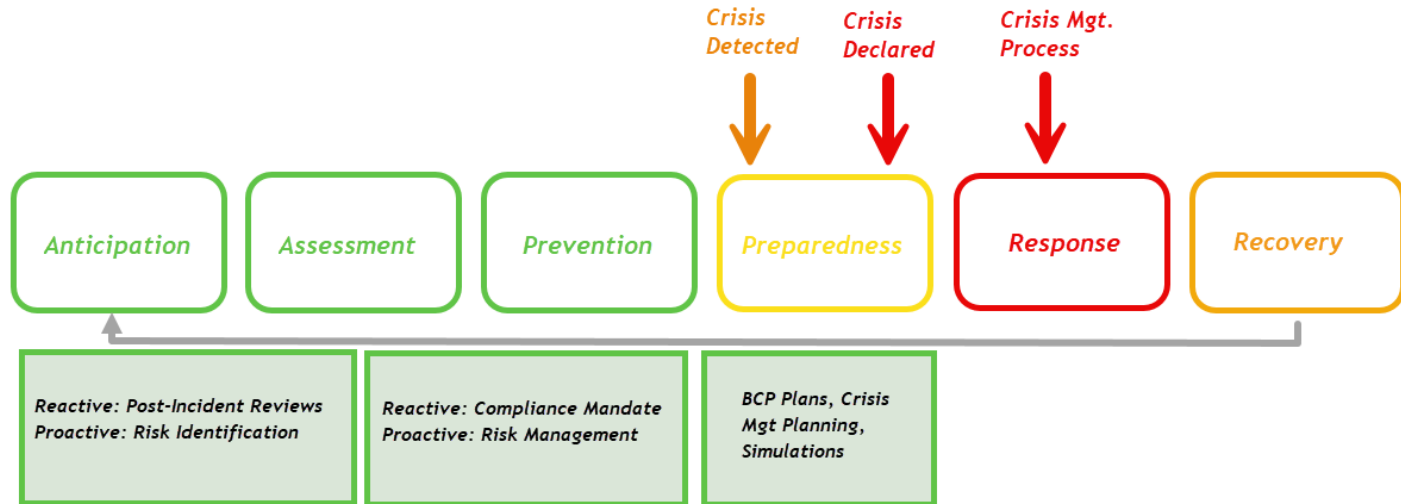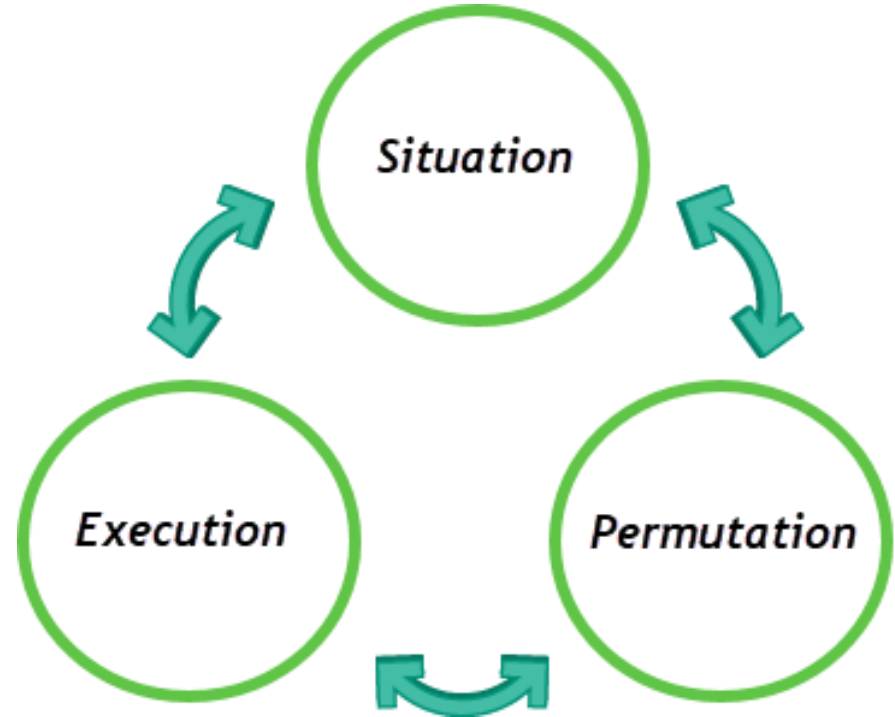
Understand the Process

The Crisis Management Process in a nutshell:

- What's the current situation?
- Are we aware of the scenario we are in?
- What are the current repercussions or consequences we are facing? **//**
- What is out objective going to be?
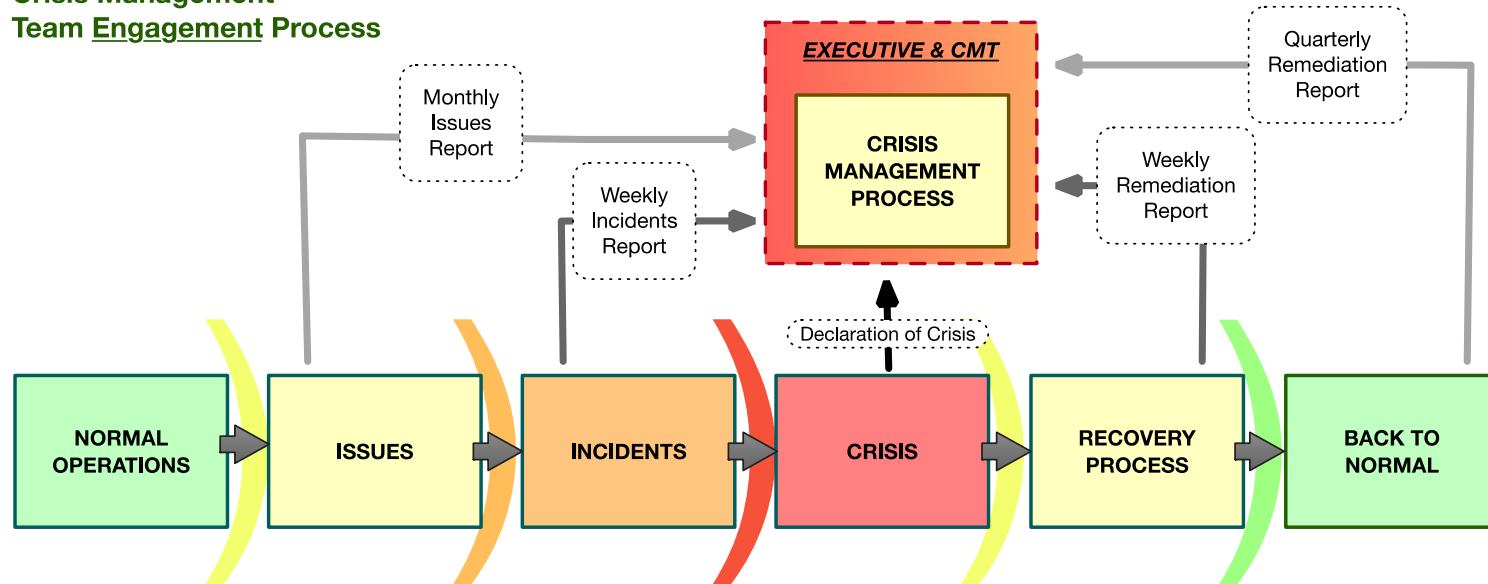- What's the plan and priorities?
- Take the course of action!

Repeat…

Communication with Executives

How the Executive (and CMT) teams should expect to receive intel before, during and after crises.
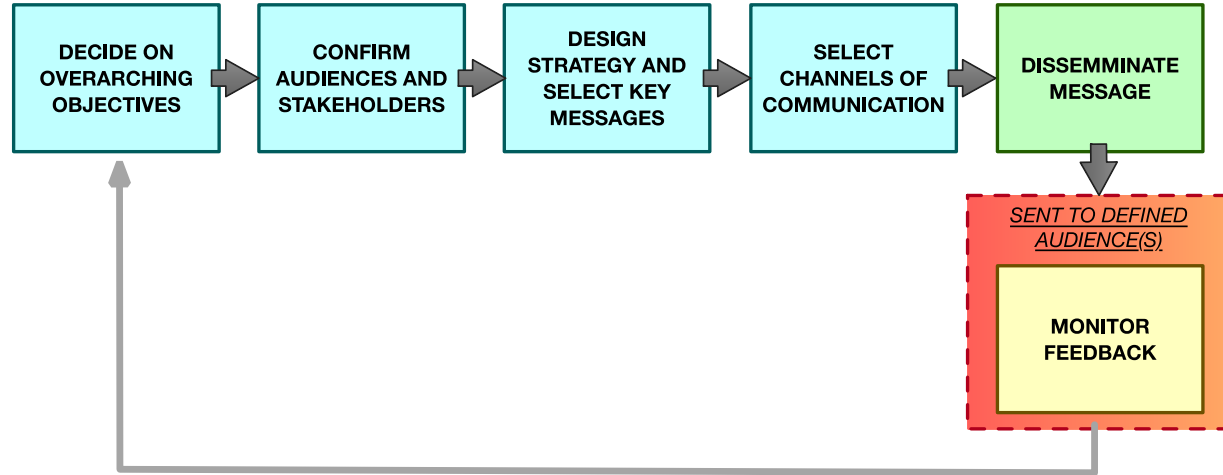
Communication during Crisis

Consistent Messaging and messaging process encourages perception of competence, confidence and reliability.

Steps:

1. Communication objectives should be clear.

2. Confirming all appropriate audiences and stakeholders are determined.

3. Have a clear communication strategy with intended effects and key messages.

4. Select the most appropriate channels of communication for maximum effect.

5. Commit to sending the message(s).

6. Monitor feedback from communications message and repeat if/when communications are needed further.

Crisis Management Communication Workflow

| DECIDE ON OVERARCHING OBJECTIVES | → | CONFIRM AUDIENCES AND STAKEHOLDERS | → | DESIGN STRATEGY AND SELECT KEY MESSAGES | → | SELECT CHANNELS OF COMMUNICATION | → | DISSEMMINATE MESSAGE |

SENT TO DEFINED AUDIENCE(S)

MONITOR FEEDBACK

NOTE: Crisis Management outcomes excel when all teams from the domain impacted, Communications and Legal are treated equally.

Crisis Bridge Abstractions

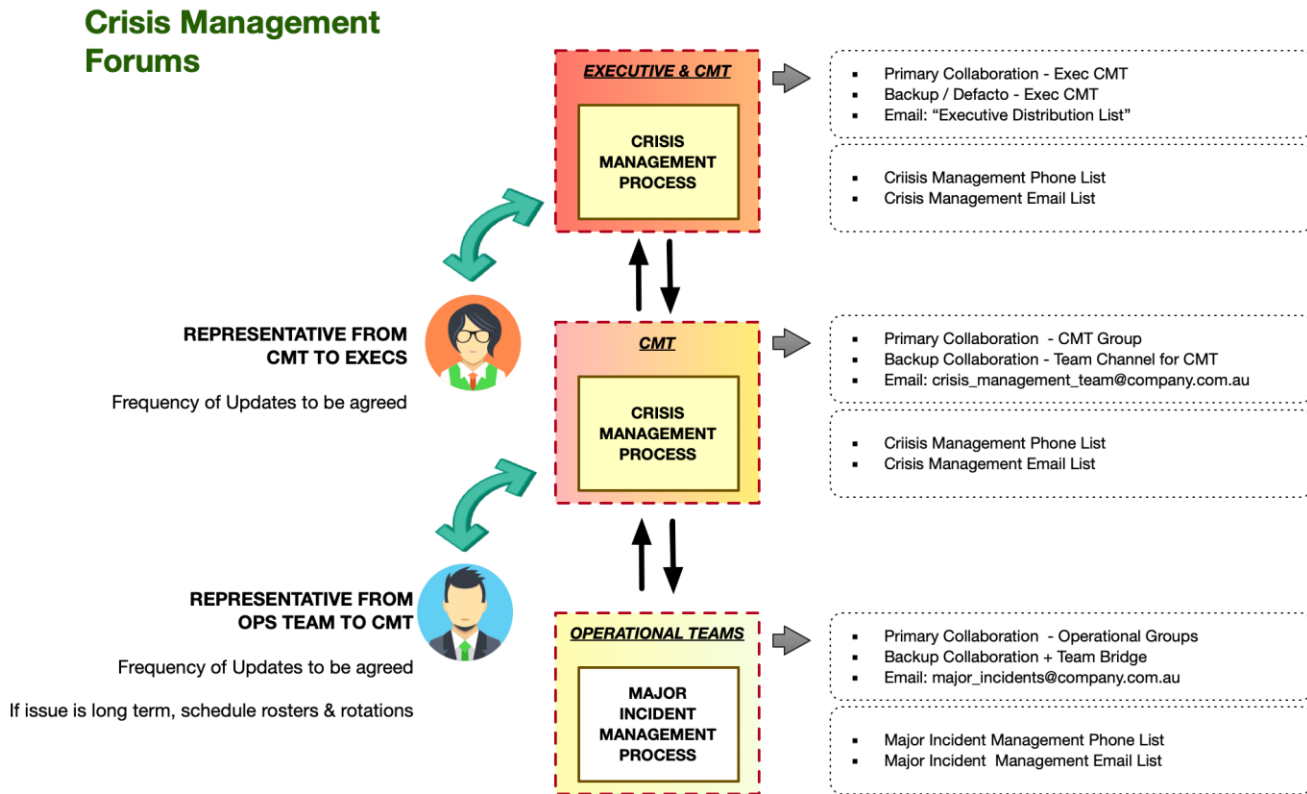There are 3 layers of crisis management proposed:

- **Executive CMT**

The most senior decision-making and authority operates at this level. All final calls are made here.

- **CMT**

The CMT engages with Operational Teams for decision making on authority and delegation from Executive CMT.

- **Ops Teams (for Incident)**

Operational teams will engage with major incident management process and provide updates to CMT.

Crisis Management Forums

EXECUTIVE & CMT

CRISIS MANAGEMENT PROCESS

- Primary Collaboration - Exec CMT
- Backup / Defacto - Exec CMT
- Email: "Executive Distribution List"

- Criisis Management Phone List
- Crisis Management Email List

REPRESENTATIVE FROM CMT TO EXECS

Frequency of Updates to be agreed

CMT

CRISIS MANAGEMENT PROCESS

- Primary Collaboration - CMT Group
- Backup Collaboration - Team Channel for CMT
- Email: crisis_management_team@company.com.au

- Criisis Management Phone List
- Crisis Management Email List

REPRESENTATIVE FROM OPS TEAM TO CMT

Frequency of Updates to be agreed

If issue is long term, schedule rosters & rotations

OPERATIONAL TEAMS

MAJOR INCIDENT MANAGEMENT PROCESS

- Primary Collaboration - Operational Groups
- Backup Collaboration + Team Bridge
- Email: major_incidents@company.com.au

- Major Incident Management Phone List
- Major Incident Management Email List

Develop Competencies

Crisis Management requires a blend of 4 types of skills:

1.   Ability to manage tasks.
2.   Ability to get the most out of others.
3.   Ability to manage oneself.
4.   Ability to manage relationships and engagements.

Take away: Developing these skills in-house across the CMT is the primary objective, not finding *'purple squirrel'* individuals.

Bringing ISO 22361 Into Cyber Playbooks

⚙️ Map ISO principles to response lifecycle

📊 Enable executive decision checkpoints

🎮 Train SOC → Executive handover moments

Crisis Leadership Ideas

- 📄 Decision log templates
- 📊 Executive situation dashboards
- 📈 Escalation triggers & criteria
- 🕐 3-min executive leadership huddles

📚 Playbooks = technical guides

🌐 Playfields = flexible decision frameworks

🏆 Goal: Equip teams for structured flexibility

Closing Summary

🚀 Evolve from responder to crisis leader
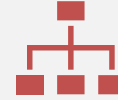
✅ Self-assess leadership strengths & gaps

📏 Embed ISO 22361 for structured response

📄 Review crisis governance & ISO alignment

⚡ Equip teams with adaptive frameworks

🚀 Take action in the next 90 days

Thanks!

Nigel Hedges ✓ 🔊 He/Him
Executive General Manager - Cyber & Risk (CISO) @ Sigma
Healthcare & Chemist Warehouse

❓ How confident is your team in leading through crisis?

💬 Let's discuss your biggest challenges