CANSO

CANSO GLOBAL SAFETY CONFERENCE 2025

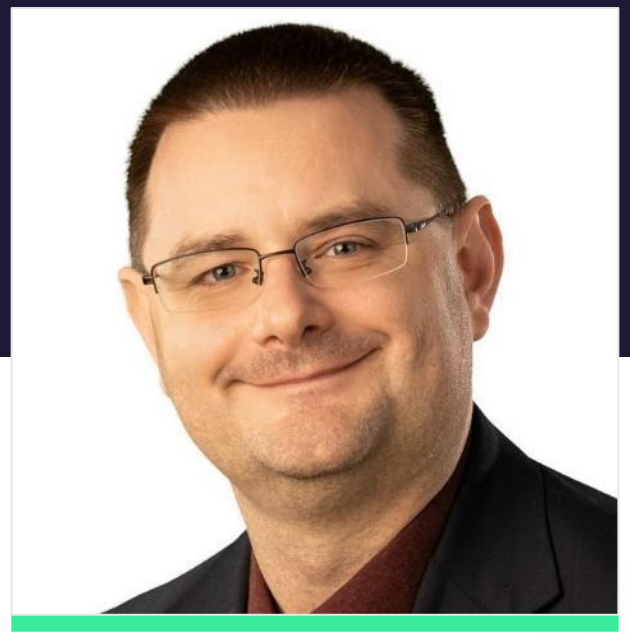
24 – 28 MARCH 2025 • CHRISTCHURCH, NEW ZEALAND

HOSTED BY AIRWAYS

RETURNING TO SERVICE AFTER A CYBER INCIDENT

ORGANISER CANSO HOSTED BY AIRWAYS

PRESENTER



Andy Boff

Technical Director for Cybersecurity

Egis

An uncomfortable question...

*What if, despite all the steps to protect our systems against cyber threats, an **incident** occurs?*

WHAT MIGHT IT LOOK LIKE?

Impact

- Core data missing – loss of **availability**
- Data obviously wrong – loss of **integrity**
- Data subtly wrong – also loss of **integrity**
- Sensitive data “leaked” – loss of **confidentiality**
- Data inconsistent across the system – loss of **timeliness**

Path of compromise

- Undetected & unprotected vulnerability
- Direct attack
- Data compromise
- Social engineering
- Through a trusted supplier

To start with, we won’t have all the information.
Investigation will be needed

HOW DO WE REALISE THERE'S AN INCIDENT?

The Good Way

- We notice an unauthorised change in the system baseline
- Monitoring tools highlight unusual activity
- Threat intelligence feeds inform us of an Indicator of Compromise

The Bad Way

- Unexpected system failures
- Undetected loss of safety barriers
- Incorrect processing
- Performance loss
- Incorrect data
- Or worse...

SO WE HAVE A CYBER INCIDENT – WHAT NOW?

Immediate objectives

- Limit the damage
- Protect safe operation
- Regain control of the situation
- Find out what happened

Longer term considerations

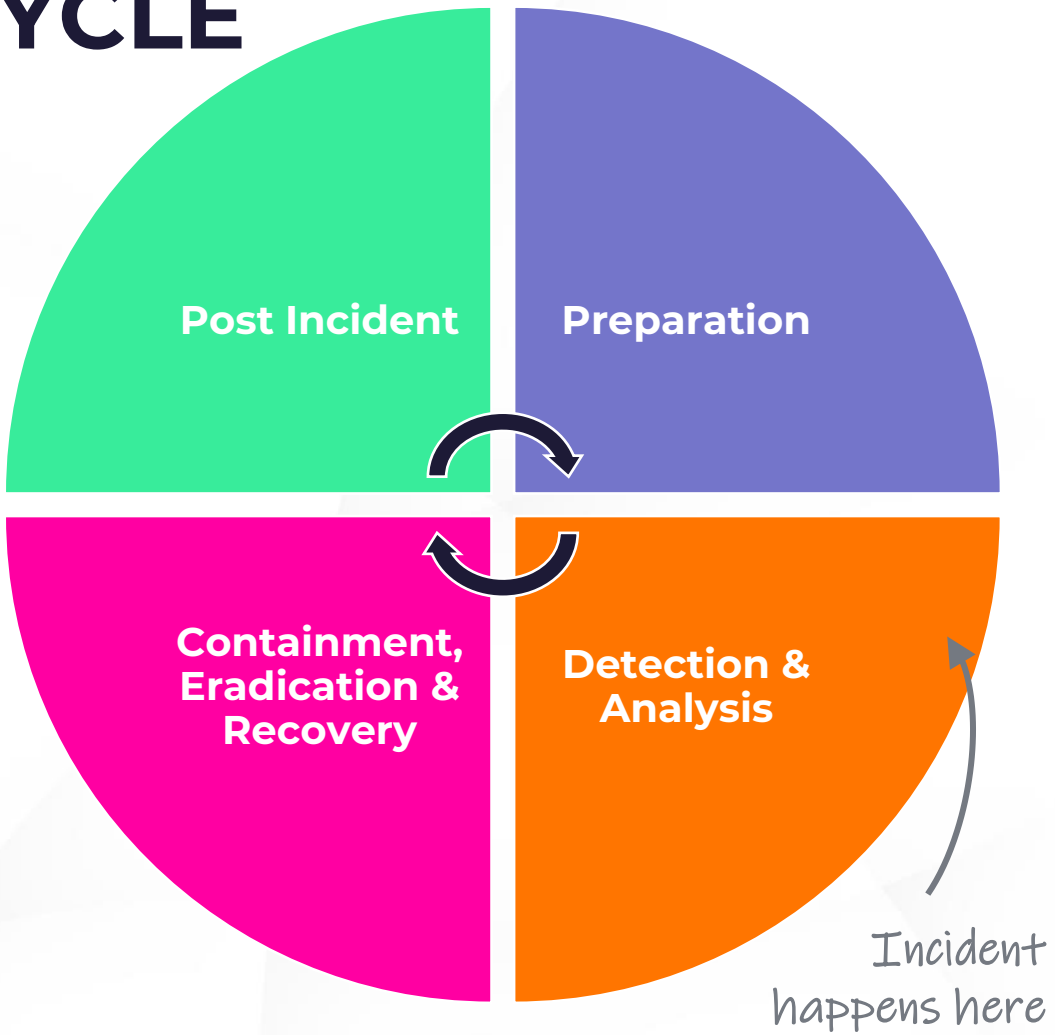
- How do we bring our service back?
- How do we communicate with stakeholders?
- How do we regain trust in our systems?
- How do we stop it happening again?

INCIDENT HANDLING LIFECYCLE

Incident response has a well defined lifecycle

In this instance, we're looking at the lifecycle defined in **NIST Special Publication 800-61**

This is specifically about handling Computer Security Incidents



1. PREPARATION

This is before the incident

(and it lays the foundations for success)

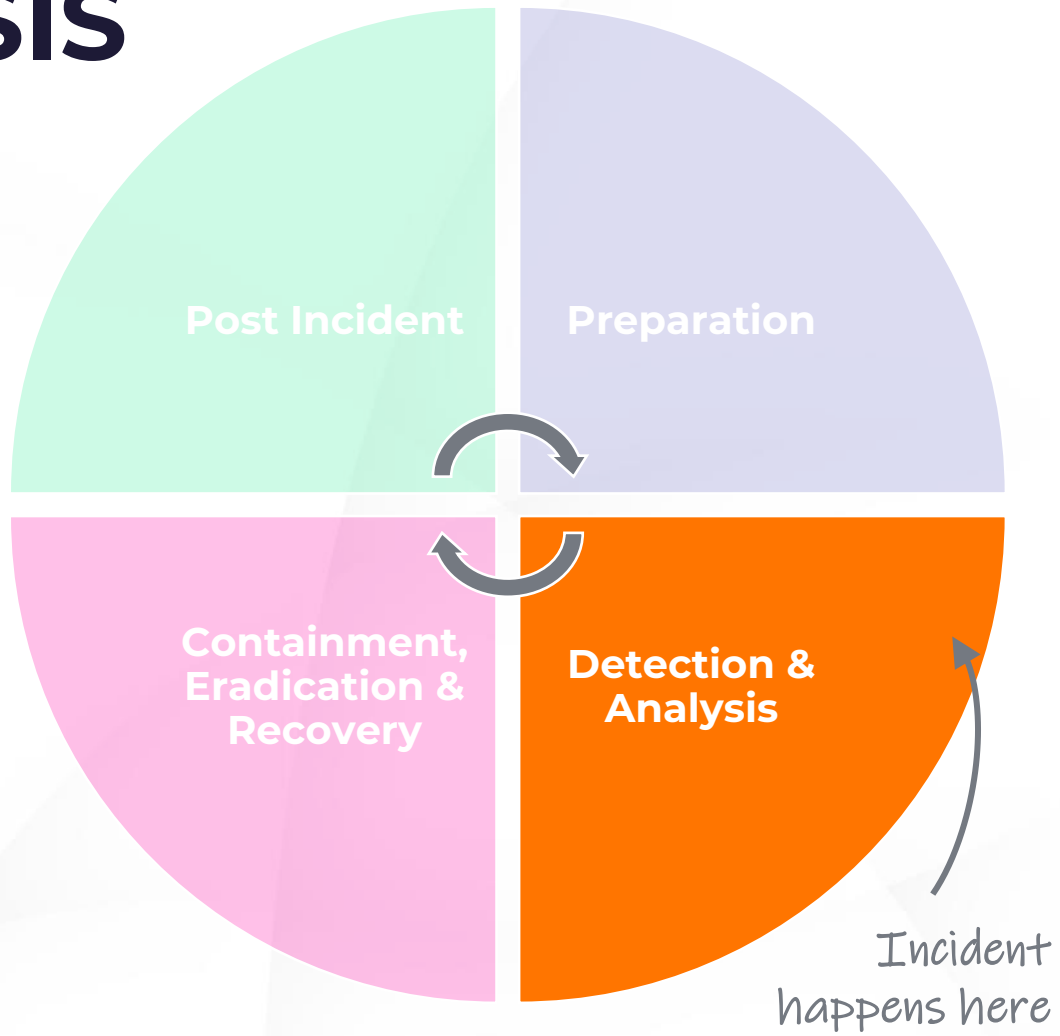
- Planning
- Staff Training
- Exercises
- Test Plans
- Build capabilities in advance

2. DETECTION & ANALYSIS

An incident has occurred

(and how soon we notice matters)

- Continuous Monitoring
- Threat Intelligence
- Indicators of Compromise
- Root Cause Analysis

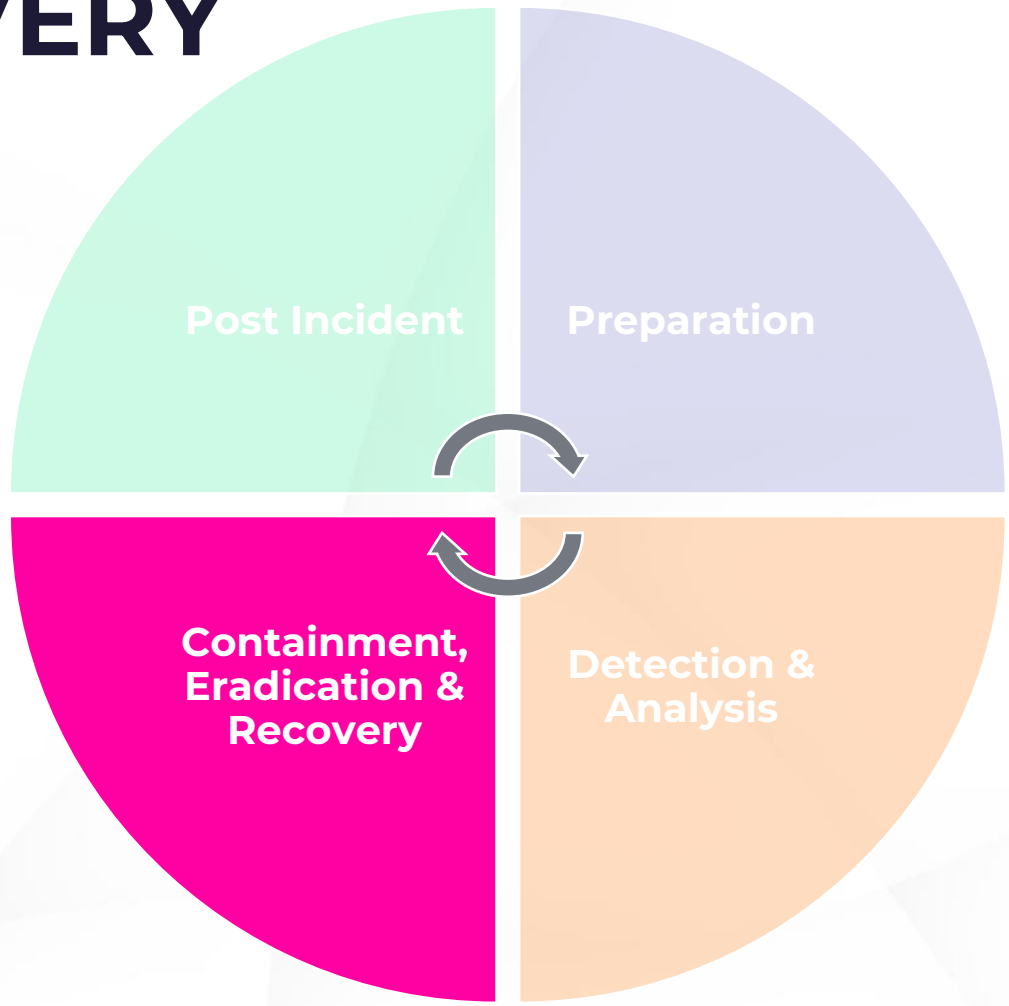


3. CONTAINMENT, RECOVERY

Responding to the incident

(balancing lots of priorities)

- Reduce the Spread / Containment
- Controlled Shutdowns
- Forensic Analysis
- Rebuild / Sanitise Systems
- Return to Service



4. POST INCIDENT

The incident is resolved

(but the more we can learn, the better)

- Lessons Learned
- Documentation
- Continuous Improvement
- Compliance & Reporting

SO… RECOVERY

How do we do it? What do we do?

- Most importantly – put **plans** into action.

  We don't want to be making it up as we go

1. Our First priority – we **contain** the incident.
2. Only slightly less important, we determine the **root cause** – because it determines our recovery options
3. We pick an appropriate recovery path:
   - **Fall Back** to an assured (but vulnerable) baseline, or
   - **Fall Forward** to something protected (but needing assurance)

FALLING BACK

This is familiar, but it's also failed us once…

- We make use of **existing**, **assured baselines**
- We **rebuild** systems, using a clean slate, to make sure they're at the expected baseline
- We use our **backups** (which of course have been tested and we know work…)
- We accept that there might be a **loss of information** between the incident and the last backup.
- We also need to find a way of **protecting** the system from a repeat of the incident

  (for which we need to understand the root cause)

FALLING FORWARD

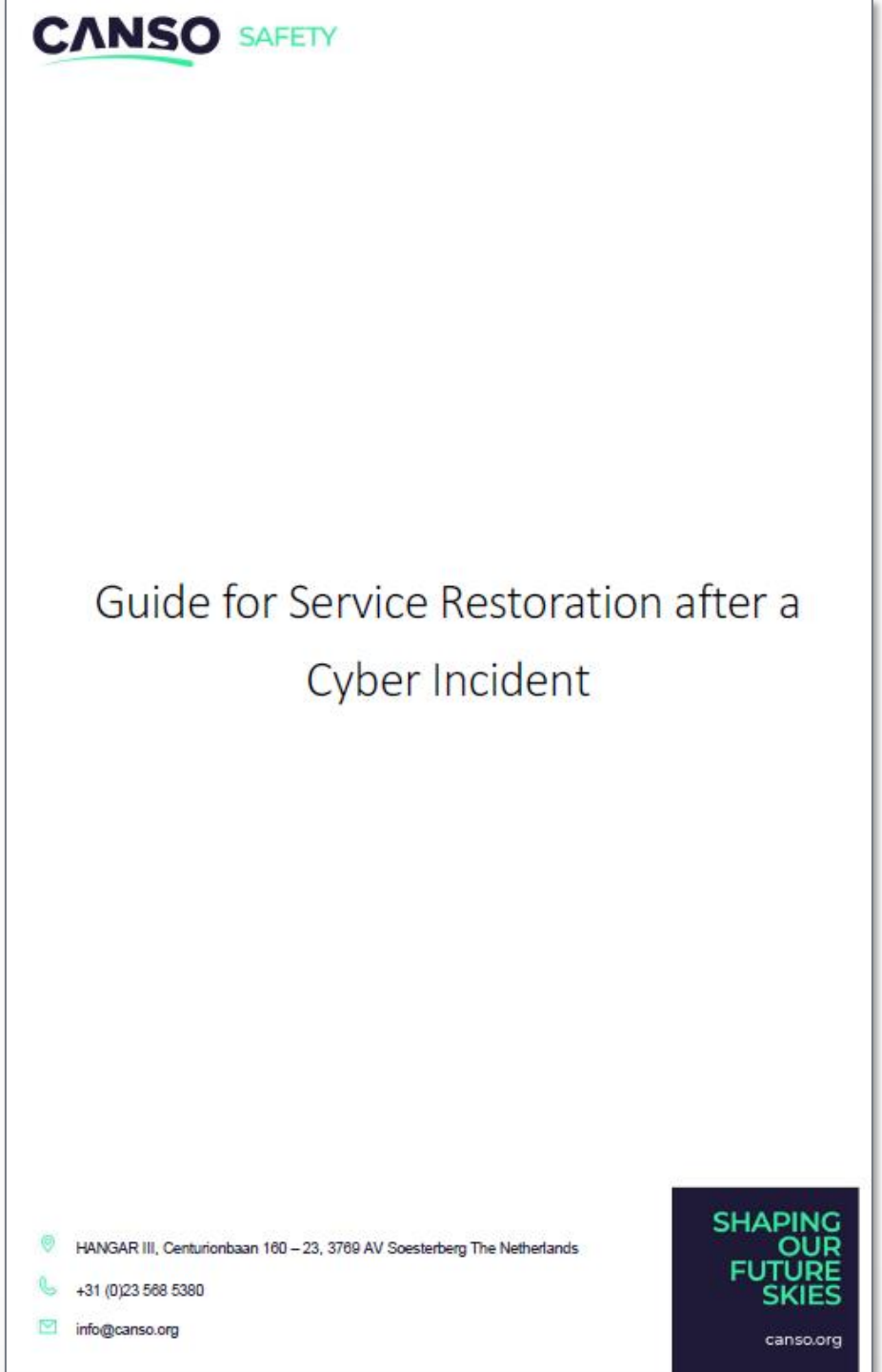
This lets us proactively close vulnerabilities, but raises assurance questions…

- We **clean** the current systems (which needs understanding about the attack)
- We perform **forensic analysis** – which helps us learn lessons later
- We **migrate** data where possible, and **restore** from backups where needed
- We **patch** systems where needed, and bring systems up to **current cyber standards** where we can
- We need to find a way of answering "**the assurance question**" about the cleansed system.

NO MATTER WHAT

We still have our key objectives

- Maintain safety
- Gather enough evidence to prevent reoccurrences
- Reintroduce in an orderly and methodical manner



FOR MORE INFORMATION

CSWG Guide to Service Restoration after a Cyber Incident

The document is currently going through review and will be released soon.

Also, the CSWG has a Slack area with reference documentation and guides – it's a resource that is available to all member ANSPs, we just need a cyber rep.

THANK YOU

ORGANISER CANSO HOSTED BY AIRWAYS