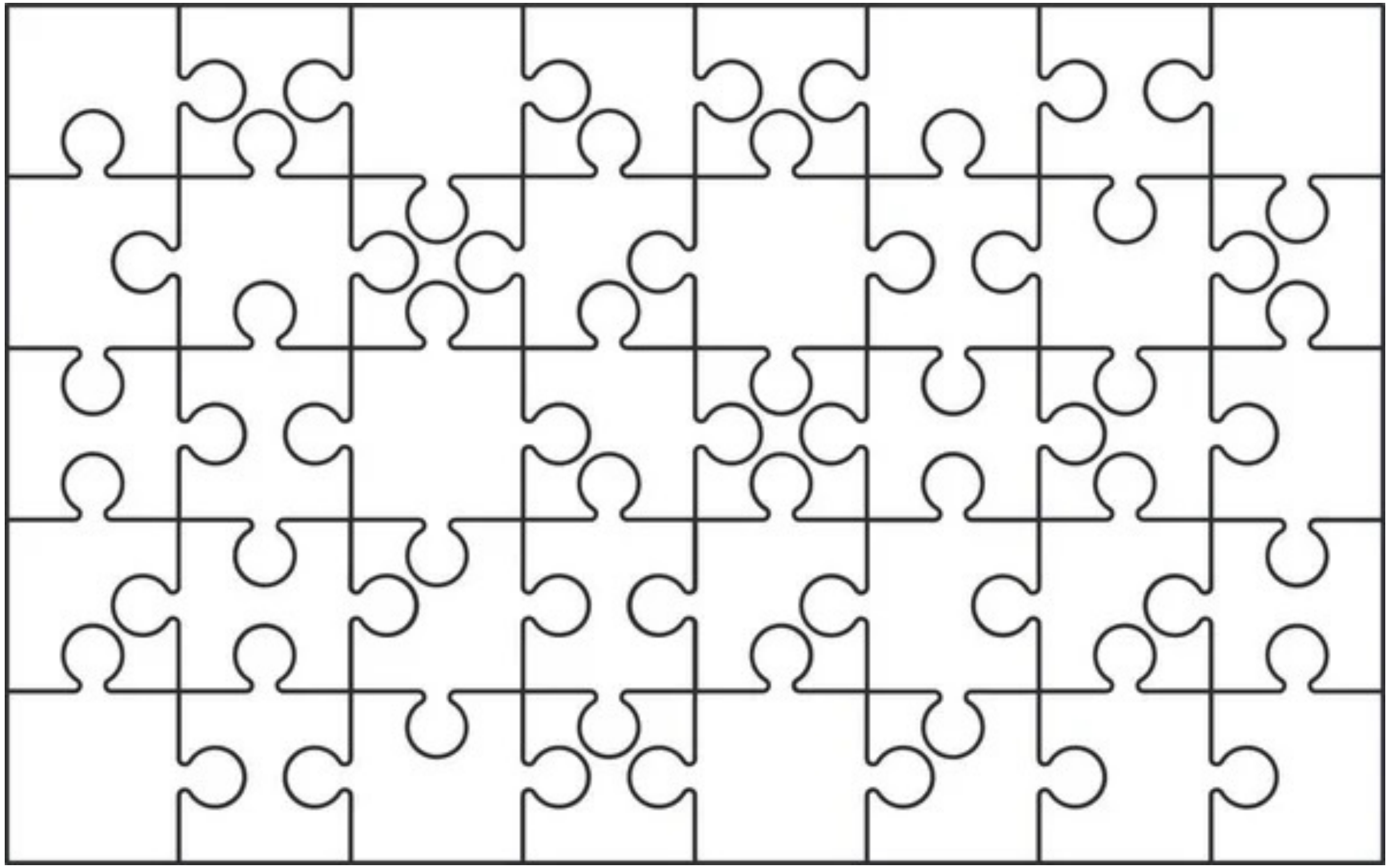
Detecting and responding to a cyber attack

Jason Symons
Mills Oakley

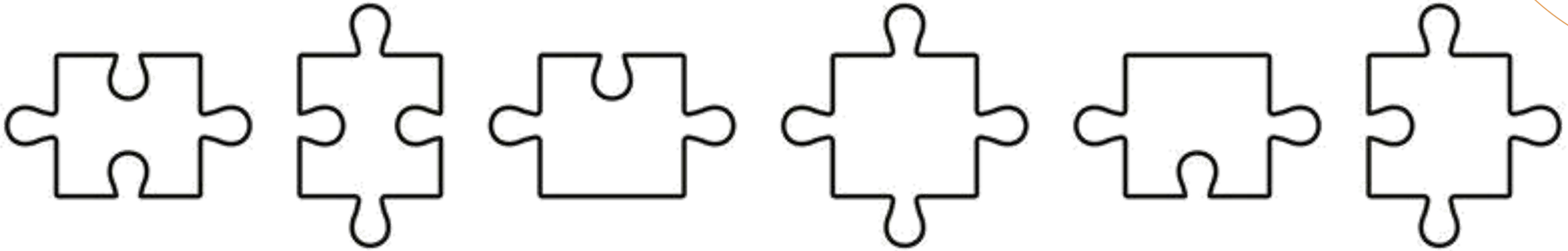
Fraser Jack
Principal
The Cyber Collective

faaa
CONGRESS
2023 ADELAIDE NOVEMBER 20–22

Cyber Security – Structured Approach



Cyber Security – Incident Response



Five Phases

Incident Plan

Who

Insurance

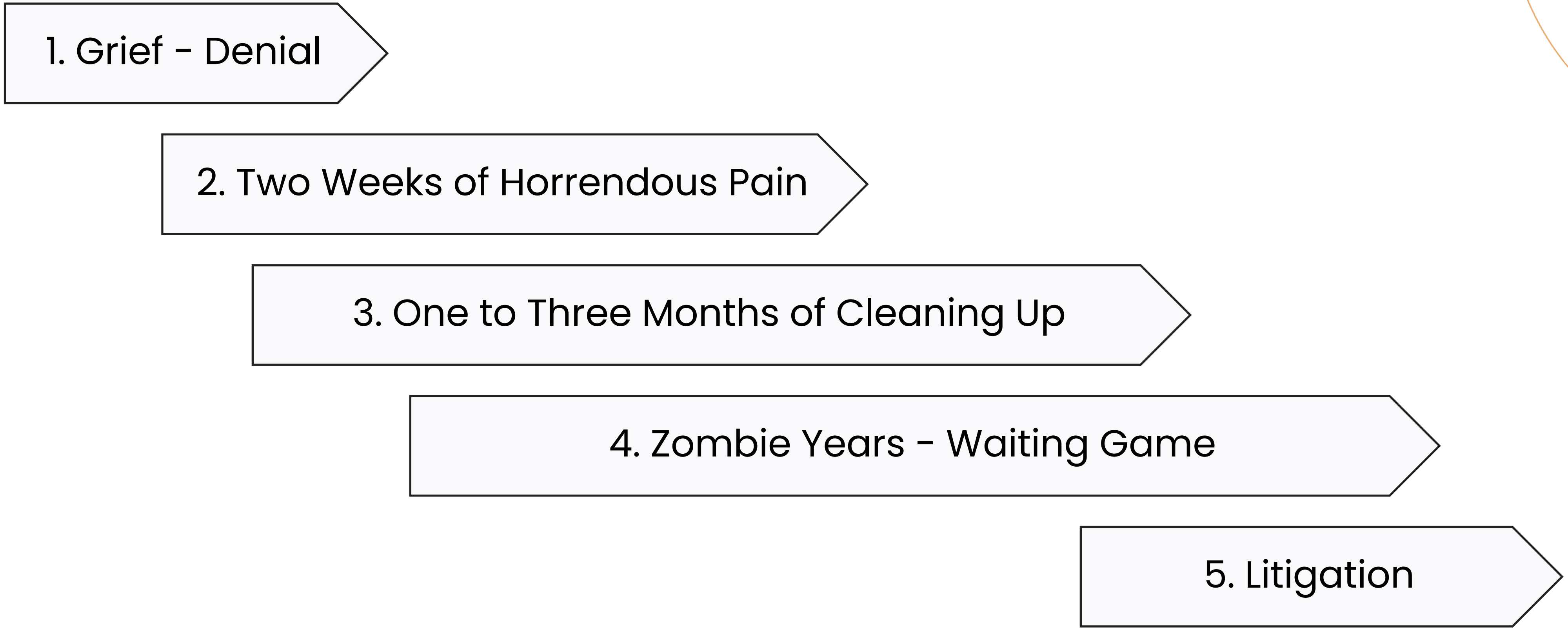
Communications

Cost

ASIC Cyber Pulse Findings - Nov 2023

- Reactive not Proactive
- Supply Chain Risk
- Disconnect between setting a policy and enforcing it
- Cyber Incident Response Plan –
  Up to date, trained teams and tested

Five Phases



1. Grief - Denial

2. Two Weeks of Horrendous Pain

3. One to Three Months of Cleaning Up

4. Zombie Years - Waiting Game

5. Litigation

Stage 1 – Detection, Grief & Denial

- It’s ‘when’, not ‘if’ – common types of incidents
- Detection - what is happening?
- Denial – it can’t be that bad…
- Grief – not us!
- What is the very first thing we do?

Stage 2 - Two Weeks of Horrendous Pain

- Cyber Incident Response Plan activated (if you have one)
- Forensic investigation
- Legal advice
- Communication with clients, staff, police, regulators, government agencies, other stakeholders, media
- Ransom negotiation
- Insurance support (if you have any)

Think About the Whole Supply Chain

- Clients
- Third-party vendors/suppliers (IT, etc)
- Software applications (CRM, etc)
- Adviser portals
- Contract obligations and assumptions

Stage 3 – One to Three Months of Cleaning Up

- System recovery
- Back to business as usual (BAU)
- Reviewing data breached
- Communication, notification and formal reporting
- Brand/reputation repair
- Insurance cover

Stage 4 - Zombie Years - Waiting Game

- Nervous times ahead…
- Harm caused to customers or other individuals
- Breach of privacy, contract claims, negligence
- Regulatory investigation (OAIC, ASIC)
- Notifying your insurer (professional indemnity, cyber)

Stage 5 – Litigation

- Legal professional privilege
- Forensic investigation, other evidence
- Privacy complaint, class action, enforcement action
- Working with lawyers and experts
- Damages, civil penalties and legal costs

CIRP – Cyber Incident Response Plan

- Immediate response steps
- Who is in your CIRT and SMT teams?
- Containment, investigation and remediation steps
- Root cause analysis
- Recording evidence and findings (legally privileged?)
- Communication pack

Cyber Insurance

- Do I really need it? I’ve got PI cover…
- What does cyber cover?
    - Incident response costs, social engineering fraud, business interruption
    - Ransom payments, third-party liability, regulatory fines
- Does it actually pay out?
- Can I get it? How much will it cost?

Jason's Tips: C.H.E.C.K.

Challenge your cybersecurity and test it out

Have an incident response plan and simulation exercises

Evaluate your cyber resilience against regulator expectations

Contact your insurance broker or cyber insurer

Know the team that will face the crisis together

Fraser’s Tips:

- Use a structured approach; no more ad hoc or Band-Aids
- Train your teams (every team member)
- 90% of incidents start with a team member
- Your teams need to be the first line of defence, not the weakest link
- Keep the evidence of everything you do

Ask us now or reach out later

Jason Symons - Mills Oakley
jsymons@millsoakley.com.au

Fraser Jack – The Cyber Collective
fraser.jack@thecybercollective.com.au

Q&A

faaa
CONGRESS
2023 ADELAIDE NOVEMBER 20–22

Rate this session

Meet the speaker zone

Thank you for attending this session

faaa

CONGRESS

2023 ADELAIDE NOVEMBER 20-22