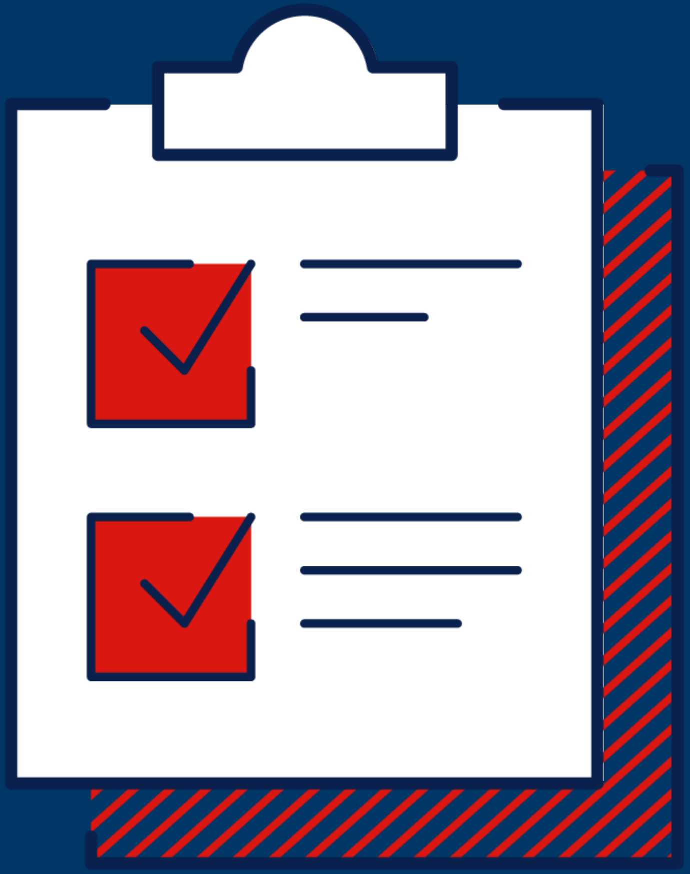
The Smith Family
Learn today, change tomorrow.

Reviewing your incident framework and response



Lisa Allan, Head of Fundraising

May 2023

The Incident

The Smith Family
Learn today, change tomorrow.

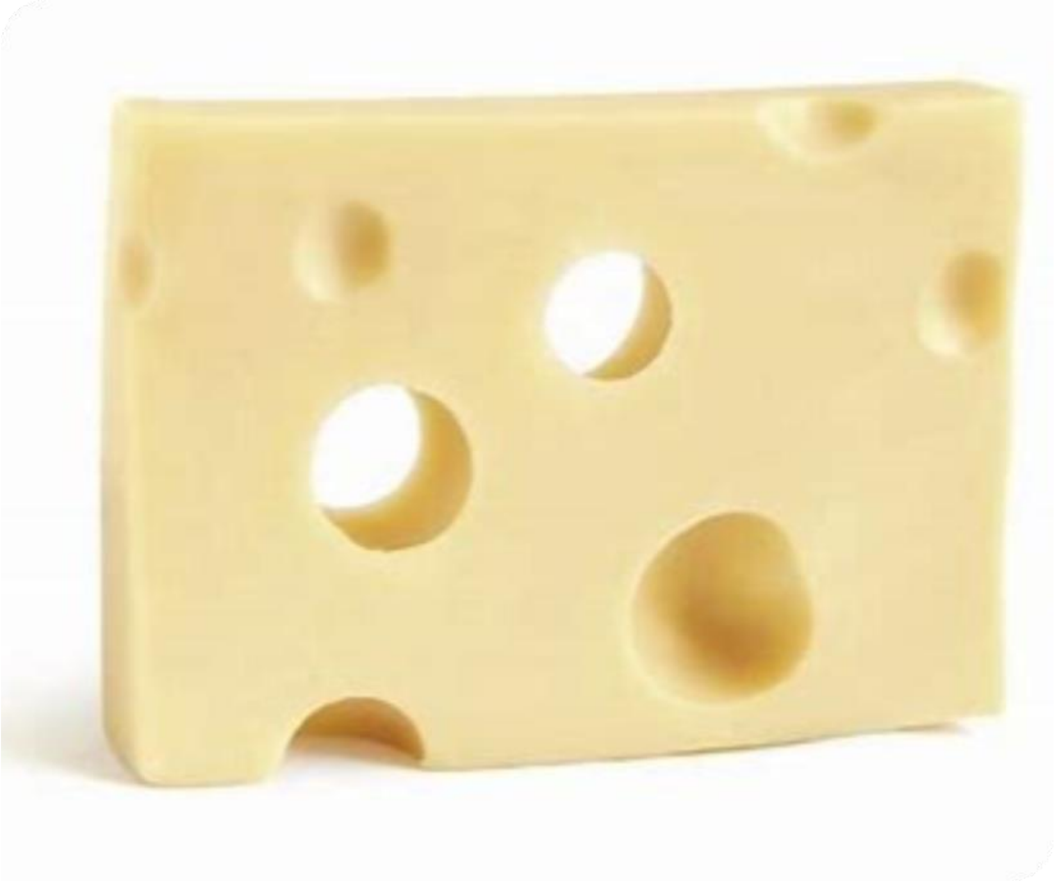
Incident = An unsuccessful attempt to steal funds

- Although thwarted, identified some supporter information MAY have been accessed
- No sensitive information
- There was NO evidence of misuse
- Took the decision to communicate quickly, openly, transparently and honestly to preserve trust

Threat of cyber attacks

- **The problems are never singular**
  - People, process and technology

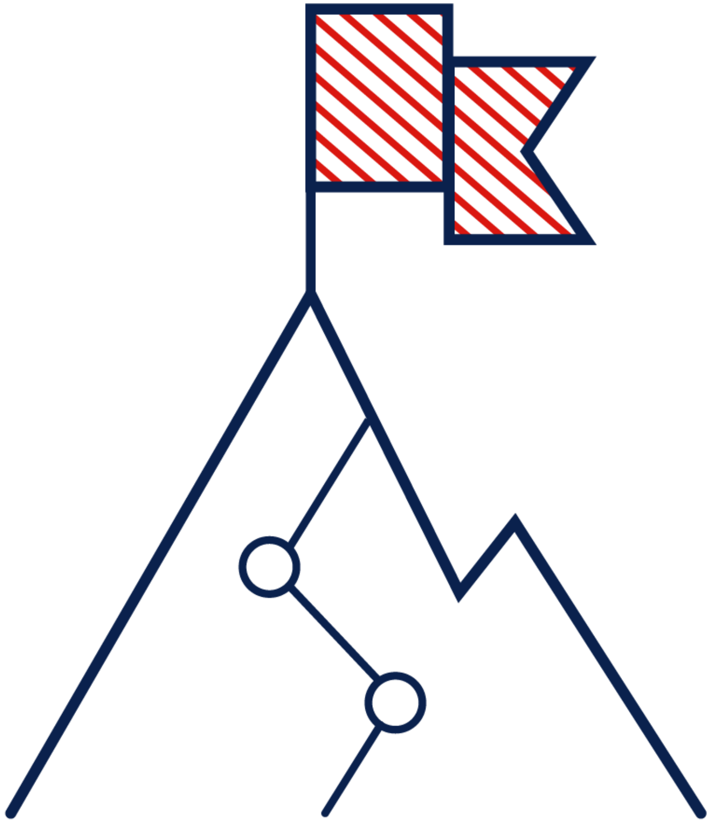
- **Keep focused on the basics**
  - ➢ People – customers and team
  - ➢ Fortification of systems
  - ➢ Data security



6 Suggested Steps

The Smith Family
Learn today, change tomorrow.

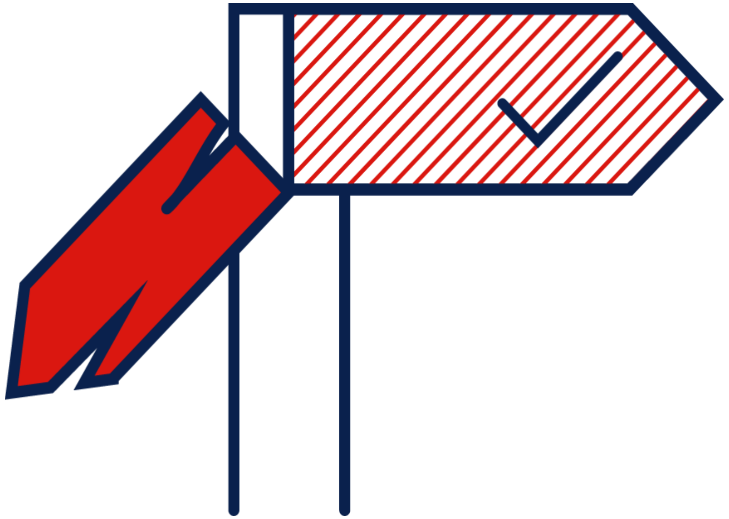
1. Form Critical Incident Team
2. Perform forensic investigation
3. Secure systems
4. Develop communications plan
5. Execute
6. Reflect



Critical Incident Management Procedure

The Smith Family
Learn today, change tomorrow.

- A policy document
- Specially formed group with specific responsibilities
  1. Identify and assess all risks to an organisation
  2. Identify vital communication audiences
  3. Determine proactive vs reactive stand
  4. Information flow determined
  5. Identify allies to support the incident
  6. Post incident retrospective



Forensic Investigation

Internal teams or third party expert/s to determine the root cause across:

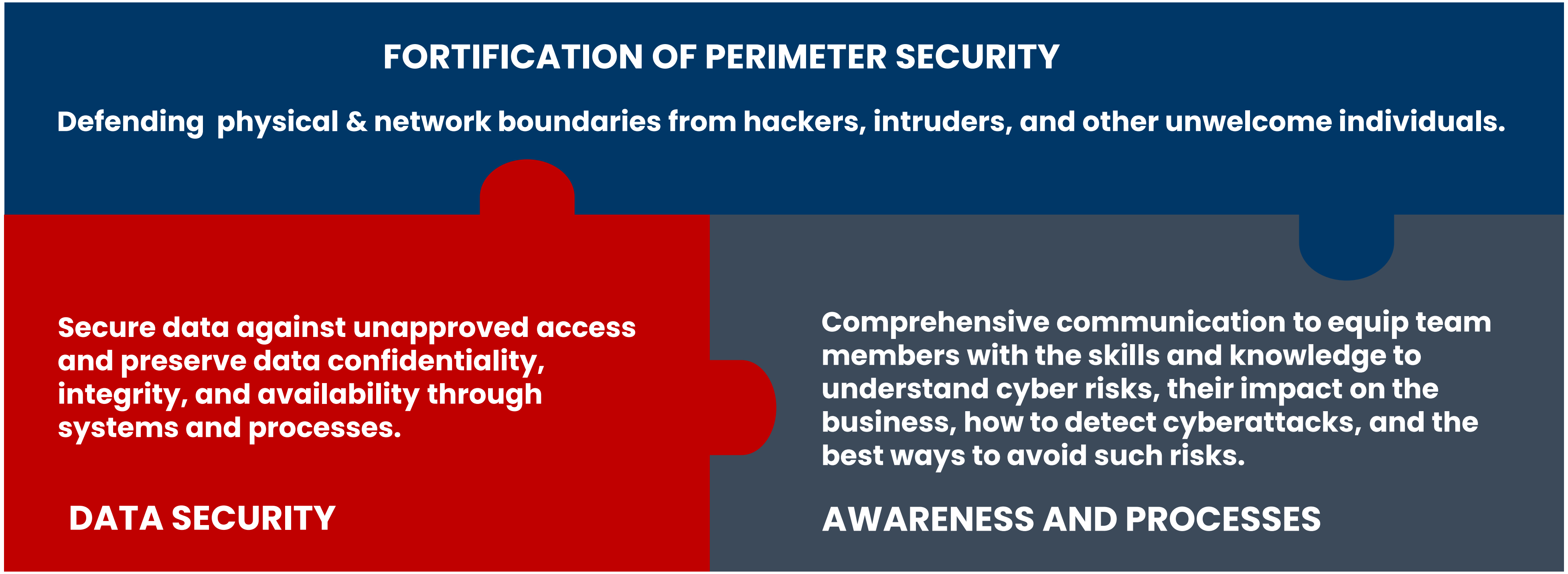
- ➢ People
- ➢ Process
- ➢ Technology

And to articulate :

- ➢ Gaps
- ➢ Mitigations
- ➢ Action

Secure Systems

The Smith Family
Learn today, change tomorrow.



FORTIFICATION OF PERIMETER SECURITY

Defending physical & network boundaries from hackers, intruders, and other unwelcome individuals.

Secure data against unapproved access and preserve data confidentiality, integrity, and availability through systems and processes.

DATA SECURITY

Comprehensive communication to equip team members with the skills and knowledge to understand cyber risks, their impact on the business, how to detect cyberattacks, and the best ways to avoid such risks.

AWARENESS AND PROCESSES

- Guided by **The Essential Eight**, recommended by ACSC: The minimum mitigations to action which makes it harder for adversaries to compromise systems

Secure Systems > Data Security

Data security requires significant effort with a focus on de-risking any data security exposure. Could be divided into three streams of work:

1 De-Risk Data Security Exposure

Identify and implement opportunities to reduce risk associated with data

2 Identify Critical Business Processes

Identify and document critical business processes

3 Categorise / label data in core systems for automated controls

Automation of privacy and policies into systems and processes

Communications Plan

The Smith Family
Learn today, change tomorrow.

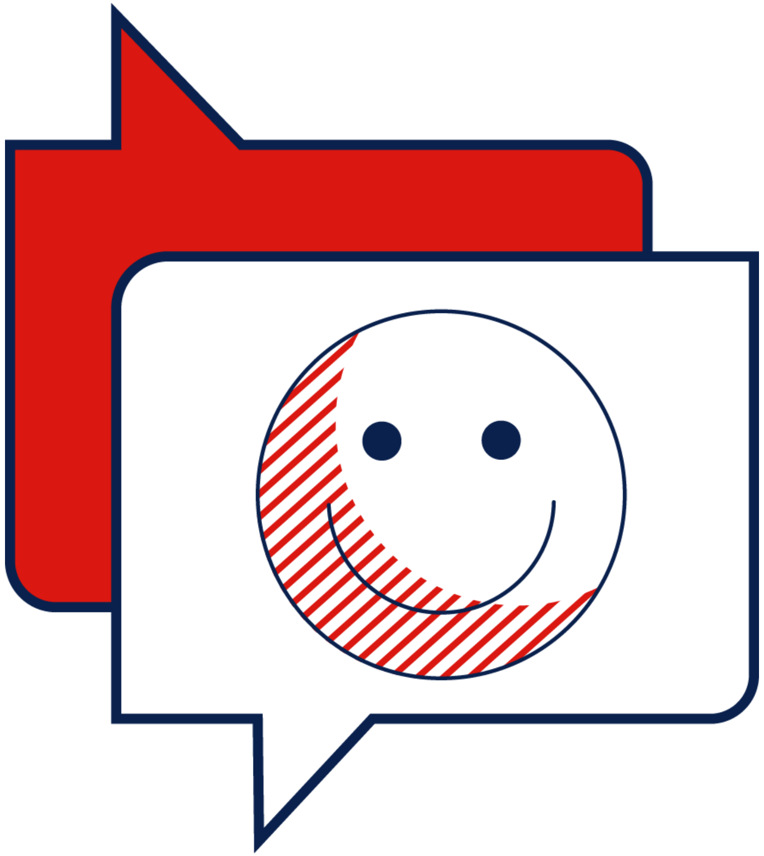
Should include:

- Stakeholder engagement consultation processes
- Voice and channel plans; who does what, how visible the CEO should be
- Communications messaging by audience
- Media strategy & approach; process for managing enquiries
- Social media strategy and approach; social monitoring and triage, escalation
- Any relevant promotional flighting

Consider support from a crisis communications expert.

Execution considerations

- Clear project lead
- One source of truth
- Capture everything in writing



Reflect

- What did we do well?
- Where were the opportunities?

Post Implementation Review to cover:

- Objectives
- Team / Skills / Resources
- Capabilities / Capacities
- Stakeholders
- Process / Stages
- Communications & Change Management
- Costs
- Lessons

Things to watch out for:

- Role accountabilities for work inside and outside of the incident (watch for duplication and missed effort)
- The people side of change

The Smith Family
Learn today, change tomorrow.

Thank you

Have further questions?
Please get in touch:
Lisa Allan
Lisa.Allan@thesmithfamily.com.au