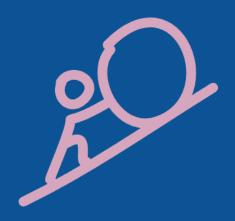# Creating big impacts with small cybersecurity teams

Pia Lange

About me

Security and Regtech Manager @ Sharesies
- *Formerly Information Security Manager*
- *Before that Security Analyst*

Professional Interests:
- Leadership and Culture
- Information Governance
- Blue team ops
- Breaking things

Personal Interests:
- Tramping
- Climbing
- Improv Theater
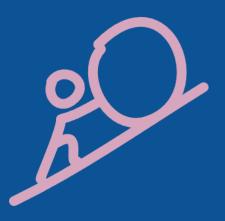
Introduction

What's in the box?
- Challenges that face small security teams
- Ideas for overcoming those challenges
- How those ideas pay off
- Pitfalls and lessons learned from experience
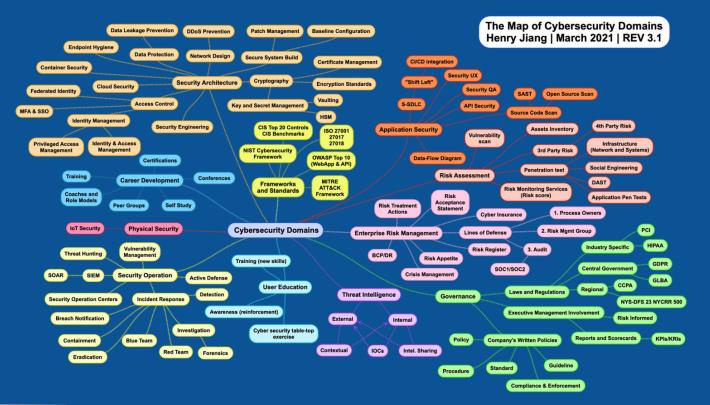- Realistic view of what your small team can do

What's not?
- Silver bullets
- One size fits all solutions

Challenges

- **Resource Constraints**
  - *Vulnerability to disruption*
- **Lack of traction**
  - Effecting cultural and organisational change as a single voice
- **Overwhelming amount of context**
  - *Complex technical and business environments*
- **Highly agile environments**
  - *Maintaining risk posture in the face of constant change*

We cover a lot of ground!

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1

Idea #1 : Compounding returns

Focus: Long term momentum over immediate outcomes

Pitfalls:

- If only…

- Framework Fundamentalism

- Confirmation Bias

- Silver Bullets

Instead:

- Have a vision, not a plan

- Pay yourself first

- Monitor your investment

- Watch for opportunities

What are the things we can do every day to move towards our vision?

Idea #2 : Be a safe pair of hands

Focus: Amplify your voice through other leaders in the business

Pitfalls:
- Over-leveraging risk
- Rubber Stamps
- Narrow focus
- Agenda Oriented

Instead:
- Focus on genuine business needs
- Collaborate
- Embrace generalism
- Mana Oriented

Idea #2 : Be a safe pair of hands

Focus: Amplify your voice through other leaders in the business

Things you can do:
- Formalise your security risk appetite
    - Get specific!
- Set-up a steering group
- Be part of the collective voice
- Seek out opportunities for <u>active</u> collaboration
    - Hackathons
    - Soundboarding
- Prioritise mana manaaki and regular connection

Idea #3 : Embrace the ~~cringe~~ cool

Focus: Engage the wider team on your mission

Pitfalls:
- Over translate
- Reductionist Security
- Assuming expertise
- Mission fixated

Instead:
- Tell the story
- Invest in the curious
- Be curious
- Keep an eye on the news

Idea #3 : Embrace the ~~cringe~~ cool

Focus:

Things you can do:
- Guilds and enthusiast groups
- Embrace the curious
    - Mentoring
    - Private Channels
    - Teachable moments
- Tabletop and Simulation Exercises
- Wear the black hoodie!

Idea #4 : Focus on the delta

Focus: Manage security risk at scale in the face of constant change

Pitfalls:
- Trying to cover all the ground
- Over abstraction
- Under abstraction
- Catastrophizing

Instead:
- Embrace the agility
- Isolate what matters
- Identify Key Factors
- Outsource the minutiae

Idea #4 : Focus on the delta

Focus: Manage security risk at scale in the face of constant change

Things you can do:
- Establish a baseline
    - Break down your environment into logic chunks e.g service/functions
    - Identify the key factors that contribute to risk
    - Document these for each chunk
    - Abstract away common patterns
- Create a trigger point to capture information relating to your key factors
- Update your context, feedback any requirements
- Close the loop

Outcomes

- ~~**Resource Constraints**~~
    - *Your organisation is your team*
    - *Compounding effect enables bigger changes over time*
- ~~**Lack of traction**~~
    - Effecting cultural and organisational change as a ~~single~~ collective voice
- ~~**Overwhelming amount of context**~~
    - *Focus only on to the immediate context*
- ~~**Highly agile environments**~~
    - *Risk management as part of operational workflow*