

Fighting the cyber people war

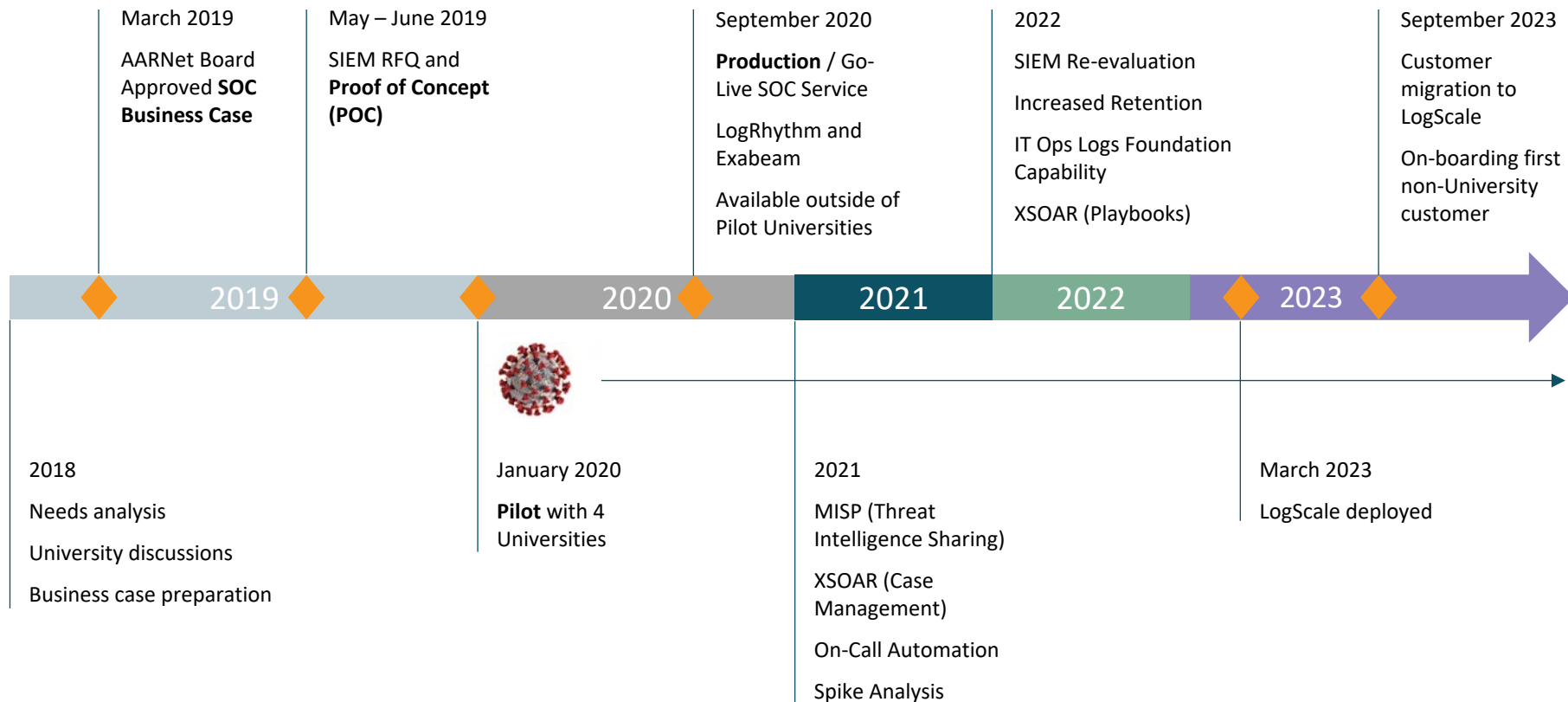
A focus on the challenges for talent facing NRENs

TechEx 2023
Warrick Mitchell

AARNet and cyber security

Some background

Our journey – creating a sector focused SOC



A SOC for Higher Education



AARNet's unique
position



Mitigates risk
in real-time



SOC + DDoS
+ ISP



Sector focused



Transparent security



Common team

Sector Focused



AUSCERT

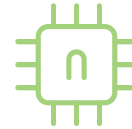


ACSC Australian Cyber Security Centre

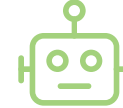


Jisc

NextGen Stack



+



+



1000+ Modelled Behaviours

End-to-End Automation

100% Transparency



Predictable Cost



Unlimited Logs



2 Year Storage



Fixed Pricing

Enterprise Grade



>30 Billion Events Per Day
(80TB of logs/day)



Full Disaster Recovery



24x7 Coverage

A changing threat landscape

Optus hack to cost at least \$140 million

The Sydney Morning Herald

Medibank faces \$1 billion bill as hackers release 1500 more sensitive records

The Sydney Morning Herald

Royal ransomware claims attack on Queensland University of Technology

BLEEPINGCOMPUTER

University of Western Australia Student Details Exposed in Data Breach

GIZMODO AU

Increased awareness and fatigue



More reporting



More questions



Increased budgets



Security training
and awareness



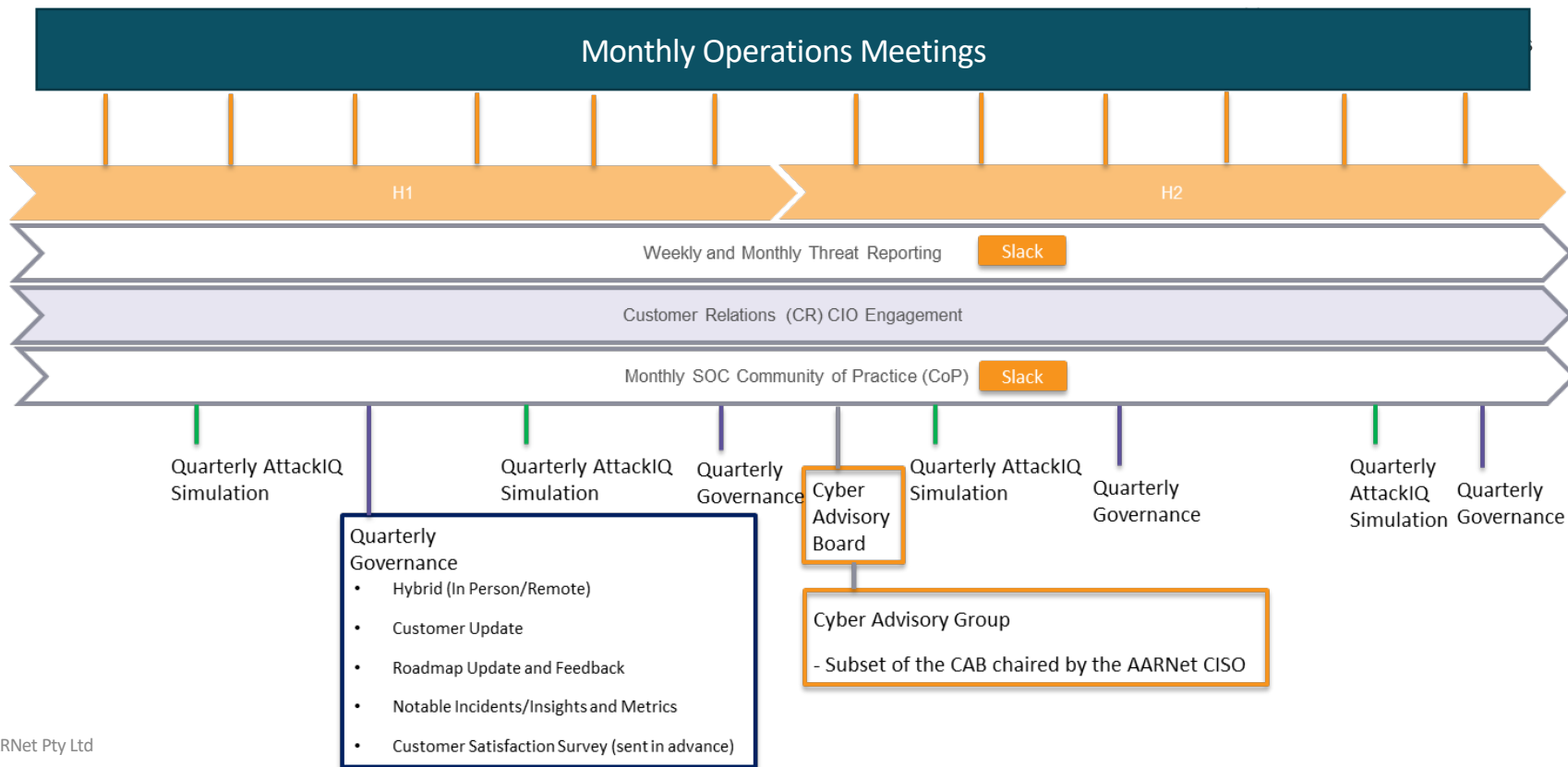
More security
controls



Higher demand

Example: high customer engagement

Weekly, monthly, quarterly, annual touch-points to maintain



The challenging environment

How to attract and retain good people

Global Tech Attrition – circa 23% and rising

23%+

High Tech
outpacing other
verticals

LinkedIn & Forbes 2023

**Intention to
Stay**

Global: 29%
Europe: 39%
Latin America: 27%
ANZ: 24%
Asia: 19.6%

Gartner 2023

Age

- 18-29yrs 20%
chance to stay
- 40-70 yrs 48%
chance to stay

Gartner 2023

Shortage

US: 25%
Europe: 43%
India: 39%

Forbes 2023

Value Prop

65% may change
mind and stay if
Flexible Work &
ESG focus is high

Gartner 2023

War

Circa 70-100K
high tech ees
disrupted

Forbes 2023

Tenure

High Tech
median now
1-2 yrs

LinkedIn 2023

Downturn

Not a cure
Bank talent now
Super charged
exit

Gartner 2023

Post Covid Attrition @ AARNet

2022

- AARNet attrition 16% (30 ees)
- Tech Industry average 17.2% (down from 21.7% in 2021)
- Cost to AARNet: Circa \$2.5M

Why?

- 40% left for higher \$ & promotion
- 26% involuntary
- 7% returning to previous industry
- 13% moving IS/OS – Family
- 13% dissatisfied with AARNet

Where From?

Operations	12
Customer Relations	7
Cyber Security	5
Applications and Architecture	3
IDG	3

2023 YTD

- AARNet attrition 5% (9 ees)
- Tech Industry average 18-22% (predicted)
- Cost to AARNet: Circa \$700K

Why?

- 44% left for higher \$ & promotion (2022 46%)
- 22% involuntary (2022 26%)
- 11% returning to previous industry (2022 7%)
- 11% moving IS/OS – Family (2022 13%)
- 11% dissatisfied with AARNet (2022 13%)

Where From?

IDG	3
Cyber Security	2
Operations	2
Customer Relations	1
Legal	1

It's a Jungle Out There

Poachers



Increasing \$ + Tight Market + Poacher Behaviour

VS

Gamekeepers



Lift the bar everyday or you'll get left behind

Analyse and Strategise now: You CAN be ahead of this

It's a Jungle Out There

Poachers

- Big \$\$ (+ 20-40%) & big landscapes
- Selling the instant fix to 20-35 year olds
- Pumping up egos & dreams
- Weighting potential heavily against ability
- Junior Staff going to senior roles that they are not ready for
- Capitalising on Covid fatigue
- Catastrophising the challenges of current hybrid model
- Not just the big players: start up's, boutique firms, security, security, security

Increasing \$ + Tight Market + Poacher Behaviour

=

The Perfect Career Storm is Brewing

VS

Gamekeepers

- Excellence in all aspects of Employee Lifecycle
- Engagement is critical
 - Policy Platform
 - Hybrid work
 - Culture
 - ESG focus
 - Diversity & Inclusion
- Societal currency – your 'WHY + HOW'
- Authenticity at every level and in every interaction
- These are not 'differentiators' – they are your 'Ticket to Play'

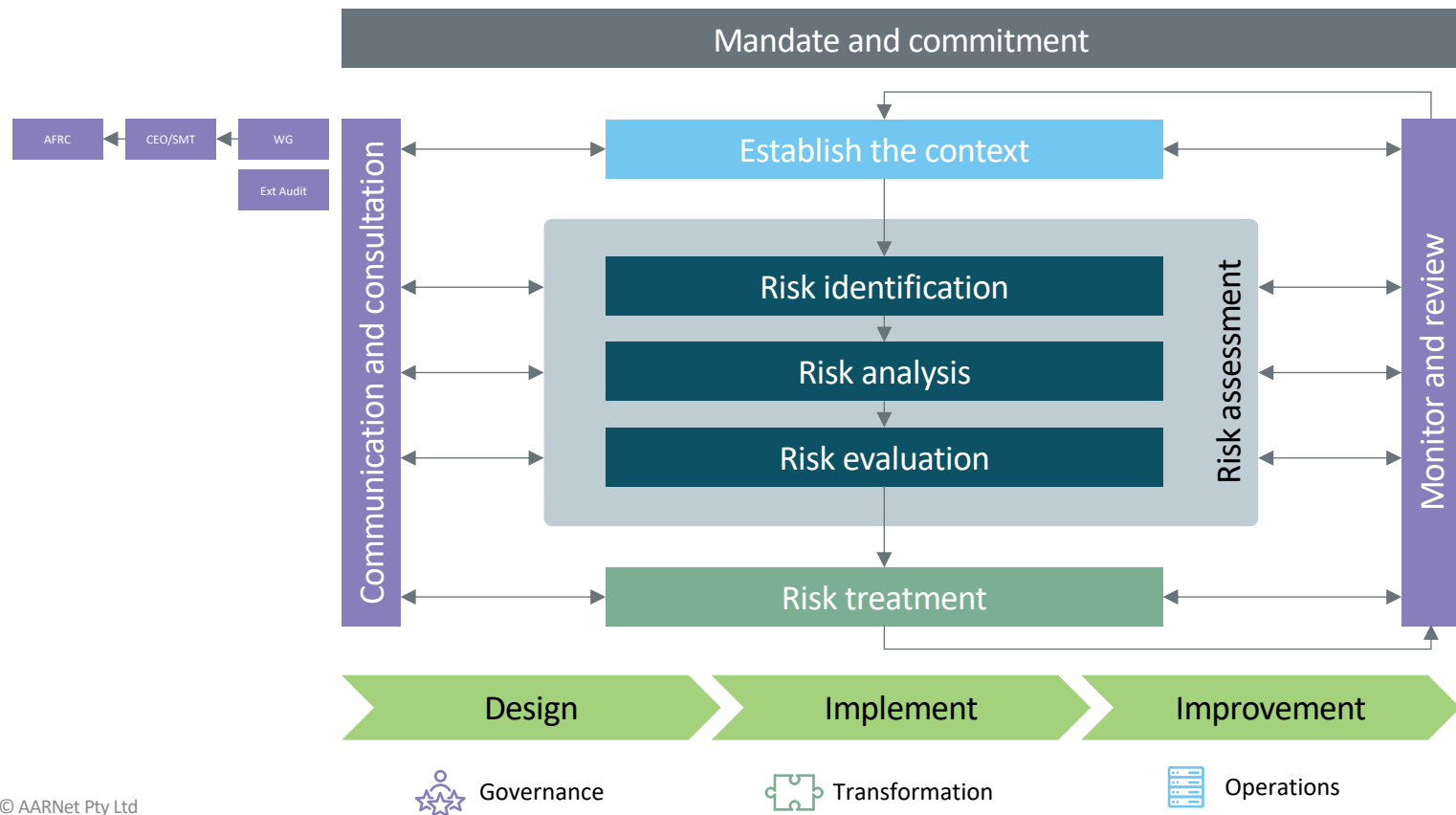
Lift the bar everyday or you'll get left behind

Analyse and Strategise now: You CAN be ahead of this

A way forward

Strategies from the AARNet cyber team

Strategy one – lead with risk and ‘top down support’



Strategy two – shifting left



Policies and standards



Security testing and checks



Guidance, advice and support

Strategy three – identify champions

apl-support – Sep 20th, 2021

Mon 23/01/2023 9:13 AM

FW: Phishing 2023 reminder to be alert

To

Cc

 This message was sent with High importance.

Good morning VIC Team,

Speaking to a couple of the team this morning I thought I'd share this Phishing awareness emails to the VIC Team.

A quick call out to @Tim who received the phishing email over the weekend allegedly from . When Tim noticed this didn't feel right he called myself to check and see how to report this to our security team. Great works Tim. One team.

Not sure how many of us in the IDG Team have received the phishing email/s over the weekend or since we have returned from a much-needed break. This is a good reminder that the bad guys and girls who are sending these emails are always working and will try and test us on weekends, holidays and anytime in-between.

Please also see below for how to report via email to apl@aar.net.au and via the report message button. Fingers crossed no one has taken the bait /clicked the links. If you have clicked the link/s please follow up with the support teams and see below instructions. Please also know were all human and everyone can be phished.

Americans. So in light of this, as a service to the public we asked people...

Strategy four – reporting, metrics & communication



Informal



Meeting Legal & Regulatory Obligations

Managing Security Risks

Protecting Information Assets

Ensure Appropriate Access to
Information and Resources

Managing Third Party Risks

Providing Assurance to Stakeholder

Cyber Engagements

Managing Security Incidents

Dashboard Reporting (NIST)



Formal

Strategy five – security, usability and automation



Example 1 – Passwords/passphrases

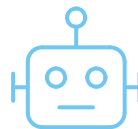
Scenario: Human fatigue when users need to remember numerous or complex passwords

Behaviours:

- Store them insecurely (e.g. post-it note)
- Password re-use
- Increased service management and frustration (e.g. locked accounts, forgotten passwords)

Response:

- Increase password length/complexity but increase the expiry period
- Target security controls for privileged accounts or protected network segments (as opposed to 'ALL')



Example 2 – automate to remove the human and manual effort

Scenario: We have to swivel chair across systems to collate data points to support security incident investigations

Behaviours:

Increased time to investigate

Response:

Utilise technology to bring the data points into a single pane of glass (SPOG) so a determination can be made and remedial action undertaken

A way forward

AARNet HR strategies

Your Action Plan



Acquire

- Review & uplift recruitment process
- Interview tools
- Set tasks
- Create Alternate pathways: Secondary School Work Experience; Graduate Programme; Cyber Academy
- Diverse education and skills acquisition



Delight

- Great offer
- Highlight benefits
- Seamless HR onboarding
- Buddy system
- Team engagement – they should never feel ‘alone’
- Immediate meaningful work
- Thank You for choosing US!



Engage

- Meaningful policies
- Open & collaborative culture
- Trust: Give licence to fail – tap their best creativity
- Diversity & Inclusion strategies
- L&D: Interest in the individual
- We Value You!



Retain

- Continual improvement of policies & Culture
- Communication at many levels
- Weekly 1:1 management touch point
- Focus on individual – not just tangible work
- Unexpected support
- Recognition



Thank You