Fighting the cyber people war
A focus on the challenges for talent facing NRENs

TNC23, Albania
Chris Hancock - CEO
David Wilde – CTO
AARNet and cyber security

Some background
Our journey – creating a sector focused SOC

- March 2019: AARNet Board Approved SOC Business Case
- May – June 2019: SIEM RFQ and Proof of Concept (POC)
- September 2020: Production / Go-Live SOC Service
  - LogRhythm and Exabeam
  - Available outside of Pilot Universities
- May – June 2019: SIEM RFQ and Proof of Concept (POC)
- January 2020: Pilot with 4 Universities
- September 2020: Production / Go-Live SOC Service
  - LogRhythm and Exabeam
  - Available outside of Pilot Universities
- 2022*: SIEM Re-evaluation
  - Increased Retention
  - IT Ops Logs Foundation Capability
  - XSOAR (Playbooks)

2018
- Needs analysis
- University discussions
- Business case preparation

Jan 2020
- Pilot with 4 Universities

2021
- MISP (Threat Intelligence Sharing)
- XSOAR (Case Management)
- On-Call Automation
- Spike Analysis

2022*
- Subject to change
A SOC for Higher Education

AARNet’s Unique Position

Mitigates Risk in Real-Time

SOC + DDoS + ISP

Sector Focused

Transparent Security

Common Team
A changing threat landscape

Optus hack to cost at least $140 million

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

Royal ransomware claims attack on Queensland University of Technology

University of Western Australia Student Details Exposed in Data Breach
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

Monthly Operations Meetings

Weekly and Monthly Threat Reporting
Customer Relations (CR) CIO Engagement
Monthly SOC Community of Practice (CoP)

Quarterly AttackIQ Simulation
Quarterly AttackIQ Simulation
Quarterly Governance
Quarterly AttackIQ Simulation
Quarterly Governance
Quarterly AttackIQ Simulation
Quarterly Governance
Quarterly AttackIQ Simulation
Quarterly Governance

Quarterly Governance
- Hybrid (In Person/Remote)
- Customer Update
- Roadmap Update and Feedback
- Notable Incidents/Insights and Metrics
- Customer Satisfaction Survey (sent in advance)

Cyber Advisory Board
- Subset of the CAB chaired by the AARNet CISO
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

Value Prop
65% may change mind and stay if Flexible Work & ESG focus is high
Gartner 2023

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

Shortage
US: 25%
Europe: 43%
India: 39%
Forbes 2023

© AARNet Pty Ltd
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?

<table>
<thead>
<tr>
<th>Operations</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Relations</td>
<td>7</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>5</td>
</tr>
<tr>
<td>Applications and Architecture</td>
<td>3</td>
</tr>
<tr>
<td>IDG</td>
<td>3</td>
</tr>
</tbody>
</table>

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?

<table>
<thead>
<tr>
<th>IDG</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security</td>
<td>2</td>
</tr>
<tr>
<td>Operations</td>
<td>2</td>
</tr>
<tr>
<td>Customer Relations</td>
<td>1</td>
</tr>
<tr>
<td>Legal</td>
<td>1</td>
</tr>
</tbody>
</table>
It’s a Jungle Out There

Poachers

Vs

Gamekeepers

Increasing $ + Tight Market + Poacher Behaviour

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

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’

Mandate and commitment

Establish the context

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Risk assessment

Monitor and review

Communication and consultation

Design

Implement

Improvement

AFRC

CEO/SMT

WG

Ext Audit

Governance

Transformation

Operations

Subject to change
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 ; @aarnet.edu.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

- 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)

Informal ▶ Formal

© AARNet Pty Ltd | AARNet Public

Subject to change
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

© AARNet Pty Ltd | AARNet Public

Subject to change
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