# The Cyber Security Skills Gap

## Real Problem or Self-inflicted Pain?

# The Cyber Security Skills Gap: Real Problem or Self-inflicted Pain?

*A multi-dimensional problem, far more complex than its media coverage is suggesting*

Why is the Cyber Security industry struggling to **ATTRACT** talent?

Why is the Cyber Security industry struggling to **RETAIN** talent?

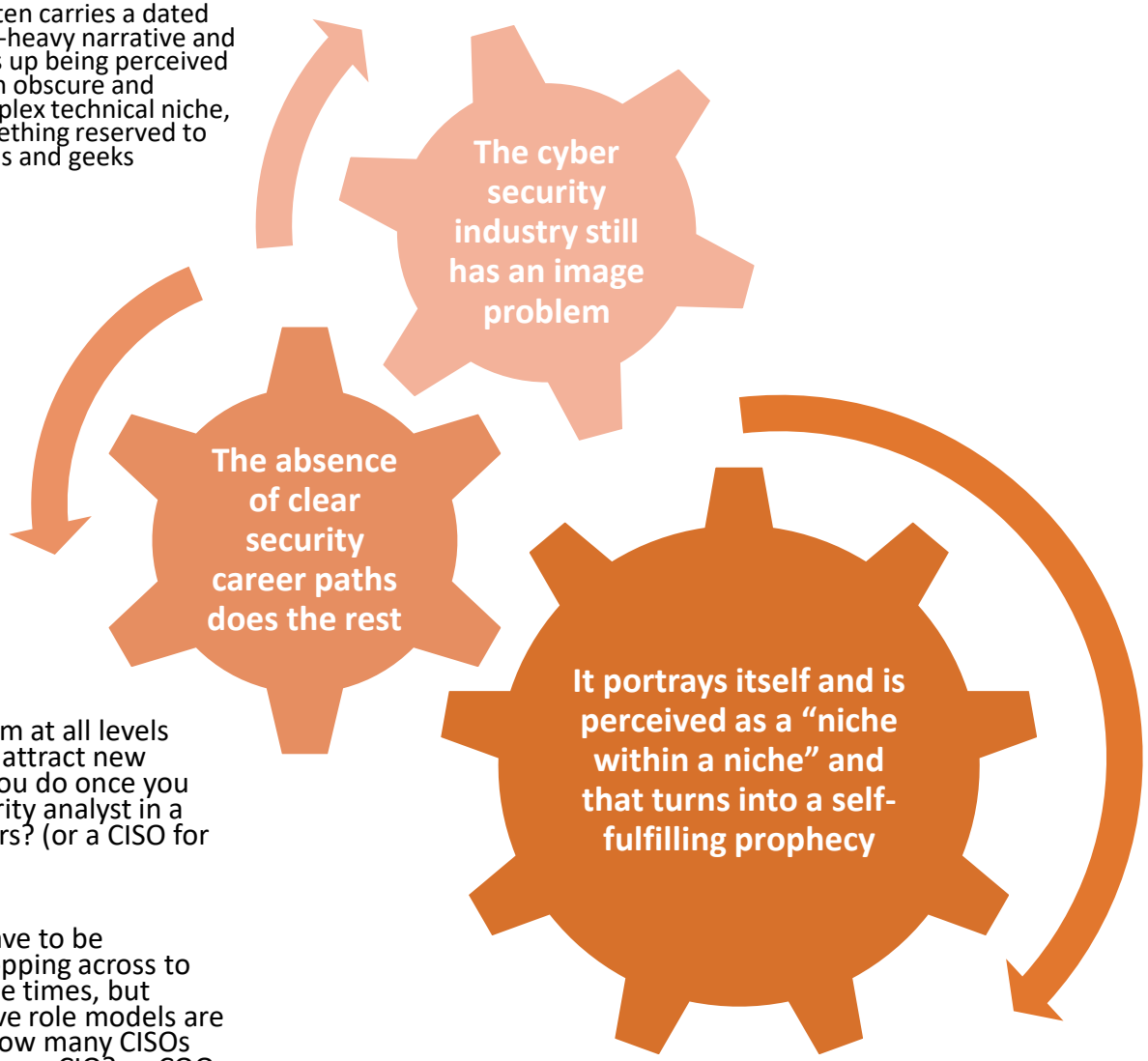
What can we do to **CHANGE** that and create different dynamics?

Only facing up to fundamental internal roadblocks affecting the cyber security industry – and removing them – will bring change

# Why is the Cyber Security industry struggling to attract talent?

*This is much more complex than not wanting to be "the guy who says no" or the "scapegoat" when something goes wrong*

It often carries a dated tech-heavy narrative and ends up being perceived as an obscure and complex technical niche, something reserved to nerds and geeks



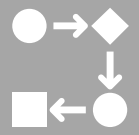

This is real problem at all levels when it comes to attract new talent: What do you do once you have been a security analyst in a SOC for a few years? (or a CISO for that matter?) …

You should not have to be condemned to hopping across to similar roles all the times, but credible alternative role models are cruelly missing: How many CISOs have actually become CIO? or COO, or CRO?

The lack of awareness around the diversity of security roles breeds a lack of relevant training courses and educational opportunities.

**The cyber security industry has never managed to make itself attractive**

# Cyber Security is not just about Tech



*Why is the message not coming through?*

- **There are countless cyber security roles which are not purely technical and require business, personal or political acumen**
  - From auditing to awareness development or training
- **There are genuinely complex, transversal, transformational projects around cyber security, in particular in large organisations**
  - Which should provide prime training ground for ambitious project/programme managers
- **There are genuine management and transformation challenges**
  - Which should provide key opportunities for ambitious middle-managers to develop and prove themselves

Could it be that many security professionals mean something else when they talk about “the skills gap” ?…

# The Cyber Security Skills Gap: Often rooted in 2 different problems

*When they talk about the "skills gap", cyber security professionals often refer to their difficulty in staffing large SOCs or large-scale projects*

1. **The attempt to prop-up manual legacy security operations processes by throwing more "resources" at them, instead of attempting the more difficult task of streamlining them**
   - Many large organisations are stuck with legacy operational processes – around identity management, security monitoring, incident handling or threat intelligence – which are mostly manual, labour-intensive, repetitive and built around countless tools (20 on average according to a 2020 Cisco report)
   - Attracting young professionals in such jobs can indeed be hard

2. **The attempt to "change everything at the same time" where maturity is found too low**
   - But building a monstrous programme of work requiring in theory tens of additional FTEs, and ignoring all dependencies between tasks and cultural aspects, is not how you change things.
   - You would struggle to staff it in any specialised industry – let alone deliver it.
   - This is just bad planning, and it is fuelled by the tech industry and large consultancies.

If the perception of the skills gap is relative to those flawed expectations, what does it really reflect? A real shortage of skills? Poor management ? Or the greed of the security ecosystem?

# The Cyber Security Skills Gap: Compounded by attritive tendencies

*One thing is certain: All this breeds attrition*

*Who would like to be a CISO in such context?*

- **Manual and repetitive security operational processes quickly become boring for young professionals**
- **Over complexifying transformative programmes of work,** ignoring dependencies, governance and priorities setting, and working against arbitrary timelines and resources requirements, simply lead to failure
- **Failure alienates senior management** and fuels the historical tendency to see security as a cost and a problem

What can we do to start changing things?

# The Cyber Security Skills Gap:
# How to start building a new cyber security narrative at all levels

*3 lines of actions for CISOs, senior management and HR teams*

- **Make security more attractive**
  - Ditch the old tech narrative and the visuals of the hoodies and the padlocks…
  - Build a positive business-oriented narrative: This is about the business and protecting it
  - Showcase the diversity of roles, and their transversal nature, working across corporate and geographical silos, beyond tech
- **Create a more stimulating entry-level for young professionals**
  - By decluttering the cyber security estates and automating processes intelligently to allow a smaller number of analysts to work more efficiently, creating a less boring environment for them to fit in and develop within.
- **Build role models and career paths, showcasing real, meaningful and credible bridges across cyber security roles and other roles**
  - At least across the broader GRC spectrum, but ideally across the entire management spectrum
  - Think outside the box and look beyond tech: There is no reason why a CISO would not come from a business role.

The Cyber Security Skills Gap: Real Problem or Self-inflicted Pain?

269 Farnborough Road
Farnborough, Hampshire
GU14 7LY
United Kingdom

Registered in England and Wales
Corix Partners Limited (No. 06774109)

Please be in touch to discuss further

jcgaillard@corixpartners.com

+44 (0) 7733 001 530

www.corixpartners.com

@Corix_JC

@CorixPartners

Thank You