RAISING A CYBER FORCE

WithYouWithMe partners with government agencies to deliver SaaS frameworks that build advanced cyber capabilities. By building, training and deploying a Cyber Force, we ensure nations are equipped to provide defensive and offensive responses to cyber security threats.

THE CHALLENGE

Cyber operations have become the tool of choice by malicious actors to gain proprietary intellectual property and gather personal data worldwide through cyber espionage and cyberattacks. This increases the risk and severity of disruption to integral government and civil infrastructure, information and security.

The conflict of physical borders has shaped 20th century geopolitics. Advancing global cyber capabilities have now added another, more complex domain of warfare. The cyber threat is gaining momentum, and it is imperative a skilled cyber force is grown rapidly.

WHAT IS A CYBER FORCE?

A Cyber Force is an additional branch of an organisation dedicated to defensive and offensive cyber security operations. Whilst the domain is cyber, **people power is at the core**. The larger the Cyber Force, the more capable an organisation is at combatting cyberattacks and espionage.

WYWM provides a SaaS platform for government to **recruit** (internally or externally), **train** and **deploy** personnel to work in a Cyber Force. This system allows for **rapid growth** to match evolving threats in the cyber domain and cast a wider net for talent attraction.

HERE'S AN EXAMPLE

WYWM partnered with the Department of Foreign Affairs & Trade (DFAT) to develop a National Cyber Security Centre (NCSC) for a Government in the Pacific Islands.

Local government workers were aptitude tested; 60+ top performers were trained in cyber security on WYWM's platform under the mentorship of WYWM Cyber Security Specialists.

With great success, learning and training was pivoted to purely online with the interference of COVID 19.

The NCSC is now a fully operational Cyber Force capability staffed by local nationals that provides robust cyber protocols and protection.

WHAT DOES THE FUTURE HOLD?

Defence and government agencies must leverage end-to-end technology to build cyber capabilities. This includes leveraging technology to upskill people and scale their workforce in response to the risks posed by external state cyber threats. Potential cyber workforces can be drawn from multiple generations, ranks, trades and industries, and can be from the military services, government, community, private organisations and businesses.

More contemporary ways of working should be embedded in cyber workforce planning to improve the productivity, efficiency, and resilience of cyber workforces.

1

Reduce reliance on uniformed members in positions where a trained civilian can undertake the same duties.

2

Transform and fast-track cyber skills training to be immersive learning incorporated into real time work environments.

3

Embed a continuous improvement culture through incorporating the skills ecosystem concept.

The inter-dependency of component actors is pivotal in getting the skills equation right – including companies and industry, education and training providers and systems, policy settings and governments, and individuals and the community.

Cyber Security Pathway

- IT Fundamentals
- Networking Fundamentals
- Linux Fundamentals
- OSINT Introduction
- Cyber Security Analyst
- Red Team Essentials
- Red Team Operator- Windows Buffer Overflow
- Cyber Security Awareness
- Phishing Attacks
- Data Protection
- Social Engineering

Accreditations

ANSI

DEFENCE INDUSTRY SECURITY PROGRAM

GCHQ CYBER ACCREDITED

If you are interested in expanding or starting your organisation's Cyber Force, please contact Javiera Soto: javiera@withyouwithme.com

WITH YOU WITH ME