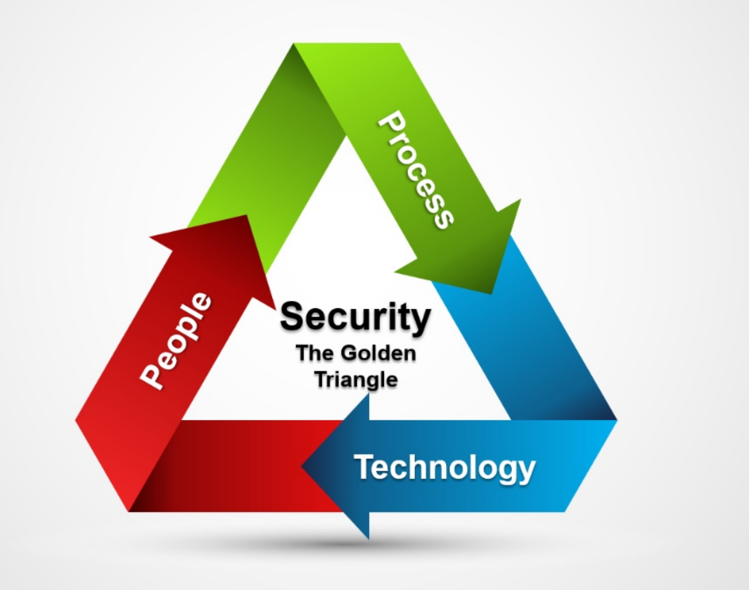
What do we do?

The problem

As cyber criminals get more determined and cleverer in targeting our staff and our organisations, stopping them has become harder by the day. These days social media and Artificial Intelligence play integral parts of cyber criminals and how they work.

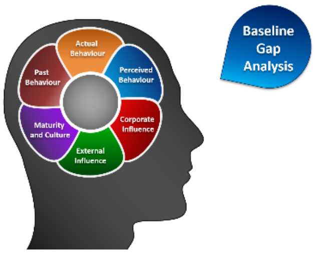
Cyber security risk mitigation, encompassing technology, processes, and people, is an ever-evolving challenge. We must look at all facets of these components.

- Ensuring that the **technology** is up to date, patched correctly, configured properly and, where possible, covering all facets of protection is essential. Even if technology is setup perfectly, this will only stop 95% of the attacks.
- **Processes** are essential to ensuring there are guidelines for staff to follow. These need to be reviewed regularly and made digestible for staff to use. Staff won't read policies that are cumbersome and lengthy.
- **People**, who represent the cause of most of the security breaches, are the only component, that we are not able to fully control. Desires, attitudinal factors, differing personalities, cultural impact, external and personal influences, knowledge levels, and ultimately, behaviour, are components of the Human Factor which require addressing within cyber security.



And ultimately, ensuring that everything fits into the limited budgets available to combat the criminals.

The Solution



To correctly address the Human Factor, we need to look at many facets of behaviour, what causes certain behaviour, and how to best address behavioural risk mitigation.

This is called the B.A.C.K.S program. Behaviour, Attitude, Culture, Knowledge for Security.

Baseline – Human gap analysis

- Knowing where you stand and how best to progress forward with the Human Factor. Incorporating actual behaviour, past behaviour, perceived behaviour, corporate impact on behaviour, cultural impact on behaviour, external influence, and the corporate maturity towards the Human Factor.
- Analysing staff attitudes, behaviour, knowledge, and corporate impact to:
    - Ensure accurate focused training, not wasting time and resources
    - Measurement, where are you now and measuring the progress of the program
    - Return on Investment for reporting
    - Report and planning for program of work

Human Factor Maturity Assessment

- Knowing the maturity of the organisation and the staff helps to better address risk mitigation.
- It incorporates:
    - Incident response procedures
    - Security Culture
    - Staff responsibilities
    - Policies
    - Knowledge
    - Attitudinal components

Security Culture Audit

- What happens when people are left to their own devices.
- Is the security culture aligned with corporate culture, easy to work within, manageable, engaging, rewarding, and deliberate?

3rd party / vendor audit

- Understanding the impact that your 3rd party vendors may have upon your organisation

Historical analysis

- Who are the staff that are most at risk, historically?

Physical security audit

- Understanding the physical security threats, who leaves paperwork lying around, who allows strangers into the building, the conversations undertaken in public spaces for others to overhear,

Social Engineering

- Phishing
  - Email
    - Spear
    - Generic
    - BEC
    - Whaling
  - SMS
  - Social Media

Training

- Online
  - Customisable Australian courses built for Australia, using Australian content.
- Face to face – Interactive and engaging
  - Lunch and Learn
  - Work shops
  - Webinars
  - Teaching
- Facilitated
- Exams – run two weeks after the training to understand the depth of knowledge retained.

Reinforcement

- Reinforcing the message, continuously:
  - Articles
  - Screensavers
  - Posters

- Videos
- Games
- Animations
- Phishing teaching sites

Games and team building

- On-line
- Physical – Cyber Escape Room

Do not just create awareness, change behaviour, and measure the change.

For more information:

Web:	https://layer8security.com.au
Web:	https://cyberescaperoom.com.au
Email:	information@layer8security.com.au
Phone	1300 706 536