

# ACH

## AUSTRALIAN CYBER HUB

Despite increased awareness of the problem in human resource management, many companies, agencies and organisations lack the cyber awareness they need to protect themselves from attack.

The challenge facing every organisation, from the smallest SME to the largest government agency, is building and maintaining a constant and positive culture of cyber awareness involving every employee.

### Three Rs of data theft or misuse

#### REVENUE



Cyberattacks can and do defraud companies and agencies, stealing large amounts of money or data from them.

#### REGULATION



Breaches of cybersecurity can open your organisation to prosecution and fines by regulatory authority when lax procedures are shown to be at fault.

#### REPUTATION



Your good name is easy to lose and hard, if not impossible, to regain. Data breaches destroy the faith of users in a company, which can prove disastrous in this internet age.

**ACH is focused on people because people are the most vulnerable point in any cyber defence.**

Simply put, it is easier to fool a person than breach a protected network.

Therefore, organisations must understand:

- ✓ How susceptible are my people?
- ✓ How can we reduce susceptibility?
- ✓ How can we measure and maintain an ongoing reduction in susceptibility?

**ACH helps organisations answer these questions.**

We provide services that help organisations prevent malicious cyberattacks by educating employees to recognise and respond to suspect activity. We do this by undertaking the following steps:

#### STEP ONE SIMULATION



Deploy email and SMS simulations of real-world attacks, e.g., a Ransomware attempt or malicious attachments

#### STEP TWO ANALYSIS



Analyse employee responses with tools such as DCOYA cognitive computing algorithms

#### STEP THREE REPORT



Report and recommend actions to mitigate susceptibility by employee segments

#### STEP FOUR ACTION



Implement recommendations (inhouse or with our help)

#### STEP FIVE REVIEW



Increase sophistication of simulations on an agreed schedule and repeat analysis