

# CULTURE EATS TECHNOLOGY FOR BREAKFAST

**CCS** CULTURAL  
CYBER SECURITY



# In this whitepaper, we explain that:

**Effective cyber security relies more on people and culture than on technology.**

**A cyber-safe organisation culture reduces risk and increases performance.**

**Cyber security culture can mitigate your number one threat vector.**

## Worried about cyber security? You should be!

**Boards, CEOs and CISOs are rightly worried about cyber security given major breaches at Optus, Medibank and Latitude Financial last year.**

**Cyber security costs trillions globally and will continue to escalate.**

People and culture are the biggest weaknesses NOT technology. Few cyber breaches (usually 5% or less) are attributed to technical or systems failures. The vast majority of breaches (95%) are attributed to people and the organisational cultures that drive their attitudes and behaviours. For example, phishing emails are still the number one threat vector for cyber breaches in organisations. According to our research, few people in organisations talk about cyber security and cyber-safe behaviours on a regular basis. Many people use the same passwords on multiple sites and do not regularly change their passwords. Some people even send suspicious emails from their personal accounts to their work email address to run them through phishing filters at work to see if they are safe!

Cyber criminals are targetting people more today than ever before. Phishing attacks are the number one threat vector. We know that cyber criminals are focusing more on people because that has been the foundation of their success. With the significant increase in the proportion of people working from home post covid, this trend will continue and will undoubtedly accelerate.

Current approaches are not working. We also know that one-off, or once-a-year, online, "tick-the-box" compliance-oriented cyber security training is becoming more popular, but it is not enough to reduce your cyber risk and truly educate people because it does not result in lasting behaviour and attitude change.

**The solution: CEOs and CISOs need to focus more on people and culture.**



### CYBER BREACHES

5% or less: technical or systems failures 

95%: people/organisational cultures, attitudes and behaviours 

# A cyber-safe organisation culture is a powerful factor affecting peoples' values, attitudes, beliefs and behaviours at work.



People must **examine each and every email** they receive more carefully.



People must **never respond** to unsolicited emails, phone calls and text messages.



People must create and use **unique, strong passwords** and pass-phrases and manage them appropriately.



Everyone must **talk to each other** about cyber security, **support** and **educate** each other, and treat each other with **respect**.



Organisations must develop cultures that encourage these **values, attitudes,** and **behaviours** and we need leaders who act as role-models.



# Why people and culture are now more important than technology for cyber security.



Increases in modern cybercrime over the last decade have been unprecedented. Starting from almost nothing in the 1980's and 1990's, cybercrime is projected to cost tens-of-trillions of dollars by 2027 ([statistica.com](https://www.statista.com)).

Today, only about 5% of breaches are attributed to systems or technical failures<sup>1</sup>.

The other 95% have to do with people and the organisation cultures that drive their behaviours. Firewalls, virus protection, application whitelisting, patching and hardening, as well as multi-factor authentication, continual back-ups and other technologies do their jobs quite well ... people are the weakest link and organisation culture is what makes the biggest difference to cyber safe behaviour and the attitudes of people. Technical solutions are necessary but no longer sufficient for successful cyber security.

OK ... so what is organisation culture and what do people and organisation culture have to do with cybercrime and cyber security?

<sup>1</sup> The Office of the Australian Information Commissioner, <https://www.oaic.gov.au/>, Notifiable Data Breaches Statistics Reports.



## Why organisation culture is important

**Culture drives cyber-safe behaviour.**

**Culture drives high performance.**

**Culture drives organisational success.**

**Culture drives individual success.**

**For example,** if everyone knows that in this organisation, we take cyber security seriously and we never get up from our computers without logging off, no matter what, this expectation will be communicated, enforced, and reinforced. If someone fails to do the right thing, someone will say something or the 'looks' they get will communicate volumes. Norms, expectations, and assumptions at the core of the cyber-safe organisation culture helps us influence people and drive cyber-safe behaviours. That is why culture is a secret to success and why people and culture are now more important than technology for cyber security.

Culture is the  
"secret ingredient"  
for success



# Reduce cyber risk by promoting cyber safe ideas, knowledge, values, and behaviours

Success and high performance take time and effort.

The connection between organisational culture and performance is straightforward. Organisation culture influences the behaviour of staff, as well as the customers, suppliers, and other stakeholders with whom they interact. These affect (i.e., it can either help or hinder) the achievement of organisational objectives. Cultures that encourage the kinds of behaviours associated with performance above the level of competitors (i.e., a high-performance culture) will provide a competitive advantage, and the reverse is also true.

What this implies for us is that if we want people to recognise and report all suspicious emails, log-out of their computers when they leave their workstations, use unique strong passwords, as well as discuss and hold each other accountable for cyber safe behaviours, we have to promote an organisation culture that guides people in the right direction, rewards and recognises cyber safety, and gradually, reduces cyber risk by promoting cyber safe ideas, knowledge, values, and behaviours.

Employee Engagement



Empowerment



Continuous Improvement



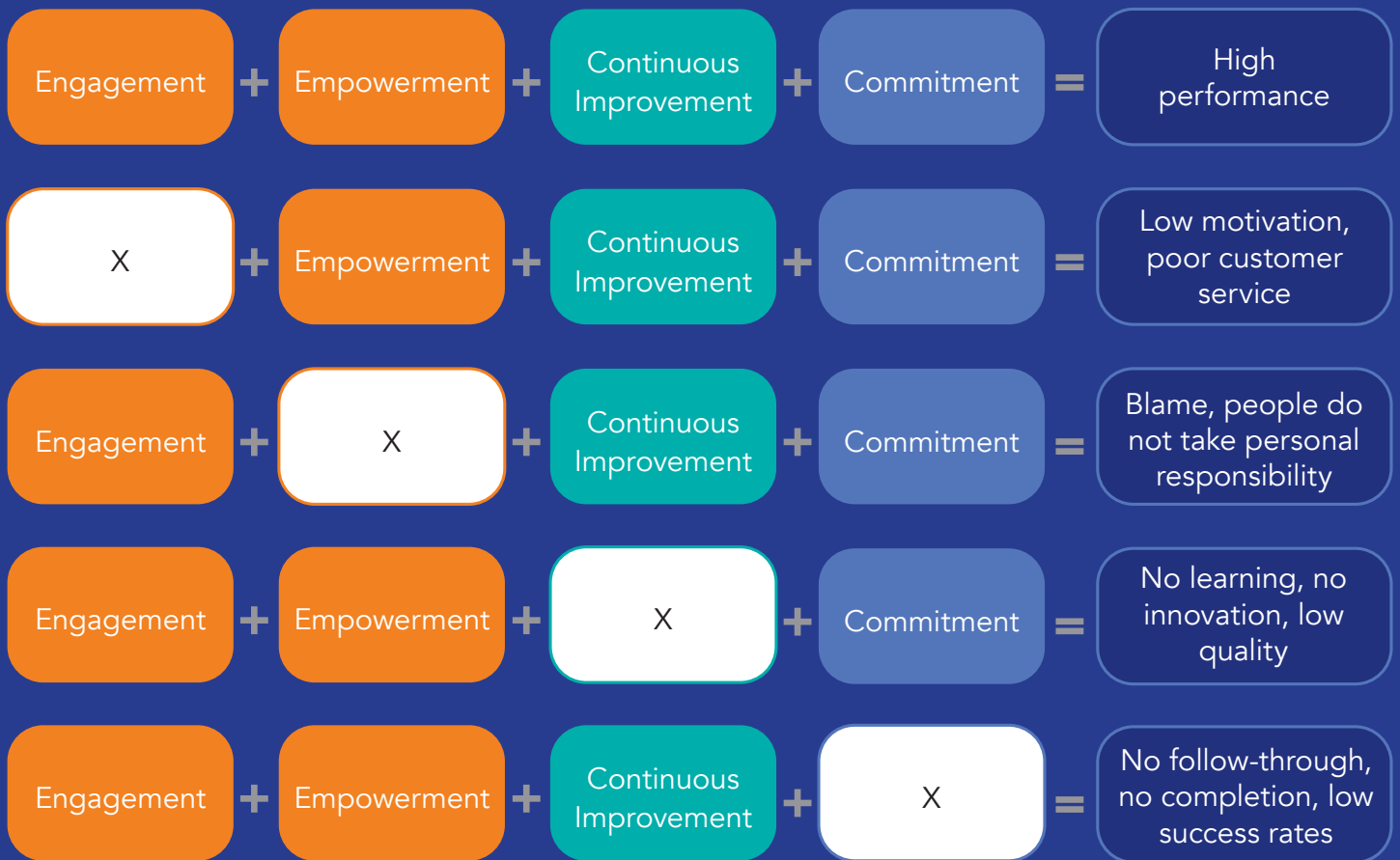
Commitment



A Culture of High Performance

## Important elements of organisation culture

## Result



**It often takes time, or an unfortunate significant cyber breach, to generate enough willingness and energy to provide the motivation to change long-standing organisational systems, policies, procedures, and cultures.**

#### **How to make cultural cyber security happen.**

Changing an organisation's culture is many times more difficult than changing its structure, its processes, or its technology. This is so for many reasons.

#### **First, an organisation, and its culture, are self-reinforcing.**

Culture is embedded in the organisation structure, processes and people, and the organisation and its people are enmeshed in the culture. Because of this, many things need to be changed in order to change culture.

#### **Second, cultural change requires both personal and organisation level changes to happen.**

Personal change is difficult. People quickly fall into routine patterns of behaviour. Habits are hard to change. Organisational systems, policies and procedures are designed not to change. Another reason culture is difficult and time-consuming to change, is that it takes time, or an emergency, for people's behaviour, values, attitudes, and beliefs to adjust.



# The program we suggest follows a rational, five step process:

## STEP 1: Establish the baseline

- Conduct a cultural diagnostic
- Identify cultural maturity levels, establish baseline, identify key areas and at-risk behaviours, acquire staff comments and insights

## STEP 2: Define desired future state

- Conduct maturity model assessment
- Identify future desired state and maturity level

## STEP 3: Planning

- Develop 3-year strategy aligned to business
- Develop roadmap and 12 month Operational or Action Plan

## STEP 4: Actions

- Establish understanding of the “why” of cyber security
- Deliver leaders and managers programs
- Staff information/learning sessions
- Improve phishing simulation program
- Integrate cyber life skills
- Gamified learning
- Develop the communication plan

## STEP 5: Accelerate

- Deliver cyber champions programs
- Continued communications, induction, education, training, awareness activities




# If you want cyber-safe behaviours, you will have to create a cyber-safe culture.



The social environment and organisation culture significantly impact individuals' thinking and behaviour.

If you want cyber-safe behaviours, you will have to create a cyber-safe culture. You will have to instil cyber-safe values and beliefs that generate cyber-safe norms and expectations that result in visible cyber-safe behaviours.

While a one-off induction to where to find policies and procedures for annual leave may work perfectly well, cyber criminals are constantly experimenting, innovating, and changing their plans and activities. People do not often remember well what they have been told only once. People are often overwhelmed during inductions as they are given mountains of information and they simply cannot recall everything they are exposed to. People get busy and distracted by urgent and important daily work pressures, and one-off or yearly refresher training often is quickly forgotten. For these reasons and others, people must be regularly and consistently reminded of cyber security principles, as with OH&S. 

# CCS can help you develop a cyber-safe culture

CCS staff have over 50 years' combined experience in combatting cybercrime and focussing on educational programs and awareness efforts to build cybersafe capabilities inside organisations and communities.

We also possess over 30 years' organisational psychology experience in building, influencing, and changing organisational cultures, thereby facilitating large-scale organisational change.

We approach this challenge with a unique and proven methodology. We focus on transformational outcomes, building quality relationships, and partnering with clients strategically for the long-term.

CCS currently supports 60+ clients from Rockhampton to Tasmania ranging in size from 100,000 seats down to 12. In addition, we now service clients in Papua New Guinea and the Solomon Islands and have a number of clients in locations throughout Asia.

If you want to reduce your cyber risk ...

If you want to drive your organisation toward cultural cyber security ...

If you want your people to adopt cyber safety as a part of everyday business ...

... contact us at Cultural Cyber Security



**Brian Hay, APM MPPA**  
Executive Director



**James Carlopio, BA MA PhD**  
Executive Director



Please contact:

0488 028 054

[jcarlopio@culturalcybersecurity.com](mailto:jcarlopio@culturalcybersecurity.com)

[www.culturalcybersecurity.com](http://www.culturalcybersecurity.com)