Education Framework

Cognitive Education Framework for Cyber Security

A COLLOBORATIVE COMMUNITY APPROACH ALIGNING TO TENETS OF AKO

Making Cyber Hygiene a Priority

Wintec
WAIKATO INSTITUTE OF TECHNOLOGY
Te Kuratini o Waikato

Agenda

01 **Re-Asserting**

Why is Cyber Security Education important?

02 **Reviewing**

Threat Matrix of a broken education framework.

03 **Motivation :Government and Industry Needs**

Initiatives in the Last 24 months and impact

04 **Present and Future Work**

Ako : the thread that binds all of this

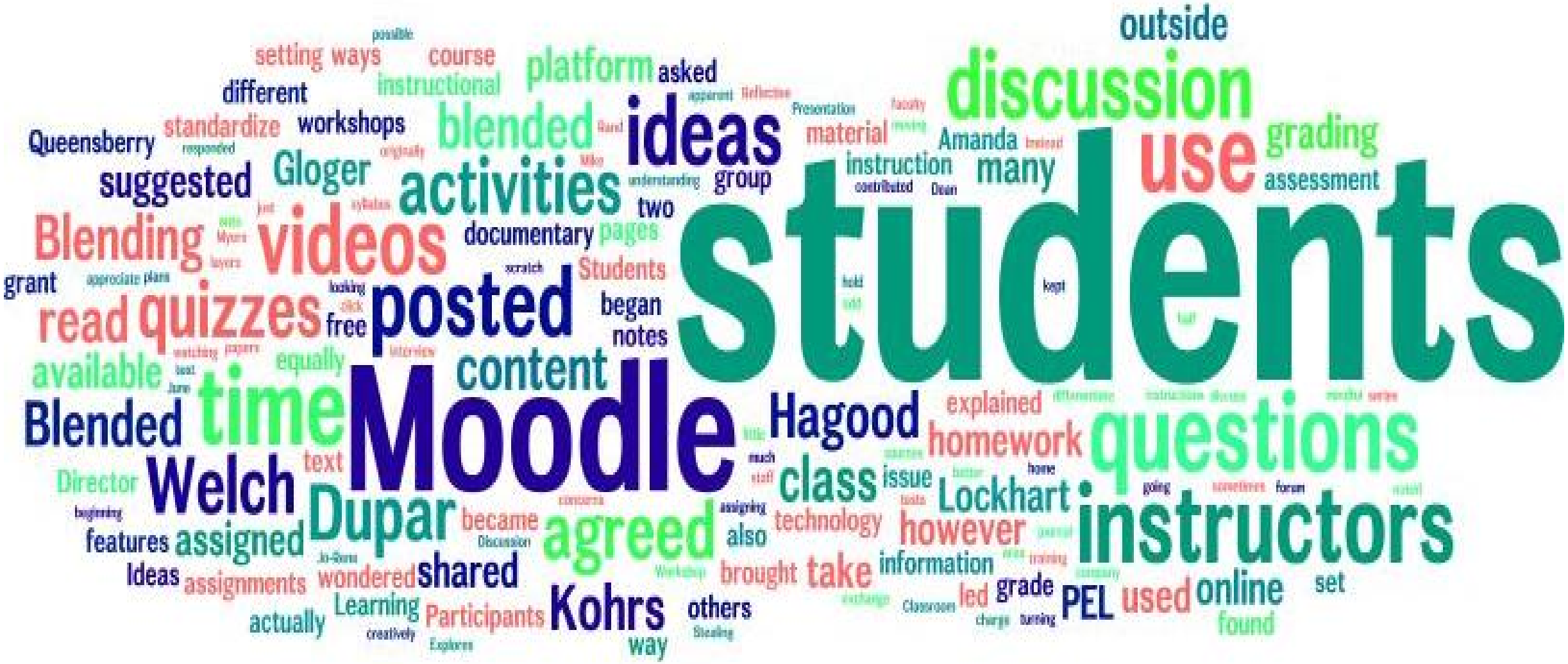
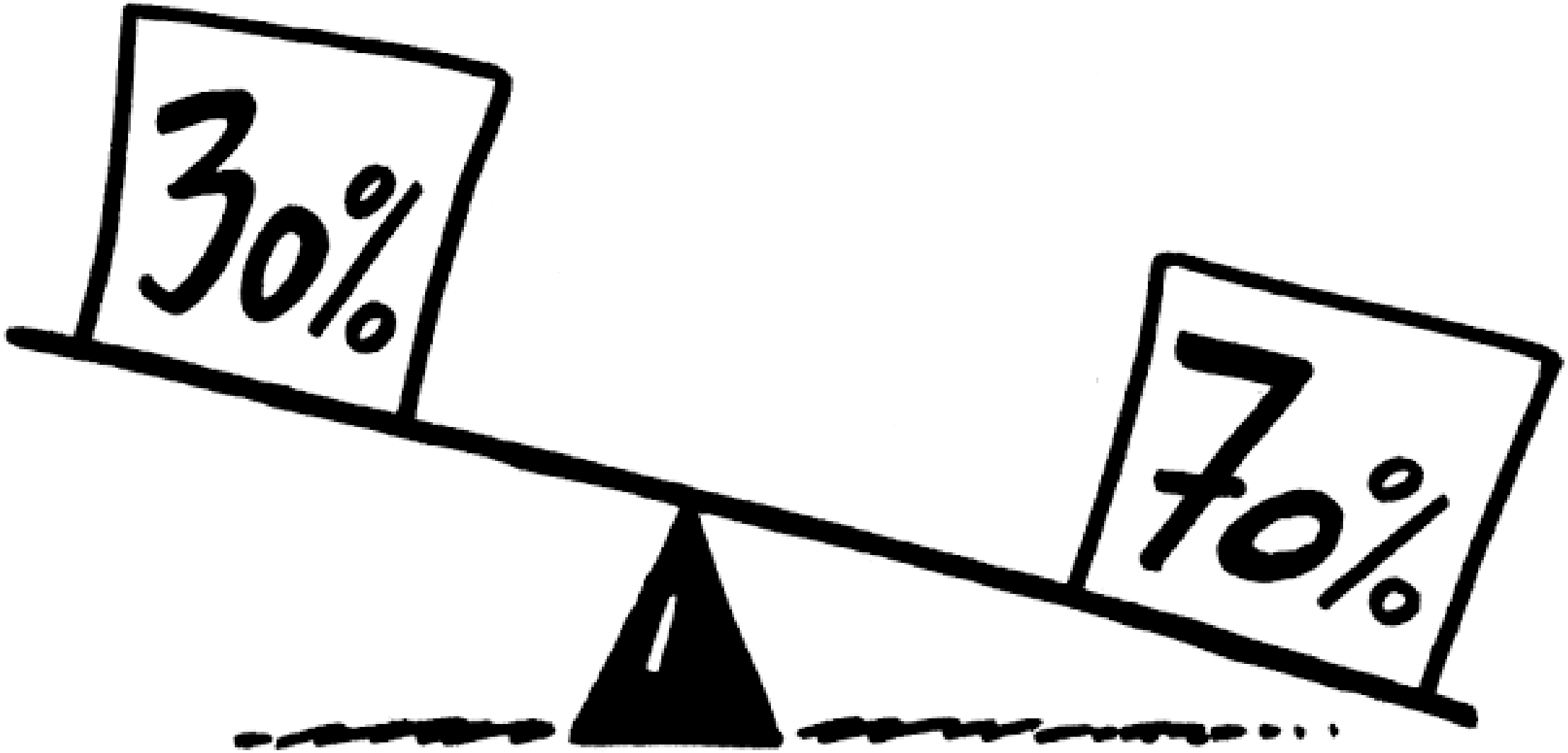


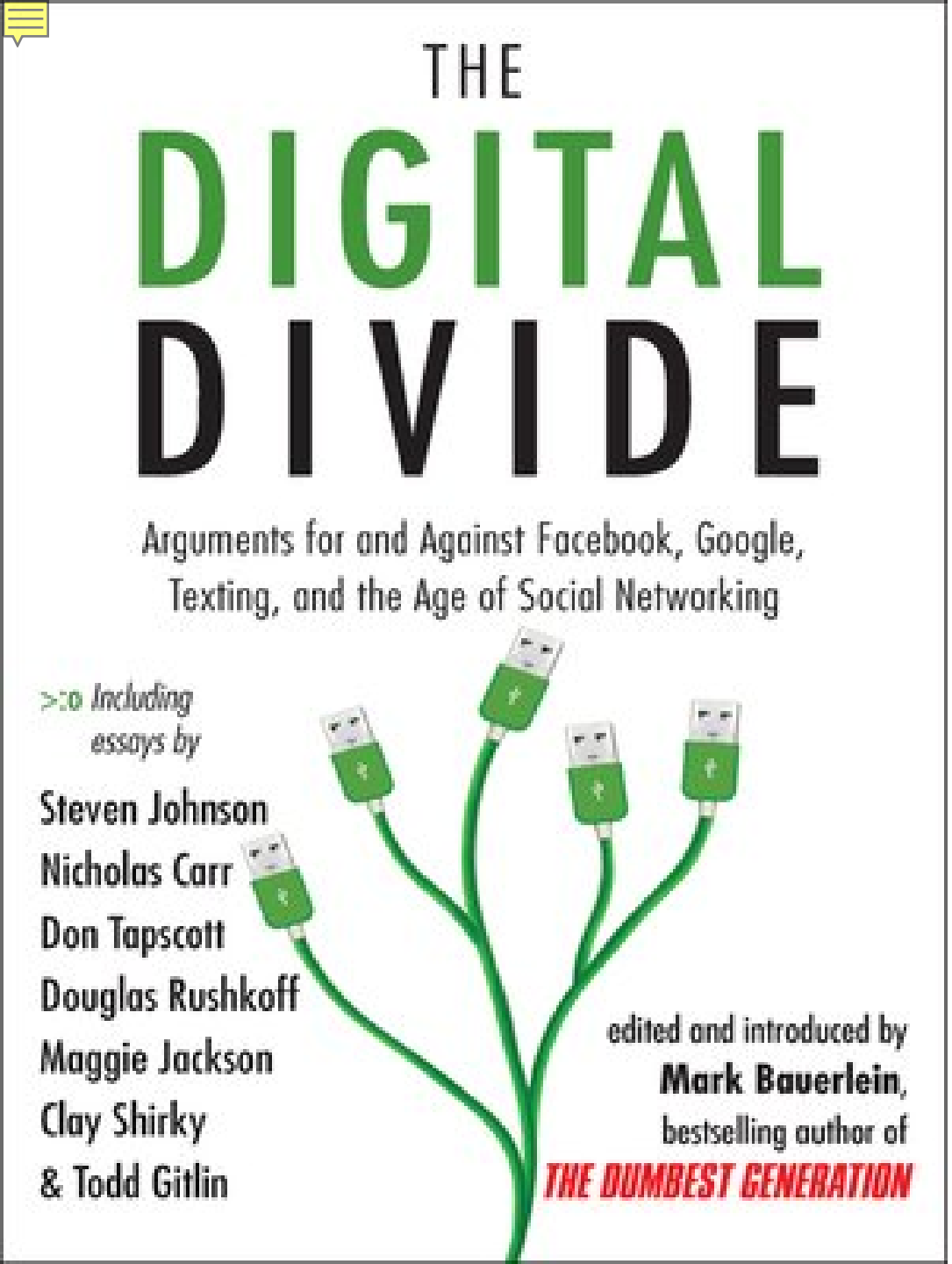
Image source : http://pelinhouse.blogspot.com/2015/12/blended-learning-tips-and-tools-blended.html

Image Credit : Julia Sowells, https://hackercombat.com/hire-hacker-latest-cyber-crime-service/

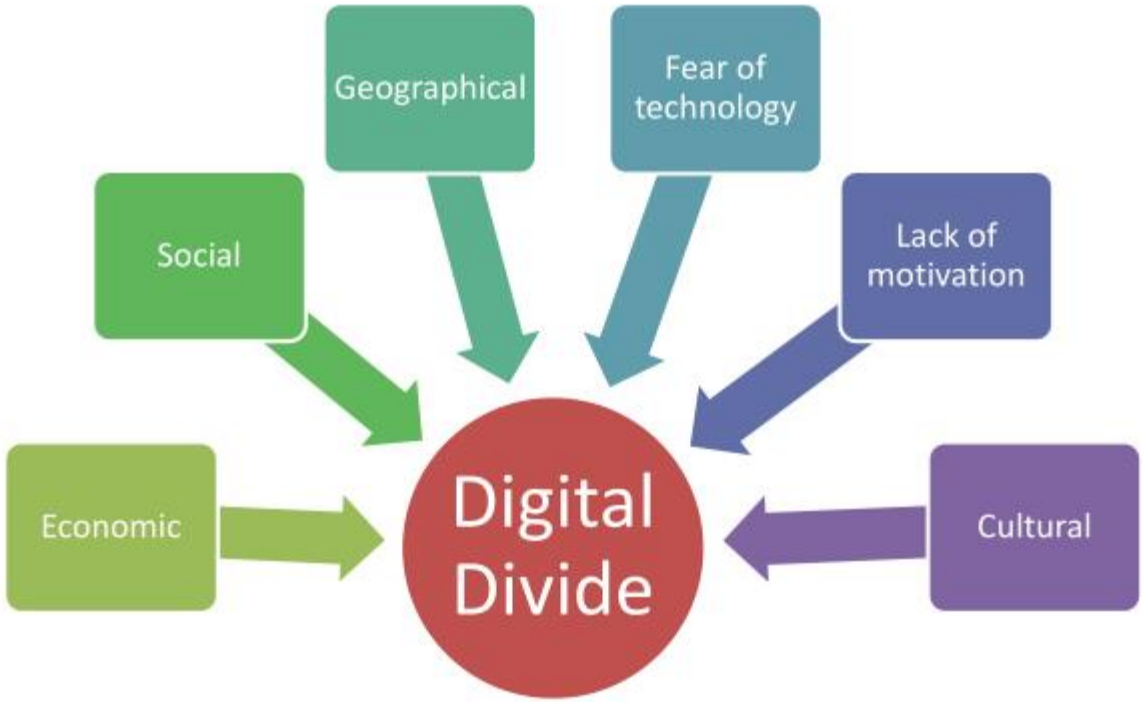
- Identity theft
- Fraud
- Digital personas Impersonation

Visible and Invisible Risks


30%
70%



5 Factors which contribute to the digital divide:



Education ?

VS

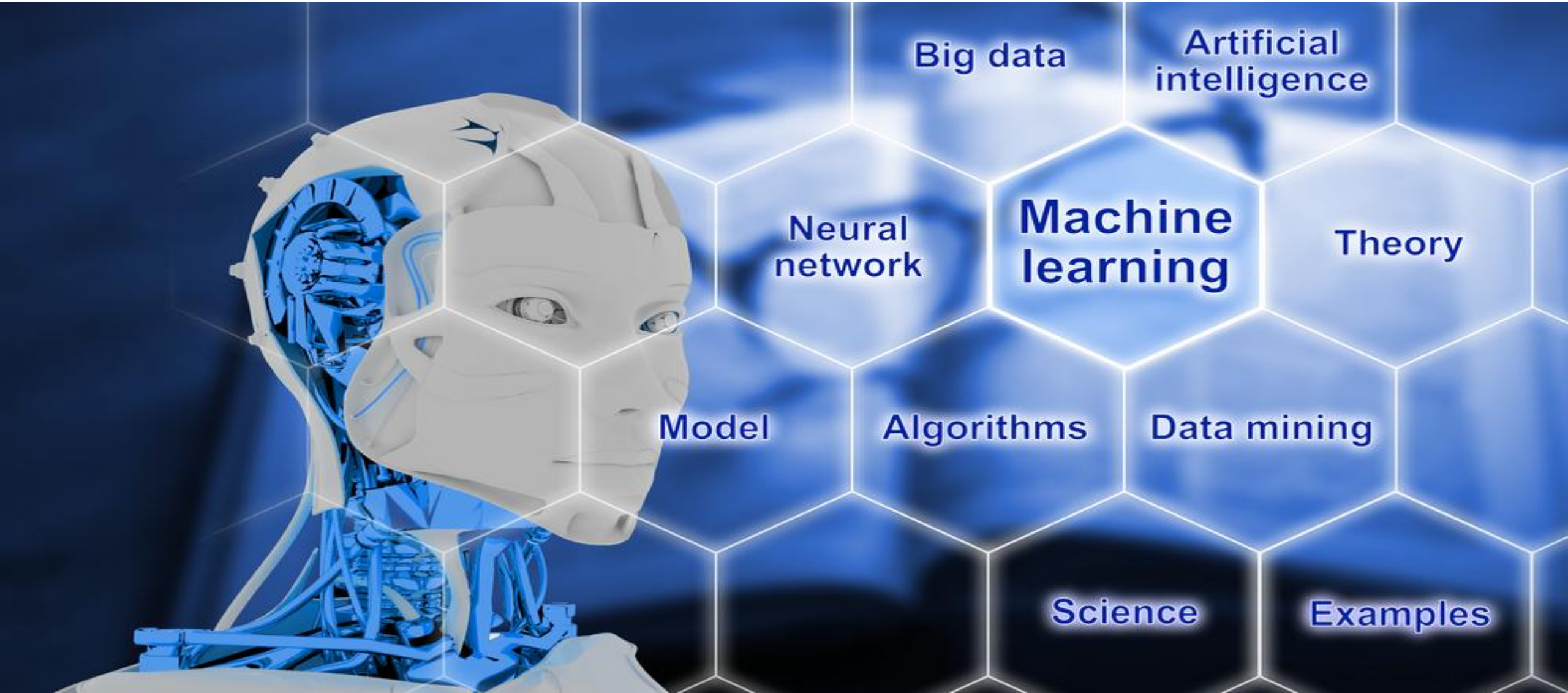
Societal Evolution

Educational Failure!

Risk Matrix in a Digitally Divided Society

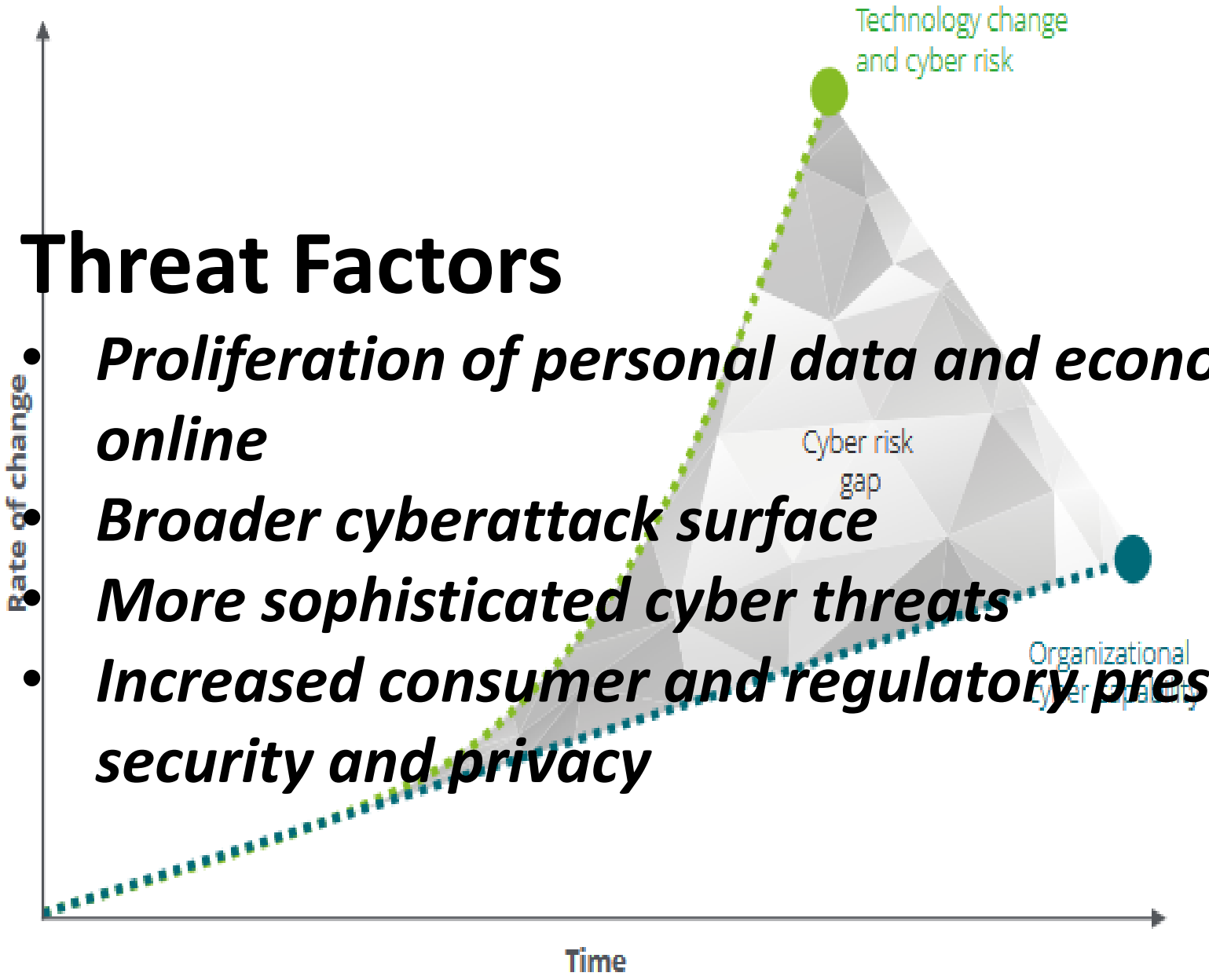
A New Zealand Context

Cyber Risks Matrix



Threat Factors

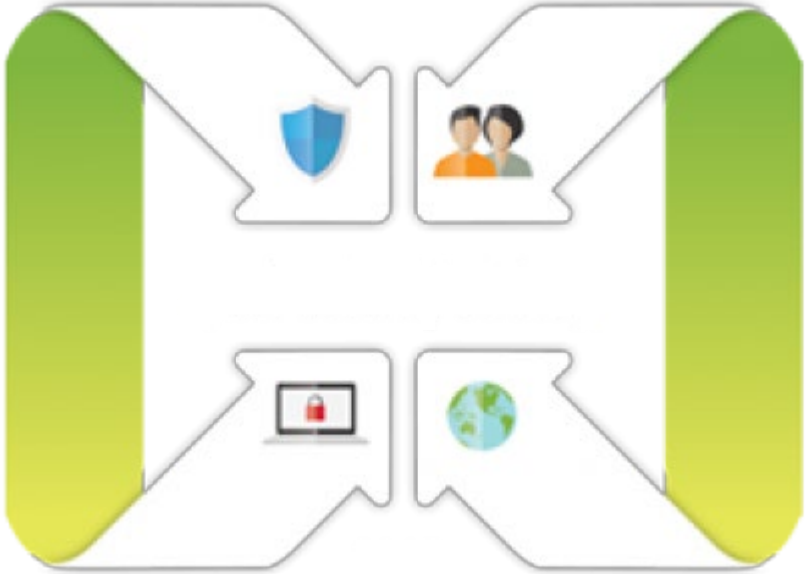
- ***Proliferation of personal data and economic value online***
- ***Broader cyberattack surface***
- ***More sophisticated cyber threats***
- ***Increased consumer and regulatory pressures for security and privacy***



$3 Trillion in Lost Economic Value

certnz

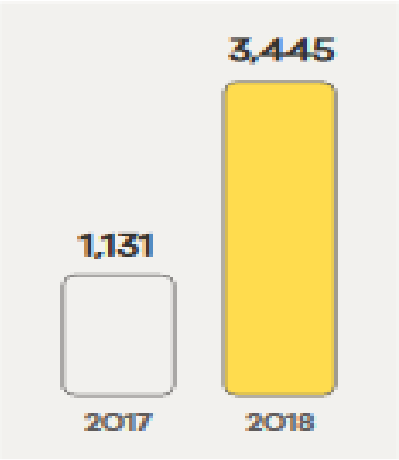
NCSC



CERT NZ /// 2018 Summary

What we've seen ///

Reported incidents

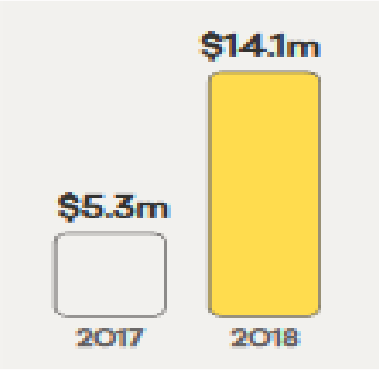


In 2018, incidents reported to CERT NZ **increased by over 200%**. These reports were received from individuals, small businesses and large organisations from all over New Zealand.

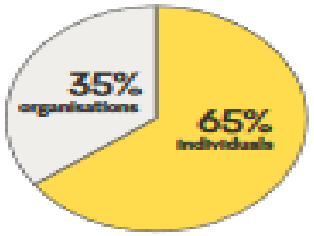
205%
increase in reports

Financial loss

18% of reports made to CERT NZ had some form of financial loss with a total value of **$14 million.**



65% of the reports of financial loss **affected individuals.**



Over $8m
of this loss was attributed to **scam and fraud reports.**

Top incident categories

The **top three incident categories** for 2018 were also the highest in 2017.

Phishing and credential harvesting	1,550
Scams and fraud	1,136
Unauthorised access	303

Vulnerability reporting

Vulnerability reports present **a chance to prevent a cyber security incident** before it occurs. Vulnerabilities reported to CERT NZ have ranged in severity and complexity.

124 vulnerabilities were reported to CERT NZ in 2018, **22 were managed** under our coordinated vulnerability disclosure service.

For coordinated vulnerability disclosure, **CERT NZ acts as an intermediary,** coordinating with the finder and the vendor to get the vulnerability fixed.

Websites and web servers accounted for over **60% of vulnerability reports** made to CERT NZ in 2018.

New Zealand Government

Up 205%

$14.1m Loss

Key Takeaways

- **Commitment to building a connected nation and harnessing digital technology for economic growth, community benefit and innovation**
- **Establish a CTO office**
- ***Responds to the clear upward trajectory of cyber security threats***
- ***Reflect on the evolving and ongoing cyber security risk***
- **Intensify cyber security efforts of our Five Eyes partners**

Comprehensive Collaborative Framework for Inclusive Cyber Security Training

Values and Priorities – NZ Plan

Values

- Partnerships are essential
- **People are secure online**
- Economic growth is enabled, and
- National security is upheld

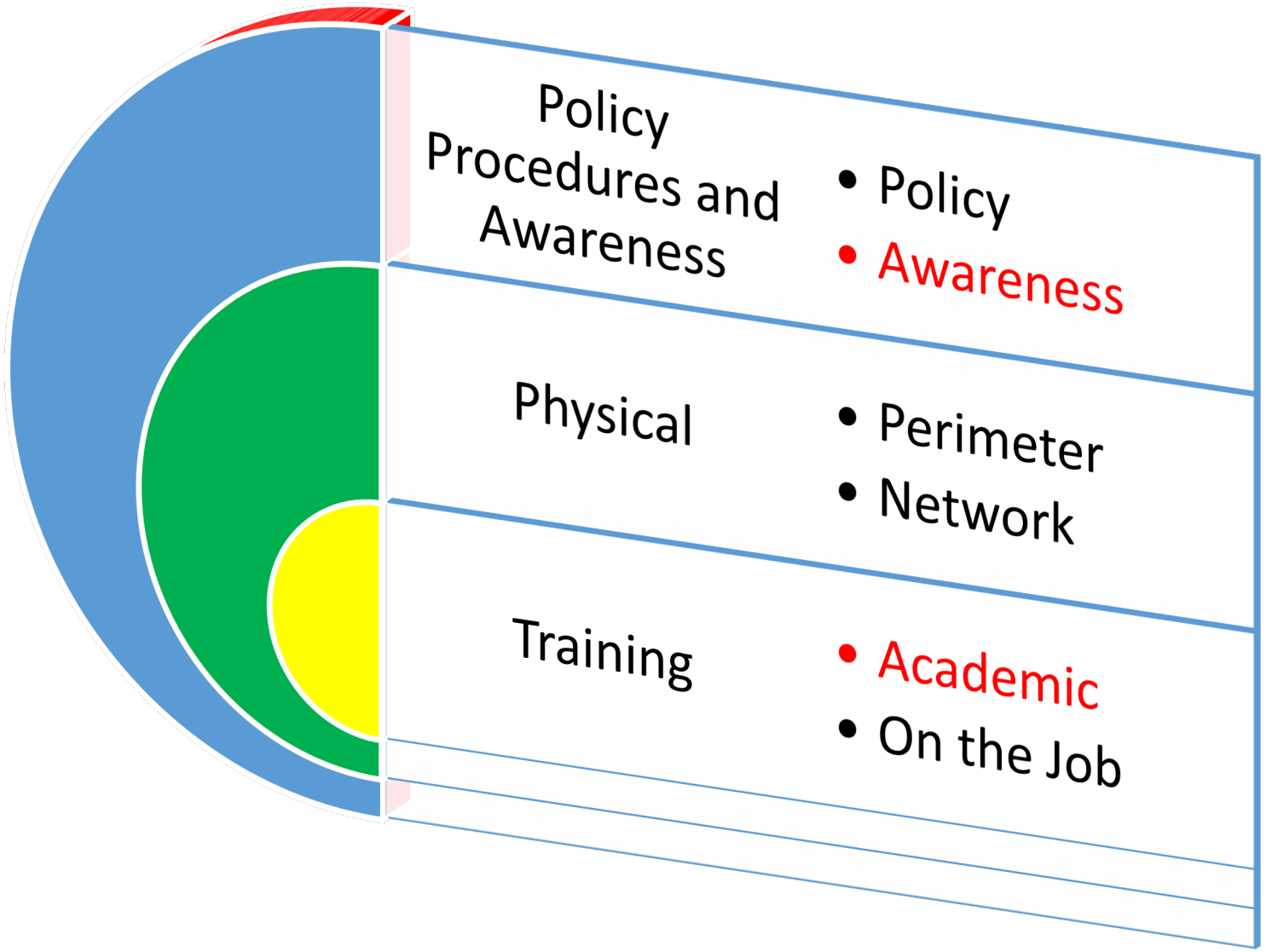
Priorities

- **Cyber security aware and active citizens**
- **Strong and capable cyber security workforce**
- Resilient and responsive NZ
- Internationally Active
- Proactively tackle cybercrime

Framework

A consequence of the Threat Matrix

Threat Response/Mitigation

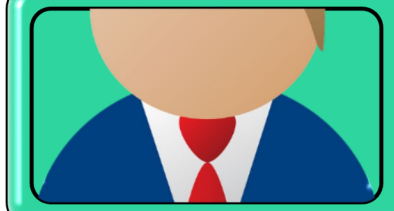


Cyber Secure
Cyber Aware
Cyber Issue
Resilient

Cognitive Education Framework for Cyber Security Education (CEF-CSE)

Training at School Level

Training at Tertiary Level

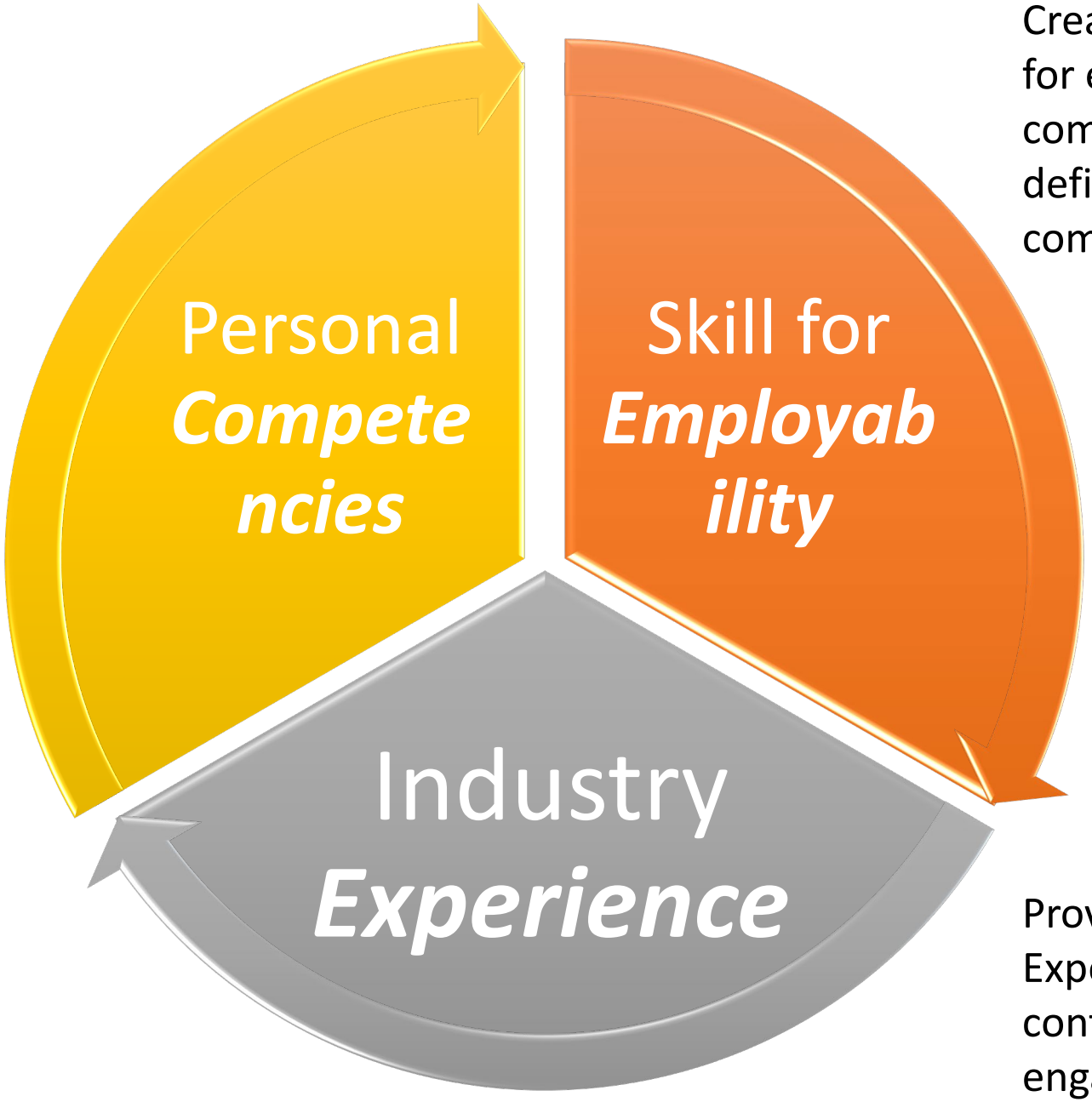


Training for Business Users

Training for Industrial Workforce

Objectives

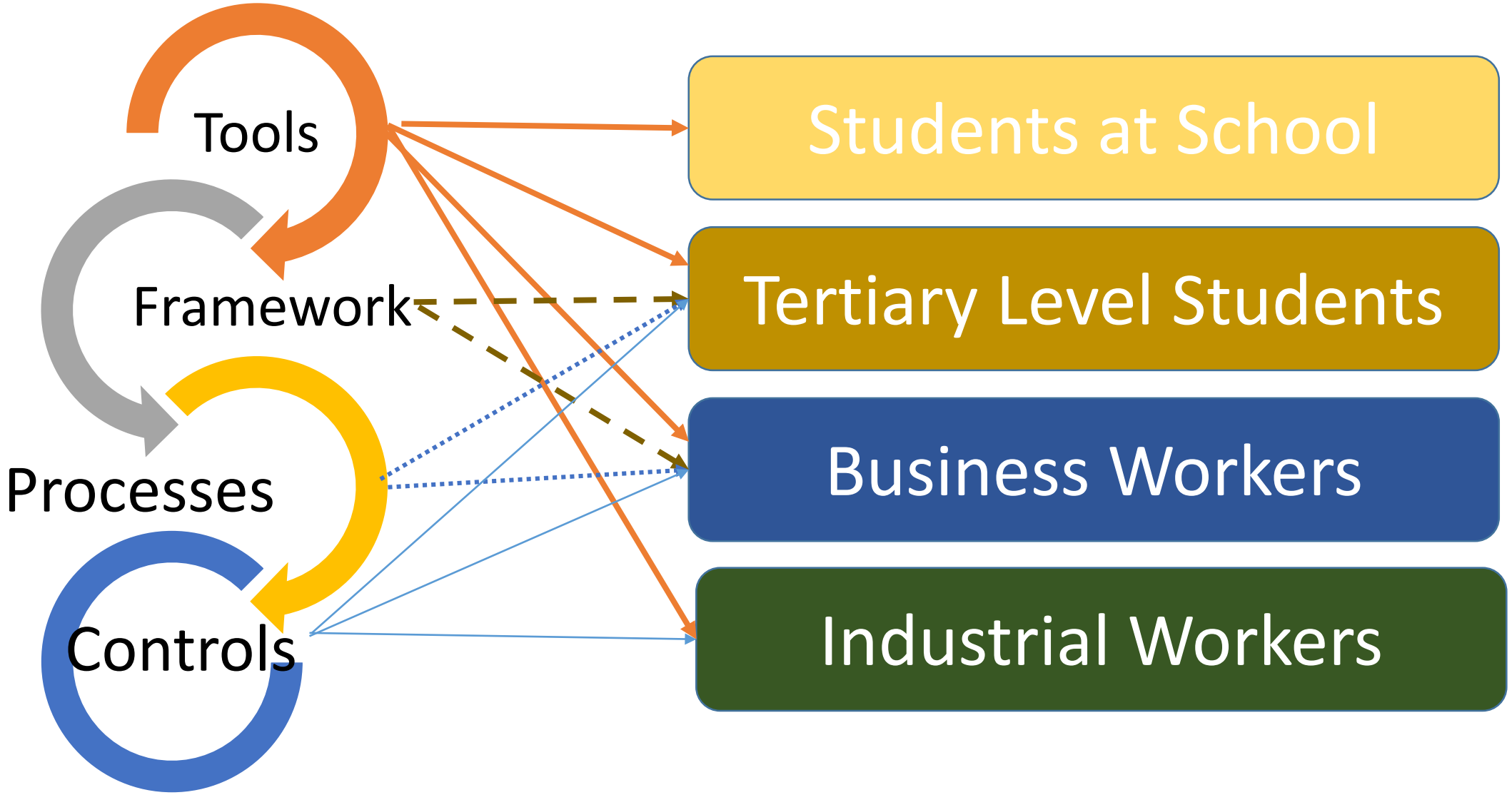
Improve personal competencies across Levels (Level 6 Diploma for Cyber Security, School Cyberstart programs, short courses for industry and business etc.



Create an Ecosystem for employment of competent workers by defining the levels of competencies desired

Provide industry Experience through a continuous upskill and engagement program

Cognitive Structure for Cyber Security Education



Educational Imperatives

- A framework to provide a curriculum for knowledge-supply chain - dovetailed for Cybersecurity – From ***School to Industry***
- Aligned with recognised certifications in the Cyber Security Domain
- Encompasses certifications, micro-credentials, exercises, seminars, courses and challenges – something for every section of the population
- Aligns with Ako

Ako Alignment

- **Mahi Tahi** – Working Together - It needs team work and collaboration at ALL levels to achieve the synergy needed for effective Cyber Security upbringing of our students.
- **Tuakana Teina** - Based on the relationship between an older person and a younger disciple – Works top down with the leaders in the whanau working to teach and train the younger members
- **Whanaungatanga** – A process which needs establishing links, connecting with people, institutions, subject area experts, schools and developing points of engagement which propels a cyber clean ecosystem.

CEF-CSE

Tools

+

Frame work

+

Proces ses

+

Contr ols

Cyber Security Posture

Used for

- Students at School
- Tertiary Level Students
- Business Workers
- Industrial Workers

To Enhance

- Personal ***Compete ncies***
- Skill for ***Employa bility***
- Industry ***Experience***

Through

Collaboration – Mahi Tahi

Mentoring - Tuakana Teina

Group Work - Whanaungatanga

Initial and Future Work

- Three terms worth of work has been put into creating scenario based cyber security and forensics training at Graduate and Post Graduate levels
- Interaction with schools in Waikato region is in the offing
- Identification of a New Zealand based taxonomy for roles in Cyber Security profession in line with the NICE structure used in the US, SmartCyber program of Canada and ISEA in India is proposed
- Reaching out to Whanau/family level cyber hygiene representatives and creating personas of ideal members is planned for a cyber hygiene program


QUESTIONS
ANSWERS

stay safe