Education Framework
Cognitive Education Framework for Cyber Security

A COLLABORATIVE COMMUNITY APPROACH ALIGNING TO TENETS OF AKO
Making Cyber Hygiene a Priority
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
• Identity theft
• Fraud
• Digital personas
Impersonation

Visible and
Invisible Risks
5 Factors which contribute to the digital divide:

- Social
- Geographical
- Fear of technology
- Lack of motivation
- Cultural

Education ?
Societal Evolution

Educational Failure!
Risk Matrix in a Digitally Divided Society

A New Zealand Context
Cyber Risks Matrix
$3 Trillion in Lost Economic Value

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
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.

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>1,131</td>
</tr>
<tr>
<td>2018</td>
<td>3,445</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Year</th>
<th>Financial Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>$5.3m</td>
</tr>
<tr>
<td>2018</td>
<td>$14.1m</td>
</tr>
</tbody>
</table>

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 cybersecurity 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.
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
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

- Policy Procedures and Awareness
  - Policy
    - Awareness
- Physical
  - Perimeter
  - Network
- Training
  - Academic
  - On the Job

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

- Tools
- Framework
- Processes
- Controls

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

Framework

Processes

Cyber Security Posture

Students at School

Tertiary Level Students

Business Workers

Industrial Workers

To Enhance

Skill for Employability

Industry Experience

Personal Competencies

Used for

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