Summary of notes from Cyber security qualification sector workshops 3 & 7 March 2017

Key question considered

Does NZ need a cyber security qualification and what evidence of need is there?

Context

IT Professionals New Zealand and the NZQA National Qualifications Services team are co-developers of sub-degree computing and IT qualifications on the NZ Qualifications Framework.

36 attended the sector meetings held 3 & 7 March 2017 in Auckland and Wellington, to explore the need for a cyber security qualification in New Zealand.

It was noted that there isn't any dedicated security or testing qualification in the new IT qualification suite, as in 2013 it was thought they may sit at Level 7, outside the scope of the review. Some existing IT/Engineering degree qualifications have a paper/course (elective) within it on these topics, but no specialist qualification.

Summary from cyber security meetings

- Evidence of need for a cyber security qualification through skills shortages in cyber security – locally, globally, and a growth area (can't get enough people to fill skills gaps in security analyst roles).
- Some vendor Certificates are highly valued in the Cyber security space (see NICCS – Cyber security Certifications list), although some less well-valued where content can be rote-learnt. Examples of existing options include CREST (Australian Cert), OSCP (hands on for offensive security - hacking), ISC2, SANS, MooC's, security boot-camps, Bug Bounty.
- NZ Cyber Security Skills Taskforce keen to develop a Level 6 qualification that would include practical placements as an alternative pathway into junior security roles.
- Sector meeting feedback that job roles most likely to be entry level security analyst and maybe engineer. Not seen as suitable for entry level pen-testers, auditors, incident responders (degree qualified and significant work experience important for these roles).
- Two key target markets - school leavers (primarily a shorter study/learn on the job practical option), and re-trainers (mature re-trainers with practical IT experience).
- Compulsory practical aspects are most attractive to employers – quality of these is important. Educators would support the qualification based on feedback from industry that they would employ graduates. *Note: Need industry commitment to providing placements for practical aspects of the qualification (providers advised issues with getting placements for current degree students).*
- Important to include practical application, industry engagement, consideration of funding for employers to support proposed internships etc. Query around apprenticeships and how these might work, along with flexibility for retraining on the job/part-time.
- 1+ year Diploma qualification outline considered by attendees – seen as an added pathway rather than a solution to the industry skills-gap problem.
- Proposed qualification could provide foundational knowledge for a Tier 1 security analyst, but thin understanding requiring on-the-job upskilling.
- NZ Certificate in IT Practitioner (IT security strand) option exists for retraining/upskilling those with suitable practical IT experience.

Following is the typed up version of what was on the whiteboard

Gaps	Job Roles	Need
• Industry certificates • Hacker mindset • Understand environment • Analytical/ability to learn • Speed of change • Foundational knowledge • Practical application • Industry involvement • Practical components /interns • Pre-requisites – broad IT base (school, Level 5 Certificate/Diploma or equivalent experience.	• Breakers – ~~Pen-testers~~ (hackers) • Builders – junior engineers • Hunters – junior analysts (next step would be ~~incident responders~~ but need more forensic skills)	• Yes – if practical component embedded (2 year option with significant 1 year internship). • Range of target markets – primarily a shorter study/learn on the job practical option for school leavers; mature re-trainers with practical IT experience