Cyber Security Staff – Attraction and Retention

The poor attraction and retention of cyber security staff is a strategic risk for which the likelihood of major operational impact will increase the longer these living and breathing mitigators against the exploitation of Australia's information assets remain undervalued. The key items affecting attraction and retention are training and remuneration.

A repeated view is that training opportunities should not be too expansive to mitigate the risk of staff movement to the private sector. This is a self-defeating concept, as if internally-trained staff don't exist, agencies will be required to approach industry to satisfy key operational requirements and mitigate core operational risks in any case. Denying opportunities for training is a tactical response to a strategic problem, though funding decreases have meant that this has been a less conscious decision in recent years: funds have simply not been made available to effectively facilitate industry-competitive qualifications.

The idea that decreased supply can somehow result in decreased demand defies the fundamental logic of economics and should be very consciously cast aside.

The trend of approaching industry to maintain operational momentum inflates prices over time, exacerbating the problem by encouraging more and more public service staff to leave to more competitively remunerate their skills and better enable their potential. It also increases the demand for marketable staff within industry to the current point where the need for accountable qualifications in the cyber security sector has been diminished to only requiring work experience, creating a circular vortex through which operational capability will eventually evaporate beyond the point of satisfying strategic intent.

The solution should be to increase the number of internally-trained and qualified staff. Freshly trained staff may in the short term still choose to move to private industry, but that trend can only be maintained if the demand for their skill sets remains steady, with high demand only maintainable through continued short supply. By increasing internal supply, the demand for external supply will diminish over time, reducing the extra amount skilled staff can earn within industry, and making that sector far riskier and ultimately less rewarding in the long term through its inability to maintain current demand.

A focused and indomitable commitment to mitigating the current skills shortage is needed to see the public service through the short-term effects of increased staff departures to get us to the point where a critical mass of internally-trained and qualified staff exist to effectively mitigate external demand.

A mitigator to the risk of both short-term staff departures and the lack of longer term retention is the enabling of a cyber security remuneration regime even remotely competitive with the private sector. As it is, private industry professionals in the cyber space receive at least double (highly conservative) the public service salaries for comparable work and qualifications, though with often markedly decreased organisational awareness and practical context for the work and strategic goals of their contracting organisations. This decreases throughput while increasing costs, all while devaluing – consciously or not – the public service staff needed to train an endless stream of new contractors while receiving far less remuneration for both their comparable work outputs and the coaching efforts needed to maintain operational momentum. This results in high APS turnover and provides an even greater incentive to move to the private sphere, creating a circular momentum that damages the public service's strategic capability to protect against cyber security exploits and defend against cyber security threats.

‘Capability building’ initiatives have been started in several organisations to offer increased remuneration to new staff to improve attraction and retention in key strategic areas, but the few private sector staff known to me who have attempted to enter the public service this way have not accepted the very limited extra pay offered. I have zero context for these initiatives being applied to current public sector staff, with the risk of diminished capability holding the highest chance of realisation through the failure to retain this staff set. Partial realisation of that same risk will have the greatest operational impact on these same individuals, increasing the risk of exodus to a more competitive – or at least accommodating – industry.

The greatest *strategic* impact will always be on Australia and its ability to ensure the continued availability and integrity of its information assets.

A return to something comparable to the previously-separate ‘Information Technology Officer’ employee levels may be called for to enable ongoing cyber security capabilities and to mitigate the risks they are increasingly needed to combat. For such a perpetually evolving industry, continual training would not just be an item of staff attraction and retention, but also strategically necessary to defend against a continually changing threat environment and the ever-evolving threat surface of Australia’s information assets.

Disclaimer

The above is my personal perspective, and does not reflect any view formally communicated by my employing public service organisation.

Dean Marden