# Uplifting and transforming Water Industry cyber security skills and awareness

The Australian Financial Review on the 19 of November 2021 highlighted the increasing pressure on cyber security nationally (refer attached). This pressure is coming from the increased availability of tradecraft, the increasing interconnectivity of devices and nation states. A key area of vulnerability is our people. It is estimated that over 66% of all successful cyber-attacks involve social engineering or compromise of our people. It is typically caused by a lack of knowledge and awareness by staff.

The Federal government has recently announced funding of $60 million to deliver innovation projects to improve the quality or availability of cyber security professionals in Australia. The Water Services Association of Australia, the NSW and Qld Water Directorates, VicWater, Internet of Things Alliance Australia together with Holmes Institute is looking to put in application for Federal government funding of between $250k to $500k to improve the training and awareness around cyber security.

In addition, this grant is targeted at increasing cyber security training for remote communities, women and indigenous participants. To this end we are seeking to have a number of fully or partially funded participants on scholarship able to do the course.

The commonwealth funding is for course development and delivery but requires matching funding. The proposal is that Homes Institute would develop and deliver a tailored and specially developed course for the water sector. The course would be developed in collaboration with key representatives from the sector to ensure it is relevant and well-constructed to meet our needs. It is intended that the commonwealth funds are used to develop the training course materials. The matching funding would be provided through the cost of attendees from water businesses doing the course. Effectively meaning the Federal government provides a 50% funding for the course.

A particular focus will be on the security of SCADA (Supervisory Control and Data Acquisition), operational technology (OT) and Internet of Things (IoT). A key aspect to consider is that the historical approach of using an air gap to separate different systems is becoming increasingly difficult to maintain as systems become more interconnected and staff come to rely more on mobile devices to manage systems remotely.

We are looking at providing three levels of training:

* **A general awareness course:** particularly aimed at educating field operators and remote workers on cybersecurity best practice. The focus is on protection of handheld and wearable devices, and systems connected through SCADA, OT and IoT devices (estimate 1d course with a cost of $1-2k per participant.).
* **A technical course (up-skill):** aimed at specialist IT and OT/SCADA staff who need to develop their knowledge of SCADA, IoT and OT cybersecurity. Focusing in on the risk and how it is managed from awareness, implementation and ongoing prevention aspects including procurement, installation and maintenance. The course would provide more general education on general cybersecurity best practice to better protect data and the organisations’ IT infrastructure. This would be an in depth online mixed content (some teacher lead and some self-led) course of approximately 5 days duration. Anticipated cost $3-5k per participant.
* **A senior management-oriented cybersecurity course:** aimed at executives and board members, so that they are aware of the cybersecurity risks posed by emerging smart technologies and how can their organisations be protected from a governance and risk perspective. This would be an online, face to face course in small group format of around 2 hours duration – estimated cost $500-$1k per participant).

To obtain commonwealth funding we require a non-binding commitment to from water businesses about their willingness to have staff attend this training. Whilst the commitment is not binding, we are seeking a conservative but reasonable estimate of potential numbers of staff that you would consider undertaking each course.

Could you please indicate if this of interest to your business and the approximate number of staff that you think would undertake each course.

|  |  |  |
| --- | --- | --- |
| **Course** | **Indicative number of participants** | **An estimate of the no of participants (if possible) that would be:** |
|  |  | **Women** | **Indigenous**  | **Regional and remote** |
| General Awareness |  |  |  |  |
| Technical up-skill |  |  |  |  |
| Senior management |  |  |  |  |

Would you be interested in funding one or more scholarships for women, indigenous or regional and remote workers in cyber security? If so, could you indicate how many?

Signed by authorised representative of the organisation.

Organisation Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Registered Address:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ABN:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_