CYBER RESILIENCE FOR SENIOR EXECUTIVES

Cyber security has become an essential skill for both our personal and professional lives, as many aspects of our daily activities now take place online.

Organisational cyber resilience is an entity's ability to continue to achieve objectives by adapting and evolving in response to volatility, turbulence and shocks. Shocks can be cyber attacks, malicious acts or significant changes in conditions.

This course is suitable for senior executives from any background and no technical knowledge is required.

OUTCOMES

At the end of this course, participants will be empowered to use the knowledge and skills gained to understand how to better lead their organisation's strategic response to the cyber security challenge and improve their organisational resilience.

- Have obtained knowledge of pragmatic and strategic approaches used by organisations to achieve resilience.
- Confidence in asking the right questions to understand how cyber security risk contributes to organisational cyber resilience
- Have gained essential personal skills in cyber security.

DETAILS

- **AUSCERT Members**: Our training courses are available exclusively to members only.
- **Delivery Mode:** In-person at the Atrium, UQ, 308 Queen St, Brisbane**.**
- **Price:** For the initial pilot offering, a discounted rate of $250 per person.

REQUIRED

No prior knowledge requied.

WHO WILL BENEFIT

- Board directors
- C-suite executives
- Senior executives
- Federal and state government SES
- New Chief Information Security Officers (CISOs)
- Newly promoted executives.

AUSCERT

APPROACH

- **Pedagogy**
  - Participant-centred, focusing on individual learning needs. An emphasis is on learner empowerment and the importance of collaboration.
- **Collaboration**
  - We intentionally create opportunities for participants to share experiences and knowledge. This course is designed to be informative, entertaining, and engaging, providing relevant and practical examples of cybersecurity threats and countermeasures that anyone can apply. It incorporates videos, quizzes, both large and small group discussions, and a scenario-based discussion exercise drawn from real-world situations.
- **Resources**
  - Information sources will be provided to continue participants' awareness of cyber security threats and countermeasures. Participants are encouraged to maintain contact with the facilitators post-course to ask questions related to course content.
- **Preparation**
  - Maximum participant return on investment will be gained by engaging in online pre-learning course activities (approximately 2 to 3 hours) before course delivery.