ENGINEERS
AUSTRALIA

Cyber Engineering Area of Practice

Cyber engineering involves the design, implementation, operation, maintenance, response and improvement of information security measures to protect the confidentiality, integrity, availability and safety (CIAS) of systems (including autonomous systems) and system security measures to assure the security of hardware, software, firmware and network components used to store, process, transmit, actuate and sense systems.

The cyber engineering workforce includes Professional Engineers, Engineering Technologists, and Engineering Associates whose role is to define requirements, analyse solution options design, develop, implement, maintain and monitor cyber solutions within intricate environments.

Cyber engineering includes:

- identifying systemic security issues based on the analysis of vulnerability, threat and secure configuration data.
- applying risk management and safety principles to identify constraints and trade-offs to determine and adapt system and/or product requirements.
- selecting and applying secure design tools, methods and techniques including automated systems analysis and design tools to design secure architectures using cyber and information security management systems knowledge and frameworks covering the entire system, including interconnected systems across the full life cycle of the system.
- performing security assurance activities such as specification and design of tests, including penetration tests, audit functions, security monitoring, resilience performance requirements and identifying, saving, protecting and storing information that will assist a cyber forensic investigation.
- conducting supply chain risk assessments associated with system components, interconnected systems (within the enterprise and systems to which the enterprise is connected) and implement supply chain management plans to minimise the risk of introducing vulnerabilities from third parties.
- applying incident response, disaster recovery and business continuity knowledge to design systems and processes to operate and maintain systems or products to continually protect confidentiality

Examples of a cyber engineer's work may include determining and assessing:

- requirements for designing, implementing, operating, and maintaining physical systems and assessing cyber risks that are posed by physical systems to the safety of people the environment and systems
- requirements for designing, implementing operating, and maintaining cyber security controls in existing systems or network environments where the effects and risks of implementation must be assessed against network capability, capacity and security
- requirements for designing, implementing and maintaining physical (e.g., biomedical devices, process control interfaces, network hardware, ICT, IoT) products that have networked interfaces where the engineer must ensure that appropriate security practices are developed and followed to ensure that the confidentiality, integrity, availability and safety of the product is not compromised
- cyber security and cyber worthiness of industry products by providing design control, governance, risk management, compliance and assurances.

Proficiency in the following practice elements are expected to demonstrate an individual's independent practice capabilities in this area of practice:

- Threat modelling and risk analysis
- Security models and standards
- Human factors
- Computer networking
- Security architectures
- Cyber laws and regulations
- System, data protection and cryptographic systems
- Advanced mathematical concepts
- Infrastructure security
- Authentication, authorisation and accountability
- Systems engineering
- Software engineering
- Cyber system design
- Supply chain management
- Business continuity and incident management
- Emerging technologies
- Vulnerability assessment and penetration testing

For more information related to this area of practice, refer to the *Cyber engineering practice guide*.

Professional Engineers typically work on complex engineering challenges within a broad discipline, Engineering Technologists typically work on broadly defined engineering challenges within a narrower engineering sub-discipline and Engineering Associates typically work on well-defined engineering challenges within a sub-discipline.

Cyber engineering is an area of practice for independent practice and available to those wishing to become Chartered. It is available to all occupational categories of Professional Engineer, Engineering Technologist and Engineering Associate.

How to apply

Visit our website to learn more about becoming Chartered and how to apply.

If you would like to know more about areas of practice and how to add cyber engineering as an additional area of practice, visit our website.

Registration eligibility

In the future, cyber engineers may need to hold statutory registration in an area of engineering in accordance with relevant legislation. Refer to respective state's registration information website for details.