I commenced my Master of Cyber Security at RMIT this year. My bachelor's degree was completed many years ago, and I have been working full time in the industry for over 18 years.

I am studying part time, which means the course will take approximately four years to complete. Balancing a full-time role as an IT Manager, part-time study, and family responsibilities is extremely challenging.

The application and acceptance process itself was straightforward. However, after reviewing all universities offering this degree, RMIT was the only institution that adequately covered the areas I want to learn and be formally accredited in—specifically the **Security Governance, Risk Management, and Compliance** stream. The remainder of the course at RMIT, as well as similar programs at other universities, is highly technical.

While I understand the importance of technical foundations, much of this content will not be directly applicable to my role once the course is completed. Unfortunately, there is currently no option to pursue a Cyber Security master's degree specifically tailored for senior management, executives, or Chief Security Officers. As a result, the program includes a large number of compulsory technical core units and a limited selection of relevant electives.

From an employment and career perspective, my industry experience allows me to clearly see the value of holding a master's qualification at this stage of my career. However, for local students without significant industry experience, there appears to be a misconception that completing this degree alone will lead directly to cyber security roles. In reality, breaking into the cyber security field without prior experience is extremely difficult.

While cyber security continues to be promoted as a high-growth industry, entry-level opportunities remain limited. The most viable pathway is through graduate programs, and even these opportunities are declining with the increasing adoption of AI and automation.