Cyber Breach Response Table Top Exercise

The defender's dilemma states that breaches occur because attackers only have to be right once, while defenders need to be right every time. Breach analysis shows that this is incorrect; attackers must successfully execute multiple stages in any intrusion, and defenders only need to break one step in this chain to prevent a breach. Availability bias affects our thinking in cyber security, with breaches making the news regularly, while successfully blocked attacks are rarely discussed.

Universities are challenging environments to apply preventive controls, but defenders can still retain an advantage by detecting preventive control failures early. This talk will discuss typical attack paths in higher education environments and show how a combination of prevention, detection, and response capabilities, combined with regular/automated control testing can reduce the likelihood and impact of a breach. Hear the experiences from the AARNet SOC in providing detection coverage for the higher education sector and sharing information to help prevent breaches.