

THE DISCIPLINE OF INFORMATION SYSTEMS AND TECHNOLOGY AT THE UNIVERSITY OF KWAZULU-NATAL
INVITES YOU TO A PUBLIC LECTURE BY



PROFESSOR GRANT ALAN PITMAN



President: Leaders Institute and Global Leadership Institute, Brisbane, Australia
Board Member: Research and Policy House, Brisbane, Australia



T H E M E

EXECUTIVES' PERSPECTIVES ON THE USE
OF ARTIFICIAL INTELLIGENCE TO ADDRESS
CYBER SECURITY RISKS

ABOUT THE SPEAKER

For 17 years, Professor Grant Pitman has been a professor, adjunct professor, adjunct associate professor and adjunct senior lecturer at the Queensland University of Technology, Griffith University, Leaders Institute and Global Leadership Institute in Criminal Justice, Public Policy, Accounting, Agribusiness and Arts. I have been an advisor to eight private and public university research and academic centres.

He has published and presented at national and international conferences and with publication companies over 50 articles in his academic field and public sector interests. He has supervised numerous PhD students and assessed 20 PhDs and Masters' theses.

He has held ministerial appointments on a TAFE Training College governance committees and regional roundtables.

Currently, he is the President and Professor of Leaders Institute and Global Leadership Institute; and a Director of Research and Policy House in Brisbane, Australia. These Institutes specialise in educating international students in masters' degrees including MBA, Agriculture, Informatics, food security, policing, counter terrorism, and cyber security leadership programs. The Research and Policy House is a research and publication centre specializing in cybersecurity leadership, higher and vocational education, police and governance and agriculture production and reforms.

His professional career was with the Queensland Police Service which spanned 40 years with 20 years as a senior commissioned officer in senior executive and management positions managing 1800 staff and \$200 million budgets and over \$1 billion in ICT projects. I have been a director or committee member of both national, state, and local government committees associated with public sector reforms, ICT, Road Safety, drug and mental health programs, counter terrorism, crime prevention programs and tertiary education and research.

THURSDAY,
17 AUGUST 2023

PLATFORM: ZOOM.
CLICK HERE TO REGISTER

10H00 – 11H30
(GMT+2, SAST)

ABOUT THE PUBLIC LECTURE

The key question is how can executives use AI tools to detect, contain, and respond to cyberthreat and develop strategies to create a more proactive security posture?

This Public Lecture will address how executives in both the private and public sectors can manage cyber security risks using artificial intelligence as a key strategy in their toolbox.

Deloitte's Tech Trends paper 2022 estimates that by 2025 the cost of cybercrime will climb to US\$10.5 billion and the average cost for a single data breach to an organization will be about US\$4.24 million in 2021.

The key areas to be addressed by organizational executives will be a proactive strategy to manage cyber risk regarding the data collected including their partners and workforce particularly homework place offices. The executive team will require the CEO, Risk, Finance, and ICT and security executives to better understand their organizational security posture, to strengthen defences using AI capabilities and whilst proactively managing the risks. The financial impact will be significant and will require funding for AI enhanced cyber defence systems and will have to be a key priority for the organizational board's consideration. Additionally, the organization will need to build capacity internally, as well as, partnering with cyber security specialists to address cyber security attacks in a timely manner. Education and training will be critical in this process. Of course, AI defences have their own vulnerabilities, and the landscape will continue to evolve. The critical issue for the executives of course will always be how they can protect their customers, their data and organization's reputation and brand.