Australian board directors urged to boost cybersecurity skills

September 27 2022

Credit: Pixabay/CC0 Public Domain

A University of Queensland study has identified a need to prioritize cybersecurity training for board directors, to better protect Australian organizations from cyber-attacks.

Dr. Ivano Bongiovanni from the UQ Business School said his research found board directors were not always sure about their duties and liability for cybersecurity, and often did not fully understand its importance.

"As the data breach at Optus this month demonstrates, no organization is immune to cyber-crime," Dr. Bongiovanni said.

"We interviewed non-executive directors of 43 organizations about cybersecurity; a lot of uncertainty emerged in terms of current best practices or industry guidelines for cybersecurity strategies.

"There is a misleading perception of cybersecurity being a purely technical topic and directors weren't engaged or confident talking about it.

"Considering the responsibility to oversee cyber risk management in modern organizations lies with their board of directors, an uplift of cyber-skills at the board level is necessary."

Cybersecurity failure is considered one of the top threats facing Australian businesses, and with customer information accessed in an attack on Optus, the Australian Cyber Security Centre is warning companies to remain alert.

Study co-author and UQ honors graduate Megan Gale said the potential impact of data breaches on Australian organizations was massive.

"A disruption to IT infrastructure could force a company to shut down, leading to financial loss or even more severe consequences," Ms. Gale said.

"In the Optus breach, sensitive, personal customer information along

with identity documents have been accessed, putting people at risk of being victims of fraud."

The researchers have called for clearer regulations and reporting practices and for cybersecurity training to be made a priority for all board directors.

"It's not just boards of large companies that need to be better equipped in this area," Ms. Gale said.

"Boards of small to medium-sized organizations across all sectors in Australia, including not-for-profits and community-run organizations, need to be vigilant."

Director of Cybersecurity at UQ and the Australian cyber emergency response team AusCERT, Dr. David Stockdale, said the study showed Australia has some work to do for boards to include cybersecurity in their enterprise risk management activities.

"As we've seen with Optus, cyber threats are a matter of 'not if, but when,' and organizations must be prepared," Dr. Stockdale said.

"More cyber risk training and regular communication between executives and their security teams will ensure the best course of action and prevention."

The study also involved Associate Professor Sergeja Slapnicar from the UQ Business School. Their research has been published in *Computers & Security*.

More information: Megan Gale et al, Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead, *Computers & Security* (2022). DOI: 10.1016/j.cose.2022.102840

Provided by University of Queensland