

The Human element of cyber risk = Unsur manusia risiko maya

Yoan Annisa Ravaie, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20479148&lokasi=lokal>

Abstrak

Laporan ini mengeksplorasi strategi mitigasi dan keberlanjutan yang digunakan untuk mengelola unsur manusia risiko cyber dan menyediakan analisis pendekatan manajemen saat ini dari Treasury Corporation of Victoria TCV . Risiko cyber adalah risiko bisnis yang berevolusi dengan cepat yang memiliki potensi untuk memengaruhi organisasi secara signifikan¹. Sebagai otoritas keuangan pusat untuk Negara Bagian Victoria, TCV sangat sadar akan potensi dampak serangan cyber dan karena itu bersemangat untuk mengembangkan pendekatan menyeluruh terhadap manajemen risiko cyber di luar sistem teknis mereka. Kombinasi penelitian primer dan sekunder digunakan untuk mengembangkan 39;Model Penentuan Risiko Maya 39; CRP yang mempertimbangkan elemen manusia risiko cyber sebagai kombinasi dari tiga parameter yang berbeda: pengetahuan, akses, dan perilaku. Model ini dikembangkan untuk membingkai penelitian tambahan kami dan menyediakan TCV dengan sarana menilai risiko manusia-cyber. Selain itu, laporan ini mengusulkan metode menganalisis dan mengukur setiap parameter untuk mengidentifikasi kelemahan potensial. Berdasarkan model CRP, tiga strategi mitigasi kunci diperiksa dan dievaluasi berdasarkan penelitian primer dan sekunder yang ekstensif: 1. Pendidikan: frekuensi dan struktur program pendidikan 2. Kebijakan: presentasi dan keterbacaan. 3. Komunikasi: prasyarat penting untuk komunikasi yang efektif.This report explores mitigation and sustainability strategies used to manage the human element of cyber-risk and provides an analysis of the Treasury Corporation of Victoria TCV rsquo;s current management approach. Cyber-risk is a fast-evolving business risk which has the potential to significantly impact an organisation¹. As the central financing authority for the State of Victoria, TCV is highly aware of the potential impacts of a cyber-attack and is therefore eager to develop a firm-wide approach to cyber-risk management beyond their technical systems.A combination of primary and secondary research was used to develop a lsquo;Cyber-Risk Profiling Model rsquo; CRP which considers the human element of cyber-risk as a combination of three distinct parameters: knowledge, access and behaviour. The model was developed to both frame our additional research and provide TCV with a means of assessing human-cyber-risk. Additionally, the report proposes methods of analysing and measuring each parameter to identify potential weaknesses.Based on the CRP model, three key mitigation strategies are examined and evaluated drawing on extensive primary and secondary research:1. Education: frequency and structure of education programs2. Policy: presentation and readability.3. Communication: essential preconditions to effective communication