# Information Security in the era of Artificial General Intelligence (AGI)

Martin Kang
College of Business,
Loyola Marymount University
Martin.Kang@lmu.edu

Anat Hovav
School of Business
Korea University
anatzh@korea.ac.kr

## 1. Introduction

The goal of this mini-track is to explore how Artificial Intelligence (AI) and Machine Learning (ML) can enhance Cybersecurity (ISEC), including improving fraud detection and optimizing security policies using AI methods.

In recent years, there has been an increased interest in ICT literature at the intersection of AI and ISEC. AI is viewed as a mechanism to achieve organizational outcomes, while ISEC is the desired outcome. However, research at the intersection of these fields has been limited.

In the business and research communities, there is a growing exploration of how AI and ML can be applied to ISEC technologies like anti-malware, firewalls, and intrusion detection systems. There is a need for improvement in both the algorithms and their organizational implications, addressing issues such as errors and considering work processes and user behavior.

The one paper selected for presentation at our mini-track of HICSS 2023 is titled "CISO-BERT: Matching Information Security Requirements by Fine-Tuning the BERT Language Model." This paper utilizes Google's BERT model to assess information security requirements from ISO 27001. This paper introduces the CISO-BERT approach, which involves fine-tuning a pre-trained BERT language model to identify similar cybersecurity requirements within ISO 27001. The results indicate that CISO-BERT outperforms baseline models, offering an innovative method for determining organizational compliance with ISO 27001 requirements using machine learning.

The paper has received positive assessments from three reviewers, highlighting its potential for publication. The CISO-BERT model aligns information security requirements with organizational needs, leveraging Google's BERT model fine-tuned on ISO 27001 and demonstrating enhanced performance compared to existing baseline models. The model's meticulous training on both general and industry-specific security policy frameworks shows promise, with initial evaluations offering a superior performance compared to existing baseline models.

We believe that the paper is expected to present a significant contribution to ISEC research by offering valuable methodological contributions that can be instrumental in ensuring compliance with information security requirements and policies at both the system and organizational levels. This topic can have the potential to enhance the field of ISEC by providing more effective tools and methods for overcoming the 'one-size-fits-all' approach to security needs within organizations.

URI: https://hdl.handle.net/10125/106544
978-0-9981331-7-1