Hamid Jahankhani

Gordon Bowen
Mhd Saeed Sharif
Osama Hussien *Editors*

Cybersecurity and Artificial Intelligence

Transformational Strategies and Disruptive Innovation

Springer

Advanced Sciences and Technologies for Security Applications

Indexed by SCOPUS

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

Hamid Jahankhani · Gordon Bowen ·
Mhd Saeed Sharif · Osama Hussien
Editors

Cybersecurity and Artificial Intelligence

Transformational Strategies and Disruptive Innovation

Springer

Editors
Hamid Jahankhani
Northumbria University London
London, UK

Gordon Bowen
School of Business and Law
Anglia Ruskin University
Chelmsford, Essex, UK

Mhd Saeed Sharif
and Engineering
University of East London
London, UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-031-52271-0 ISBN 978-3-031-52272-7 (eBook)
https://doi.org/10.1007/978-3-031-52272-7

Contents

Impact of Artificial Intelligence on Enterprise Information Security Management in the Context of ISO 27001 and 27002: A Tertiary Systematic Review and Comparative Analysis

Heiko Kreutz and Hamid Jahankhani

Abstract The use of Artificial Intelligence (AI) by enterprises has dramatically increased over the last decade and is estimated to accelerate further. This research aimed to identify, which impact AI will have on enterprise information security and how to address this in the context of the widely used security standards ISO 27001 and 27002. Guided by AI security aspects relating to AI enhanced cyber attacks, AI enhanced cyber defences, attacks against AI systems, AI malfunctions and AI human and societal impact, combined with the context of governance and regulations and additional dimensions of risk management and quantum computing, a systematic literature review was conducted to find current AI security challenges and defences, which were then comparatively analysed with ISO 27001/27002 controls. The results of this analysis confirmed, that existing ISO 27001 ISMS and security controls were not sufficient to address the emerging AI security challenges. To improve this lack of adequate security controls, six new security controls and ten modified existing security controls were proposed.

Keywords AI · ISO 27001 · ISMS · Artificial Intelligence · Risk · Machine learning · Cyber attack

1 Introduction

AI, which in lieu of a more precise definition, may be described as a computer system with the ability to accomplish tasks typically considered requiring some level of human-like intelligence [1], is a wide term used to describe a number of different technologies. Including Machine Learning (ML), which can be either classical shallow ML or, when based on Neural Networks (NN), Deep Learning (DL).

H. Kreutz · H. Jahankhani (✉)
Northumbria University London, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Cybersecurity and Artificial Intelligence*, Advanced Sciences and Tec
https://c

Both classical ML and DL can learn either in the form of supervised, unsupervised or reinforcement learning (RL), or a combination thereof.

When approaching AI and its security impact, one can note, that the topic AI has become a matter of intense public debate in recent years, which may follow a hype cycle pattern of boom and bust over time [2, 3] and which may reduce business

hype and instead should follow an approach based of assessing benefits and risks and conducting appropriate risk management [5] in accordance with the organisation's chosen risk appetite. This research intends to illuminate, which modifications may be needed for EISM to maintain its relevance and effectiveness in the future and where new measures and controls could be beneficial to enterprises.

The research hypothesis is, that the use of AI by threat actors for cyber attacks will likely increase the security risks for enterprises. Additionally, the use of AI by enterprises themselves will likely introduce new security challenges. Therefore, enterprises may need to upgrade how they manage information security.

2 Literature Review

2.1 Enterprise Information Security Management

It is a widely accepted requirement for enterprises to conduct risk assessment and management (RAM) and implement corporate governance as part of their businesses, which is for example included in the UK Corporate Governance Code [6]. Many enterprises follow a similar approach to managing information security, which is based on RAM, embedded in appropriate governance [7]. Over the years a number of different national and international standards and frameworks have been developed to support enterprises in their information security management, including for example the prescriptive SP 800-53 [8], which mandates security and privacy controls for US government organisations, the Cybersecurity Framework [9], which describes cybersecurity functions to protect critical infrastructure, and COBIT [10], a framework for enterprise IT governance and management, also applicable in the context of risk and security. Further internationally recognised standards for enterprises, albeit with some uncertainty around growth of adoption rates [11], are ISO 27001 [12], describing how to setup, manage and maintain an information security management system (ISMS), and ISO 27002 [13], describing the approach to implementing, managing and maintaining security controls. The latest versions of these two standards have been published in 2022 and 2023, requiring enterprises with ISO 27001 certifications to adapt their information security management to these new editions within the next years to maintain their certification status [14]. The latest versions of these standards contain a number of new controls [15], catering to some emerging technologies, like cloud services, and evolving cybersecurity requirements, like threat intelligence and the cybersecurity functions [16].

However, one area where ISO 27001 and 27002 fall short is AI. AI and ML are only mentioned once by ISO 27002 in the context of their potential use for security monitoring.

2.2 AI Security Aspects

Kaloudi and Li [17] mapped in their survey AI enhanced cyber attacks to the Cyber Kill Chain (CKC) [18], a widely used model describing the stages of cyber attacks in their temporal and logical progression, and developed on that basis a new AI enhanced cyber attack framework with three attack phases: planning, intrusion and execution. For each of the phases relevant attack objectives, attack impact and proposed defences were analysed. Resulting insights included the potential of AI to improve speed and scale of cyber attacks, but also to improve scope, including more diverse, complex and accurately targeted attacks. Kaloudi and Li recommended the use of AI for cyber defence as only viable response to the threat of AI enhanced cyber attacks. Guembe et al. [19] followed a similar path in their SLR, using a modified CKC, where the 2nd stage, normally the weaponization stage, was replaced by access and penetration stage, allowing an increased variety of attack techniques to be included. The findings confirmed results and recommendations from Kaloudi and Li. In general, while both studies investigated AI enhanced cyber attacks, they narrowly focused on external threat actors only, excluding both insider threats and AI malfunctions.

Mirsky et al. [20] differ in their review from the previously discussed studies by mapping offensive AI enhanced cyber attack capabilities to the MITRE ATT&CK Enterprise Matrix (MAEM) [21]. The study identified 32 AI enhanced cyber attack capabilities, which were organised in 7 categories. Employing MAEM for this mapping allowed the inclusion of techniques, tactics and procedures typically employed by malicious insiders, for example the capability to evade insider detection, which was included in the category stealth. The findings included the aim of attackers to use AI to improve scale and precision of attacks through automation and to increase speed and success rate of the attacks. AI enhanced cyber attacks may also add new threats compared to traditional attacks, by developing new ways of exploiting vulnerabilities. Furthermore, the study identified possibilities to use defensive AI methods for malicious purposes. This means, that also risks associated with the use of AI enhanced cyber defences should be addressed in this research. Mirsky et al. predicted, that AI enhanced cyber attacks will likely increase in the near future, mostly in early and late attack stages, which will likely persist due to lack of AI capabilities to conduct attacks through all attack stages fully autonomously. Overall, the study predicted that enterprises will be forced to use AI enhanced cyber defences, but recommends that corresponding security aspects for AI enhanced cyber defence should be addressed.