Combating Cyber Criminals with the EU AI Act: Unveiling the Power of Regulation in GRC Market

Written: 23 October 2023

Sean Much, Co-CEO/CFO, AI & Partners, s.musch@ai-and-partners.com, +31(6)572 85579, Sean has an extensive background in the entertainment industry (e.g., film and art), and has a specialism in design. Alongside this, Sean has more than a decade of experience in the professional services sector, including holding the position of a tech accountant for 5 years. Sean knows about auditing and has helped with an IPO on the New York stock exchange. As well as being a compliance expert, he has deep expertise in implementation aspects of audit & assurance engagements and has been working with the largest global tech MNEs over the past 5 years.

Michael Charles Borrelli, Co-CEO/COO, AI & Partners, m.borrelli@ai-and-partners.com, +44(0)7535 994 132, Michael Charles Borrelli is a highly experienced financial services professional with over 10 years of experience. He has held executive positions in compliance, regulation, management consulting and operations for institutional financial services firms, consulted for FCA-regulated firms on strategic planning, regulatory compliance, and operational efficiency. In 2020, Michael set-up the operations model and infrastructure for a crypto asset exchange provider and has been actively engaged in the Web 3.0 and AI communities over the last 4 years. He currently advises a host of AI, Web3, DLT and FinTech companies.

Christopher Allix, Managing Partner, Temple Avenue Group, Christopher.allix@templeavenuegroup.com, Christopher is a Transformational business leader providing strategic advisory support to executives, coupled with hands-on delivery with operational teams. Over the past 20 years has supported a number of leading global brands, hypergrowth companies and mature organisations to transform. Accordingly, Temple Avenue Group was founded to help service organisations optimise their transformation, drawing on our expertise in Digital Transformation, Cyber Management Response, Strategic Change, and Delivery.

Combating Cyber Criminals with the EU AI Act: Unveiling the Power of Regulation in GRC Market

Introduction

The proliferation of artificial intelligence ("AI") has ushered in a new era of concern for cyber threats. Is AI a friend or foe to the cybersecurity space? This article delves into the emerging challenges posed by cybercriminals who harness the capabilities of AI for nefarious activities, all while considering the prospective impact of the European Union ("EU") AI Act (the "EU AI Act" or "Act") on this evolving landscape. The governance, risk, and compliance ("GRC") market practitioners' sphere of operations faces an increasingly complex and potent adversary in the form of AI-augmented cybercrime. This investigation scrutinises the fusion of AI and cybercrime, outlining the fundamental concerns, and subsequently, the regulatory dimensions that the EU AI Act presents as a viable solution to address these formidable challenges.

AI Cyber Security Rhetoric versus the Reality

The attention-grabbing headlines are designed to make us believe that AI will introduce an all-powerful and unstoppable enemy like none-before and replace all cybersecurity jobs. Is this really the case, and what problems and opportunities may AI pose for the cybersecurity realm?

AI will replace all Cybersecurity jobs – Myth

Talk to anyone in the cybersecurity field, and you'll learn about the skills shortage. With the rapid growth of the digital world, this isn't just a local issue; it's a global one. Furthermore, the world economic forum predict that Cybersecurity will be one of the biggest drivers of jobs growth over the next 5 years. So, our view is clear AI will augment the work of cybersecurity professionals rather than replace them and help bridge the skills gap. Better still, AI automates routine tasks, detects threats more quickly, and handles large volumes of data, allowing human resources to focus on more complex aspects of cybersecurity.

AI will advance cyber criminals – Fact but it also advances cybersecurity defences

AI's integration into cybercrime is evident in the automation of phishing and malware distribution. Through AI, cybercriminals can accelerate malicious email and malware deployment, increasing the scale and efficiency of their attacks. This automation reduces labour and diversifies attack vectors, making it harder for conventional security measures to keep pace.

Polymorphic malware, enabled by AI, can morph and obfuscate its code continually, rendering signature-based detection methods largely ineffective. This requires advanced AI-based defences such as the use of heuristic analysis to identify suspicious or risky behaviour, even when specific signature or patterns are not known.

In phishing attacks (one of the most common and successful forms of cyber-attacks), cybercriminals exploit AI to eliminate easily detected signs like poor language. They're also using AI for highly personalised 'spear-phishing' messages, utilising social engineering and publicly available information to create convincing personalised messages. Consequently, making it harder for victims to discern the fraudulent nature of these communications.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://www.linkedin.com/company/ai-&-partners/

Temple Avenue Group Service Business Consulting
christopher.allix@templeavenuegroup.com
https://templeavenuegroup.com/
https://www.linkedin.com/company/temple-avenue-group/

Conversely, cybersecurity specialists are leveraging AI to undertake pattern recognition, anomaly detection, and content & behavioural analysis making it more difficult for basic phishing attacks to succeed. All-in underscoring the need for improved defences in this cat-and-mouse game between cybercriminals and cybersecurity practitioners.

So is AI better for the Good guys or the Bad guys – Jury's out

The definitive answer to this question remains uncertain. Our current view is that AI benefits cybersecurity professionals more than it aids cybercriminals and has already had a demonstrable impact on the industry. AI is helping cyber security specialists to stay a step ahead in the fight of cybercrime – but to optimise this position it is imperative for a principled set of AI rules to be followed.

In light of these advancements in AI-augmented cybercrime, and the development in AI supported cyber security, the GRC market must adopt a proactive stance to mitigate the risks posed by such malevolent innovation, and optimise the opportunities. This starts with the need to continuously evolve their defences, including incorporating AI-driven security tools and monitoring for signs of AI-driven attacks. Additionally, regulations and policies may be needed to control the use of AI in certain contexts to protect against malicious activities.

The impending implementation of the EU AI Act offers a ray of hope by providing a regulatory framework aimed at curbing these AI-driven threats and ensuring the security and integrity of digital ecosystems

The EU AI Act – An Overview

The EU AI Act, a pivotal regulatory framework, endeavours to tackle the multifaceted challenges posed by AI-driven cybercrime. At its core, this legislative initiative embarks on a mission to establish unequivocal rules governing AI development and deployment. These rules are meticulously designed to instil a sense of order and responsibility in the ever-evolving realm of AI technologies.

Moreover, the Act places a profound emphasis on transparency, accountability, and the ethical utilisation of AI. By doing so, it aims to ensure that AI technologies operate within the bounds of ethical and legal standards, thereby averting their misuse in the hands of cybercriminals. The Act underscores the significance of adhering to strict ethical guidelines, assuring that the potential for AI to perpetuate harm remains constrained.

In its pursuit of fostering trust and security in AI technologies, the Act ushers in a notable transformation. By promoting a culture of trustworthiness and upholding the security of AI applications, the Act offers a resolute response to the threats posed by AI-empowered cybercriminals. Consequently, the Act stands as a beacon of hope for the governance, risk, and compliance market, furnishing a comprehensive and structured approach to address the intricate challenges that emerge from the malevolent fusion of AI and cybercrime.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://www.linkedin.com/company/ai-&-partners/

Temple Avenue Group Service Business Consulting
christopher.allix@templeavenuegroup.com
https://templeavenuegroup.com/
https://www.linkedin.com/company/temple-avenue-group/

Combating Cyber Criminals with the EU AI Act: Unveiling the Power of Regulation in GRC Market

AI Regulation and Cybersecurity

The EU AI Act presents a significant step forward in addressing the challenges posed by cybercriminals who wield AI as their weapon of choice. This legislative framework stands poised to enforce crucial cybersecurity measures by virtue of its key provisions.

One of the Act's potential contributions to the cybersecurity domain is the establishment of mandatory cybersecurity assessments for AI systems. These assessments would serve as a pivotal checkpoint, ensuring that AI systems meet rigorous security standards. By incorporating stringent evaluation processes, the Act seeks to curb vulnerabilities and weaknesses that cybercriminals might exploit.

Furthermore, the Act imposes explicit requirements for data security within AI systems, especially when they process sensitive information. This imperative ensures that personal and confidential data remains shielded from potential breaches, thus minimising the potential for malicious exploitation.

Promoting transparency and accountability emerges as an essential component of the EU AI Act. This emphasis is not merely a regulatory formality but a strategic move to fortify cybersecurity. Transparent AI operations facilitate a clear understanding of system capabilities and limitations, empowering cybersecurity professionals to pre-emptively address vulnerabilities. Accountability, too, serves as a deterrent to nefarious AI deployment, holding actors responsible for their actions.

This messaging works in tandem with existing legislation and requirements such as the need for organisations to have an Incident response plan for the preparation and mitigation of data breaches as required by the European General Data Protection Regulation (GDPR).

In the world of GRC market practitioners, these provisions lay a foundational framework for bolstering cybersecurity resilience and readiness in the face of the AI-augmented threat landscape, paving the way for a more secure digital ecosystem

Ethical AI and Cybersecurity

The EU AI Act underscores its pivotal role in addressing ethical dimensions of AI and their profound implications for cybersecurity. This legislative framework embarks on the essential mission of combating biases, discrimination, and profiling ingrained in AI systems, recognizing that these ethical shortcomings pose inherent risks in the cybersecurity landscape. The Act acknowledges the importance of fairness and justice in AI-powered cybersecurity measures. It seeks to rectify imbalances within AI algorithms, fostering a more equitable digital realm. The Act's commitment to ethical AI underpins its broader objective of upholding cybersecurity ethics.

By imposing regulatory guidelines and standards, the EU AI Act is poised to prevent AI from being misused for illicit purposes. This proactive stance serves as a deterrent to the malevolent utilization of AI in cybercrime, ensuring that the technology is employed for legitimate and constructive purposes. The Act acts as a sentinel, striving to strike a balance between technological innovation and the ethical considerations vital in AI-powered cybersecurity, ultimately fostering a more secure and equitable digital ecosystem for all stakeholders in the GRC market.

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://www.linkedin.com/company/ai-&-partners/

Temple Avenue Group Service Business Consulting
christopher.allix@templeavenuegroup.com
https://templeavenuegroup.com/
https://www.linkedin.com/company/temple-avenue-group/

Compliance and the GRC Market

GRC professionals operating within the contemporary landscape must harmonise their strategies with the burgeoning regulatory framework embodied by the EU AI Act. Aligning their practices with the Act's stipulations is not merely a compliance exercise; it's a strategic imperative.

Compliance with the Act serves as an essential mechanism for maintaining trust and reputation in the GRC market. Adherence to the regulatory requirements conveys a commitment to ethical and secure AI practices, bolstering confidence among clients and stakeholders.

Furthermore, the Act's implications reverberate into risk assessment and governance strategies within the GRC market. It mandates an elevated vigilance against AI-driven cyber threats, necessitating an evolution in risk assessment methodologies. GRC professionals must navigate this transformative landscape with an acute awareness of the regulatory environment, underlining the pivotal role that the EU AI Act plays in shaping the future of the GRC sector.

Conclusion

In conclusion, the EU AI Act is poised to be a linchpin in the fight against cybercriminals who harness AI for illicit activities. Its comprehensive provisions, emphasising ethics, transparency, and security, offer the GRC market practitioners a crucial framework to safeguard against evolving threats in an AI-driven landscape.

Sources

World Economic Forum (WEF), (2023), 'Future of Jobs Report 2023 | Insight Report | May 2023', accessible at https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf (last accessed 22 October 2023)