Mitigating cyber-security risks is a prerequisite for releasing AI's potential for businesses

May 2024

Adam Salač

Despite groundbreaking progress over the past two years, AI is still in its very early stages, and few technologies have yet managed to reach their widely predicted potential. Nonetheless, even at its current nascent stage, AI is already transforming enterprise productivity and paving the way for innovative business practices. The hype and optimism around AI are tempered by the risks associated with its implementation. Companies are facing difficult decisions regarding AI adoption, particularly concerning security and regulatory compliance.

What challenges lie ahead?

Decision-makers may feel they are walking a tightrope: excessive caution means a high risk of falling behind competition; insufficient caution could lead to disastrous outcomes. The impact of losing ground to competitors is clear. The risks posed by a laissez-faire approach to AI are more varied and complicated, and include:

- **Data protection:** Many publicly available language learning models (LLMs) such as ChatGPT have a permissive privacy policy and will store and use user input for further training of the AI model, potentially leading to public disclosure of sensitive corporate information. Even on-premises AI systems may be used in a manner that could lead to the disclosure of information to unauthorised personnel.

- **Regulatory compliance:** Given the novel nature of AI, many pieces of regulation specifically targeting AI systems – the EU AI Act is a leading example – are yet to take effect. Even so, companies need to prepare for adherence to these regulations, as well as existing regulatory frameworks such as the Network and Information Systems Directive 2 (NIS2) and General Data Protection Regulation (GDPR).

- **Governance:** Companies lacking clear accountability and policies (for example, acceptable use policy) face distinct risks in the AI context. Public cloud-based LLMs involve different challenges compared to on-premises LLMs, requiring tailored policies to address their unique threats.

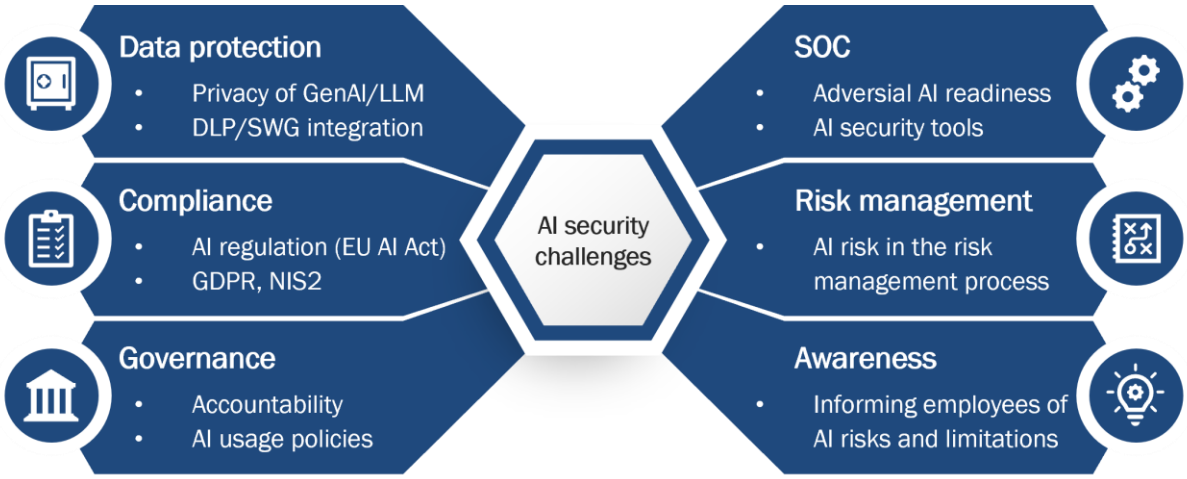
- **Security operations centre (SOC):** Companies using or exposing LLM interfaces will need a specialist function that manages and responds to cyber-security threats. Ensuring operational readiness of the SOC function is key, given that the vast potential of AI is being used not just by businesses, but also by potential intruders and hackers (adversarial AI). Larger players need to establish or enhance their own SOCs, whereas smaller entities may use cloud suppliers that have their own SOC function.

- **Risk management:** Existing risk management processes are unlikely to cover the full scope of AI-induced risk, such as the security of AI-generated code in software development. Companies must therefore adapt all elements of their risk management process to cover these threats.

- **Awareness:** Employees may not be fully aware of the security implications and limitations of AI systems. Companies must therefore engage proactively in training to ensure employee awareness of AI-related risks.

Figure 1 provides an overview of the various domains of cyber security, which are facing new challenges due to the emergence of AI.

Figure 1: AI cyber-security challenge dimensions



Source: Analysys Mason

Businesses can realise the potential of AI while mitigating the risks it poses

Achieving the right balance of risk is critical to the successful and safe implementation of AI. Businesses need to be aware of any and all regulations and guidance applicable in their regions of operation.

In the USA, the cyber-security frameworks published by the National Institute of Standards and Technology (NIST) from the US Department of Commerce are omnipresent throughout all domains of cyber-security. NIST's approach does not solely consider the IT security of AI systems, but also caters for other associated risks such as the bias and accountability of AI systems. Since 2023, NIST has been providing organisations with the AI Risk Management Framework (RMF), a framework to help manage AI risks. The RMF targets the mapping, governance and management of AI-linked risks.

In the EU, the approaching implementation of the AI Act means enterprises will have to adhere to AI-relevant International Organization for Standardization (ISO) standards such as ISO 23894 and ISO 42001.

However, to be fully prepared for AI implementation, businesses need to move beyond baseline compliance with regulation: minimising risk means rethinking and adapting all aspects of cyber-security frameworks, from awareness to security operations. Businesses need carefully integrated security solutions, including secure web gateways (SWG), data loss prevention (DLP) security information and event management (SIEM) to address AI-related risks. By controlling these risks, organisations will give themselves the freedom to exploit the opportunities and advantages that AI offers.

About us

Analysys Mason has a proven track record of providing policy and regulatory advice to clients across the telecoms, media and technology (TMT) sector. Our *Transformation* practice has been helping clients to understand and react to the known and emerging AI risks, and to set up processes and policies that help a business to gain the right balance between the risks and opportunities that AI presents.