

The road to success when implementing AI

MARC PEISER

Daemon

Abstract: Everyone's talking about artificial intelligence and many organisations are adopting it in one form or another in the hope of reaping business advantages, finding new opportunities or just out of a fear of missing out. Yet how confident are these organisations that their AI efforts will result in the benefits they seek? And is there a smarter way to go about this?

AI has proven to be a clear favourite for businesses working to level up all facets of their operations. Recent research into businesses' attitudes towards digital transformation found that 99% of organisations are looking to use artificial intelligence (AI) or machine learning (ML) to seize new opportunities.¹

Appetite is particularly strong in the retail, distribution and transport sector, where 97% of organisations report either 'some' or 'significant' adoption of AI. Further to this, 98% of organisations have some vision for the use of AI and the majority are planning to implement it within the next six months.

However, despite these encouraging statistics on AI adoption, 49% of senior decision-makers have low confidence in its implementation.

This statistic may raise concerns for security leaders and induce hesitancy around their company's implementation strategy. However, I believe this is an opportunity to increase cross-organisation collaboration and work together to build the right AI implementation strategy that eases low confidence. So, how do we do this? Here are my top three tips for security leaders to consider on the journey to successfully implementing AI.

Cross-business strategy

Undergoing 'AI transformation' across an organisation is a formidable task, and mapping out the implementation strategy should not be decided in siloes. In fact, the research shows that 13% of senior decision-makers have low confidence in AI and ML technology because they don't have a clear strategy. Alignment is critical and security leaders need to establish clear lines of communication, and collaborate with key stakeholders to ensure everyone is clear on the approach.

Alongside broader stakeholder engagement, it is also important that cyber security and AI teams work closely together to further refine the strategy. Early involvement and collaboration from both teams ensures that security considerations can be integrated into the development lifecycle, and that any AI security is ingrained into the broader cyber security strategy of the organisation.

By bringing everyone together, you can facilitate knowledge sharing and ensure that all considerations have been discussed early in the process.

Vet existing security protocols

If the business is already using third-party AI solutions or services, security leaders should conduct a thorough vendor security assessment. Check adherence to robust security practices by evaluating third parties' security controls, data protection measures and overall cyber security protocols. Establish clear expectations regarding security standards, and you can even consider incorporating contractual agreements that prioritise the security of the AI solutions provided.

This diligence is essential in order to mitigate potential risks associated with external AI partnerships and safeguard the organisation's overall security ecosystem.

Ongoing training for all employees

Employees are the first line of defence and often businesses can underestimate the role of human error, causing them to provide inadequate training for employees. Once the rollout strategy for AI has been identified, ensure that employees don't become a reason for increased vulnerabilities across the organisation. The research indicates that 24% of senior decision-makers have low

confidence in AI/ML because they don't have the right skill level. Training will be vital for alleviating this concern.

Training must go beyond cyber security professionals and the IT department and should be ongoing, as use cases and solutions for AI continue to evolve. I recommend taking a multi-layered approach to training for all employees. For example, cyber security professionals should be provided with additional training to stay informed about evolving regulations related to AI and ensure that your organisation complies with them.

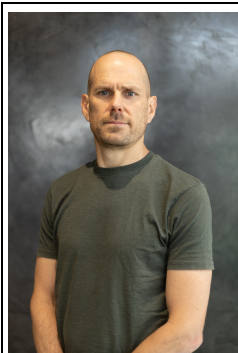
AI-specific teams should also be trained on AI development and deployment security best practices. This includes awareness of social engineering attacks and the importance of secure coding. You can also provide security training and awareness programmes for all employees, to ensure that they are aware of security best practice and potential risks associated with AI technologies.

Imagining a digital future

While strong economic headwinds have resulted in organisations accelerating their spending on digital transformation, AI has forced organisations to reimagine a digital future beyond the confines of current ways of working. AI is no longer a non-tangible technology that will come to fruition in a few years, it is here now, and organisations are racing to adopt and reap the benefits it can bring.

As you consider your implementation strategy, I urge security leaders to play an instrumental role in the development of this plan and ensure collaboration across an organisation to ensure success for years to come.

Figure: Marc Peiser, Daemon



About the author

Marc Peiser is a principal cloud consultant at digital transformation consultancy Daemon. He is a solution-oriented cloud infrastructure engineer with several years of diverse career experience in systems architecture, implementation and management. He has more than 10 years' experience in the cyber defence and security field.

References:

1. 'Is AI a craze or crucial: what are businesses really doing about AI?'. Daemon. Accessed Mar 2024. www.dae.mn/hubfs/Is%20AI%20a%20craze%20or%20crucial%20-%20What%20are%20businesses%20really%20doing%20about%20AI.pdf.