Cybersecurity and AI:
Threats and Opportunities

AI has captured the imagination of people and organizations around the world. However, alongside its advancements, AI brings forth a myriad of security challenges that cannot be ignored.

AI as a tool for cybercriminals

As AI systems become increasingly sophisticated and pervasive, cybercriminals are harnessing its power to launch more sophisticated and targeted attacks.

For example, **phishing emails** have evolved from simple deceptive emails to ones that have become more advanced, harder to spot and significantly more dangerous. Attackers are also successful at using methods like **deepfakes** — a form of AI that can be used to create convincing hoax images, sounds and videos — to perpetrate fraud or manipulate an audience into action.

And AI's adaptive nature is one of its most potent features in **social engineering attacks**, which manipulate people into giving away sensitive information or compromising security.

By using AI in these attacks, cybercriminals can appear more credible and trustworthy, leading more victims to fall for fraud attempts or manipulation, which could lead to system compromise.

40% of all **phishing emails** targeting businesses are now generated by AI according to VIPRE Security Group.

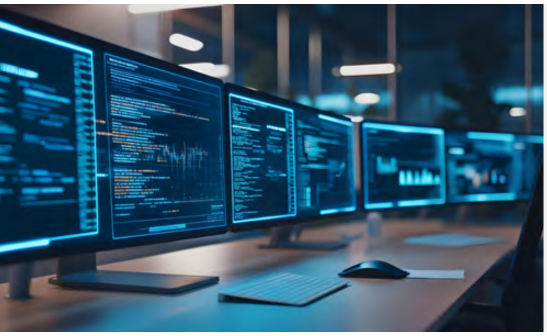
Empowering defenders at the speed of AI

At its heart, AI recognizes patterns and abnormalities in massive datasets — that is why it is such an important component of modern cybersecurity.

For example, AI enhances threat detection through advanced pattern recognition and anomaly detection. Unlike traditional methods, AI can analyze vast amounts of data in real time, identifying threats that might be missed by human analysts. This leads to faster incident response times and reduces the window of opportunity for cybercriminals.

AI also enables predictive analytics, allowing businesses to anticipate and mitigate potential threats before they materialize. By analyzing historical data and identifying trends, AI systems can provide insights into future attack vectors, enabling proactive defense strategies.

For example, DXC is working with Microsoft product teams to help shape **Microsoft Security Copilot**: a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes.



44% of organizations can confidently identify ways AI could **strengthen their security systems** (Ponemon Institute).

AI as a force multiplier

As organizations confront the complexities of escalating cyber threats, they need people with the right skills to protect their data and systems.

The good news is AI can work as a force multiplier for smaller security teams, which gives organizations a better chance against the newest strains of cyber risk.

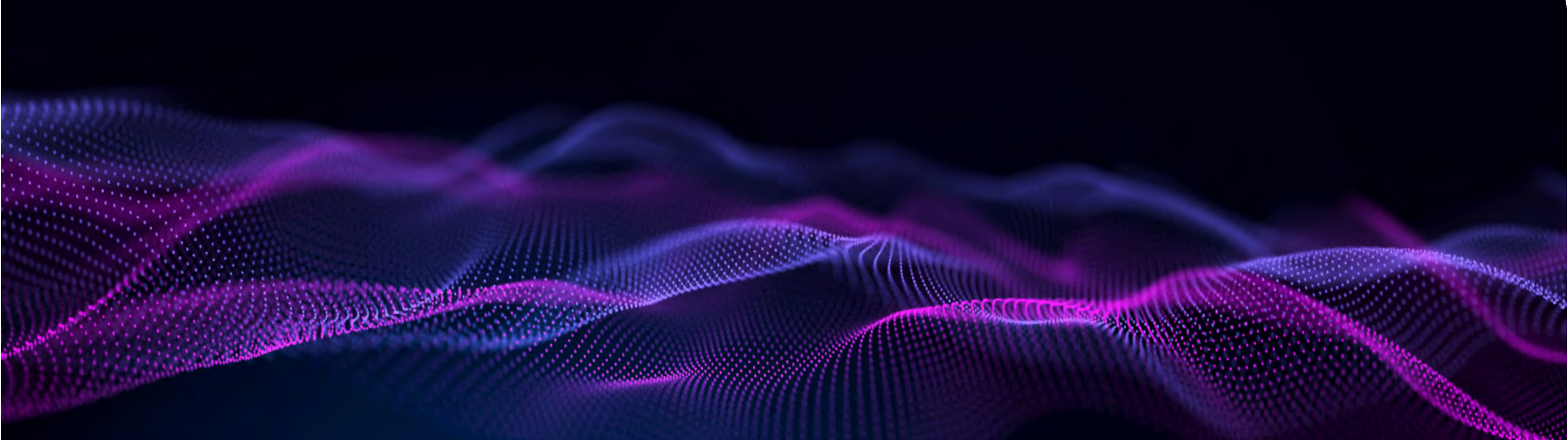
This is not meant to replace valuable and scarce expertise, but rather augment it by using AI to support overtaxed security analysts, identity management professionals and incident responders who need to sort through an increasing amount of information to do their jobs. For example, the integration of AI in security operations centers automates **repetitive and time-consuming tasks**. AI can handle routine monitoring, data analysis, and initial incident responses, freeing up human analysts to focus on more complex issues and higher-value tasks.

This not only increases efficiency but also improves the accuracy and reliability of security operations.

The good news is AI can work as a force multiplier for smaller security teams, which gives organizations a better chance against the newest strains of cyber risk.

50% of organizations say they're using AI to compensate for a **cybersecurity skills gap** according to the Ponemon Institute.

AI can handle routine monitoring, data analysis, and initial incident responses, freeing up human analysts to focus on more complex issues and higher-value tasks.



The same capabilities that make AI a powerful ally in the fight against cybercrime can also be exploited by malicious actors to develop more sophisticated and targeted attacks.

The big picture

AI's role in cybersecurity is paradoxical: a tool for both attackers and defenders. The same capabilities that make AI a powerful ally in the fight against cybercrime can also be exploited by malicious actors to develop more sophisticated and targeted attacks.

DXC Technology recognizes that there will be no one-size-fits-all method to safeguarding the use of AI, just as there is no one-size-fits-all approach to security. Every organization has distinct requirements.

Our teams assist customers in securing their environments by first analyzing and mapping threat models and vectors, identifying new technologies they are embracing, and putting in place the essential safeguards to keep the company secure.

Learn more at **dxc.com**

Get the insights that matter.
dxc.com/optin

f 𝕏 in

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.