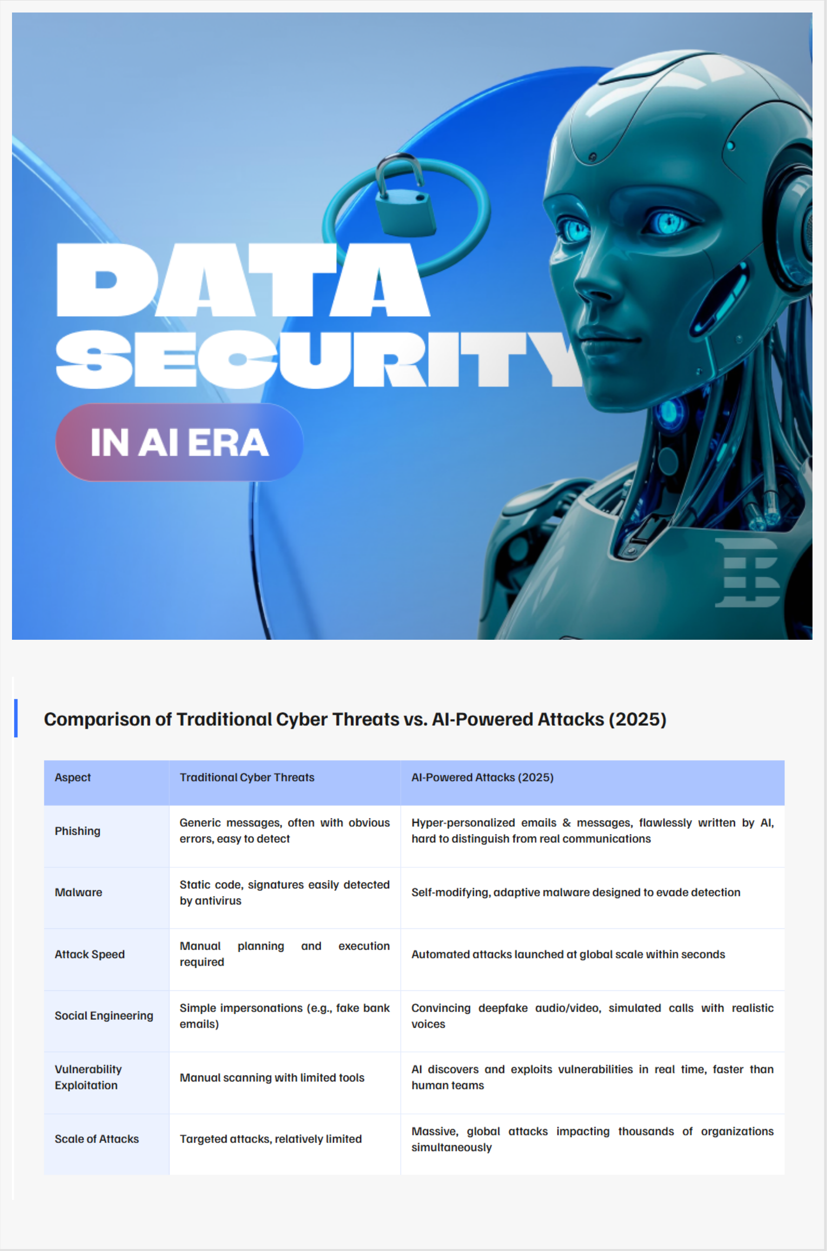
EINPRESSWIRE

Businesses Face a New Era of AI Cyber Threats in 2025 – Insights from TechBehemoths

DeepSeek and Arup cases reveal why businesses need trusted cybersecurity partnerships in the age of AI threats



Comparison of Traditional Cyber Threats vs. AI-Powered Attacks (2025)

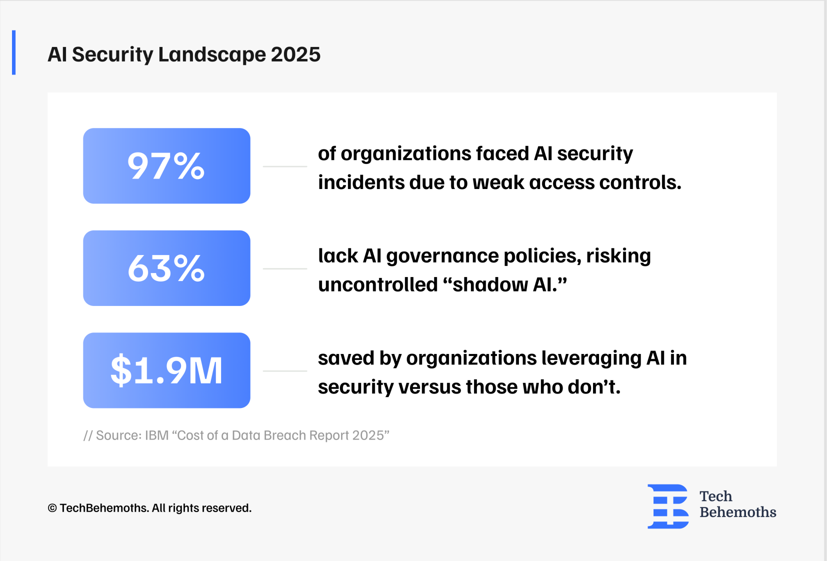
Aspect	Traditional Cyber Threats	AI-Powered Attacks (2025)
Phishing	Generic messages, often with obvious errors, easy to detect	Hyper-personalized emails & messages, flawlessly written by AI, hard to distinguish from real communications
Malware	Static code, signatures easily detected by antivirus	Self-modifying, adaptive malware designed to evade detection
Attack Speed	Manual planning and execution required	Automated attacks launched at global scale within seconds
Social Engineering	Simple impersonations (e.g., fake bank emails)	Convincing deepfake audio/video, simulated calls with realistic voices
Vulnerability Exploitation	Manual scanning with limited tools	AI discovers and exploits vulnerabilities in real time, faster than human teams
Scale of Attacks	Targeted attacks, relatively limited	Massive, global attacks impacting thousands of organizations simultaneously

BERLIN, GERMANY, October 2, 2025 /EINPresswire.com/ -- The latest research from TechBehemoths, the global platform that connects companies with verified IT service providers, shows that businesses are facing unprecedented cybersecurity risks at the same time as artificial intelligence becomes critical to daily operations. The study examines the real impact of AI-based attacks on data security and outlines the growing need for trusted cybersecurity partners.

AI-Driven Threats Enter Corporate Reality

DeepSeek (China, Jan–Feb 2025) – Over 1 million sensitive records - including API keys, backend metadata, and conversation logs - were exposed due to a misconfigured ClickHouse database. The platform also faced massive DDoS attacks and supply chain risks via malicious PyPI packages. Governments, including Italy, South Korea, the USA, Taiwan, the Netherlands, and Australia, restricted or banned DeepSeek in public-sector environments due to security concerns.

In Hong Kong in 2024, the Arup Deepfake Fraud occurred, where an Arup employee was duped by an AI-generated video call pretending to be a CEO. This resulted in 15 unauthorized financial transfers - a total loss of approximately HK$200 million (US$25-26 million). Although internal systems remained intact, the incident highlighted the dangers of deepfakes and the need for robust identity verification.



AI Security Landscape 2025

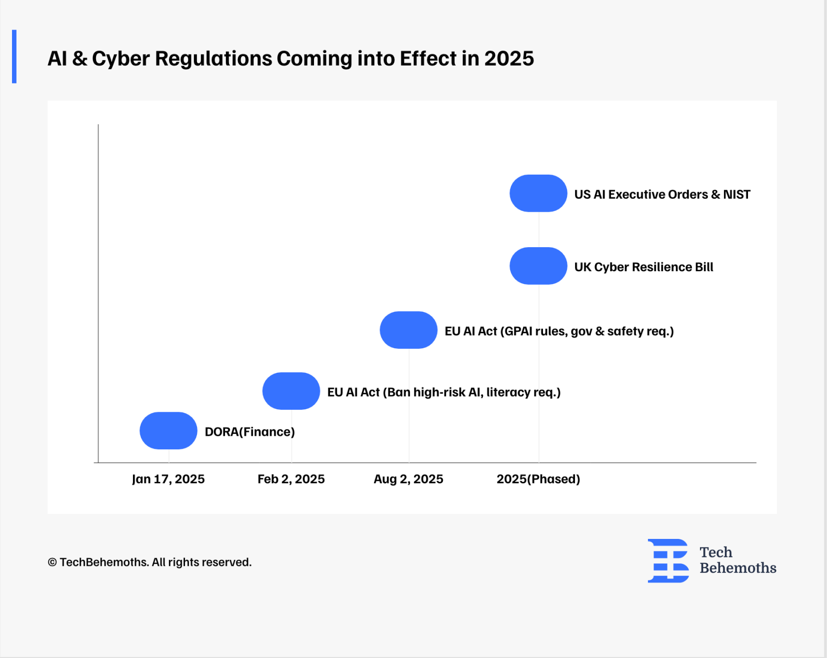
97% of organizations faced AI security incidents due to weak access controls.

63% lack AI governance policies, risking uncontrolled “shadow AI.”

$1.9M saved by organizations leveraging AI in security versus those who don’t.

// Source: IBM “Cost of a Data Breach Report 2025”

AI & Cyber Regulations Coming into Effect in 2025



“These examples show that even small misconfigurations or weak identity verification can lead to catastrophic losses,” said a TechBehemoths research analyst. “AI-powered threats demand a proactive, multilayered cybersecurity strategy.”

From Misconfigurations to Identity Exploits

The TechBehemoths research team has discovered the current hidden vulnerabilities of artificial intelligence that companies may be overlooking:

- Shadow AI usage, where employees operate unapproved AI systems
- Data poisoning and adversarial attacks on machine learning models
- Model hijacking, exposing sensitive data, or producing erroneous outputs
- Deepfake and synthetic identity fraud targeting financial or operational processes
- AI-enabled ransomware, rapidly identifying and encrypting high-value assets

TechBehemoths states that absolutely all enterprises - small, medium, even large, well-established ones - must assess these risks and prioritize security measures that protect AI infrastructure and sensitive data.

Regulations Setting the Tone in 2025

The latest research conducted by TechBehemoths shows the evolution of the regulatory environment in terms of addressing AI risks:

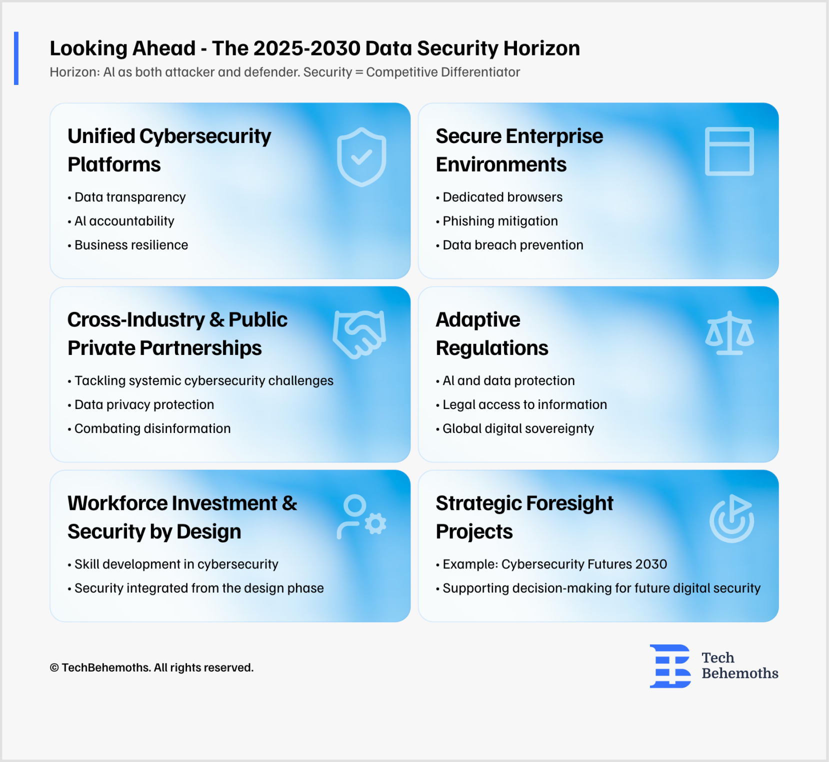
EU AI Law (2025): Implements a risk-based approach to AI systems. The obligations came into effect on 2 February 2025, including bans on high-risk AI and literacy requirements. On 2 August

2025, key provisions on governance, transparency and audits for general-purpose AI models were adopted.

DORA – Digital Operational Resilience Act (EU): Mandatory since January 17, 2025, requiring financial institutions to conduct resilience tests, incident reporting, and operational risk management.

UK Cyber Resilience Bill: Expands incident reporting and critical infrastructure protection requirements.

USA Executive Orders & NIST Frameworks: Establish secure-by-design AI principles, monitoring standards, and accountability guidelines for federal agencies and the private sector.



Looking Ahead - The 2025-2030 Data Security Horizon

Horizon: AI as both attacker and defender. Security = Competitive Differentiator

Unified Cybersecurity Platforms

- Data transparency
- AI accountability
- Business resilience

Secure Enterprise Environments

- Dedicated browsers
- Phishing mitigation
- Data breach prevention

Cross-Industry & Public Private Partnerships

- Tackling systemic cybersecurity challenges
- Data privacy protection
- Combating disinformation

Adaptive Regulations

- AI and data protection
- Legal access to information
- Global digital sovereignty

Workforce Investment & Security by Design

- Skill development in cybersecurity
- Security integrated from the design phase

Strategic Foresight Projects

- Example: Cybersecurity Futures 2030
- Supporting decision-making for future digital security

Tech Behemoths

Compliance with these frameworks is essential to protect organizations from operational, financial, and reputational risks in the AI era.

Businesses Seek Credible Security Partners

Amid these developments, companies increasingly rely on verified cybersecurity and AI risk management providers. TechBehemoths facilitates these connections, allowing businesses to:

- Identify cybersecurity and AI security specialists with proven expertise
- Evaluate provider credentials, certifications, and client feedback
- Access companies experienced in threat monitoring, data protection, and regulatory compliance
- Submit project details for tailored matching with relevant providers

The platform hosts over 1,800 cybersecurity-focused firms and more than 540 IT security & crime prevention experts across more than 120 countries, covering services from penetration testing to advanced AI threat detection.

About TechBehemoths

TechBehemoths is a German global platform that connects companies with over 54,363 IT service providers across all major specialties, including cybersecurity, artificial intelligence, software development, marketing, and many other derivatives of the most essential in tech. Through verified profiles, advanced filtering, and manual matching, TechBehemoths helps companies identify trusted partners capable of addressing today's complex technical and compliance challenges.

Marcel Sobetchi
Mobiteam GmbH
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
X