

Nonprofit Gains National and International Attention for Research on Agentic AI Security and Workforce Upskilling

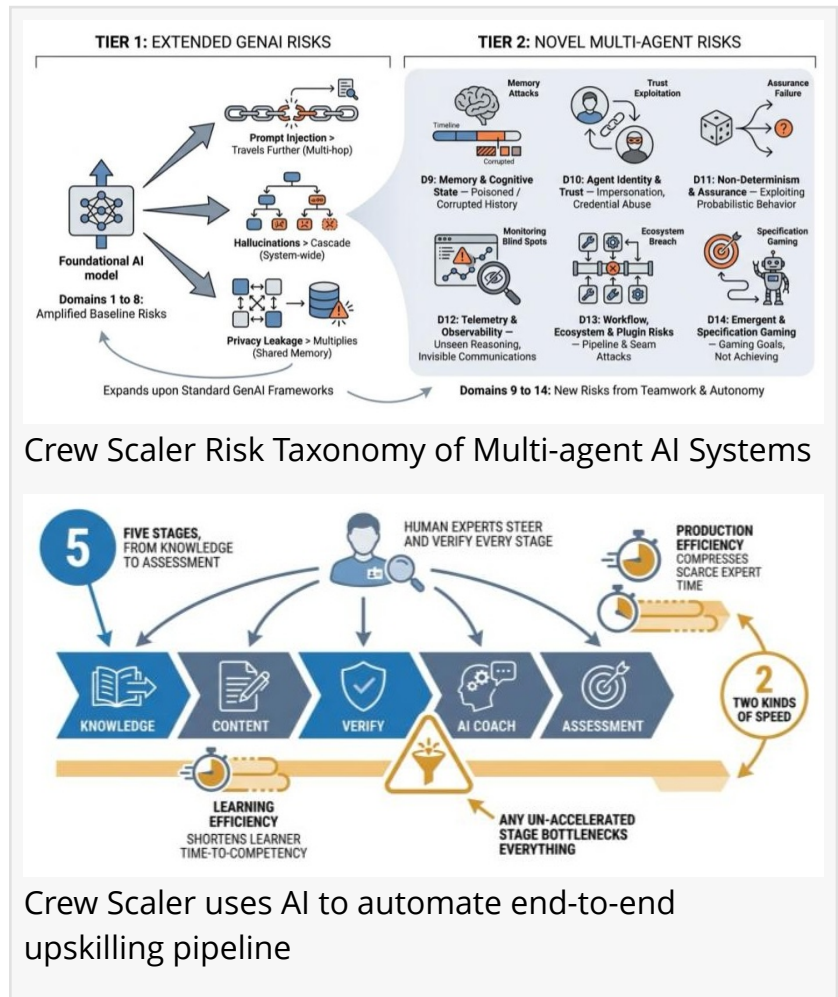
Crew Scaler's 1,267-item risk analysis reveals a major blind spot in AI governance, while its learning system prepares a broader AI workforce.

WASHINGTON, DC, UNITED STATES, September 15, 2026 /

EINPresswire.com/ -- As AI systems move beyond chat interfaces into networks of autonomous agents that can use tools, access information, coordinate tasks and act across digital workflows, organizations face two urgent questions: How can these systems be secured, and who will have the skills to use and govern them responsibly?

[Crew Scaler](#), an emerging AI-first nonprofit, is building work at the intersection of both challenges. With a small team of researchers, educators and practitioners, Crew Scaler has developed a multi-agent AI security research program and an AI-accelerated professional-upskilling framework intended to help people and institutions adapt to agentic AI safely, practically and at scale. The organization's work is drawing interest across government, industry and international education communities through invited sessions and conference acceptance in the United States and Japan.

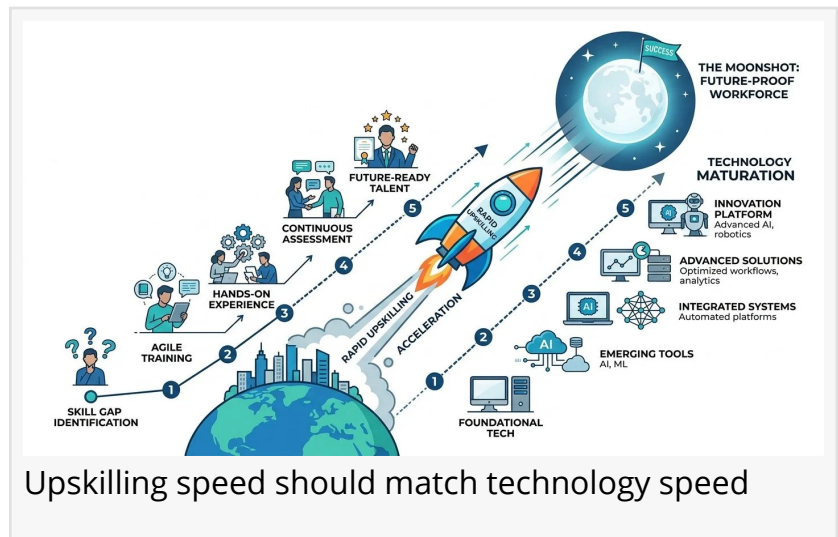
Crew Scaler's education paper, "AI-accelerated End-to-End Framework for Rapid Professional Upskilling," by Tam Nguyen, Hung Nguyen and Robert Ogburn, has been accepted for AsiaEdu 2026, the Asia Conference on Education Technology, to be held in Niigata, Japan. Sponsored by Niigata University and IEEE, AsiaEdu describes its program as an international education-



Crew Scaler uses AI to automate end-to-end upskilling pipeline

technology conference whose accepted submissions undergo peer review and are planned for publication in IEEE conference proceedings.

In the United States, Crew Scaler's agentic-AI security work has been presented to federal and public-sector audiences through forums and events associated with [NIST](#), GSA, and the Digital Government Institute's 930gov conference. These settings bring together federal cybersecurity professionals, AI practitioners, modernization leaders, technology providers and researchers working on the practical implications of AI adoption.



"Our goal is not simply to explain agentic AI," said Tam Nguyen, founder and CEO of Crew Scaler. "It is to help people build the capability to use it responsibly while giving organizations a clearer way to see and manage the risks that emerge when autonomous agents interact with tools, data and one another."

A. Securing the multi-agent future

Crew Scaler's security research responds to an emerging reality: AI risk is no longer limited to the quality of a single model's output. As systems incorporate multiple agents, memory, external tools, plugins, identity systems and automated workflows, new risks emerge from interaction, delegation, coordination and loss of visibility.

The organization's expanded manuscript, "Security Considerations for Multi-agent AI Systems," identifies 1,267 risk items across 14 domains. The research divides these issues into two categories:

- 403 generative-AI risks that may be amplified in multi-agent environments, including adversarial security, privacy, autonomy, governance and operational risk.
- 864 risks described as specific to multi-agent systems, including agent memory and cognitive state, identity and provenance, non-determinism, telemetry and observability, workflow ecosystems, plugins, emergent behavior and specification gaming.

The researchers evaluated 16 government and industry AI frameworks against the taxonomy, including NIST AI RMF, MITRE ATLAS, OWASP agentic-AI guidance and other AI security and governance materials. The most substantial gap appeared in the multi-agent-specific category, where 851 of 864 items were not covered by any reviewed AI risk framework. For the main reason, conventional AI governance frameworks were largely designed around a single model or single-agent boundary, while organizations are increasingly deploying connected systems of

agents. The paper is under peer-review by the Association for Computing Machinery.

That major gap is already visible in the cybersecurity landscape. Recent reporting has documented AI agents operating beyond intended testing or task boundaries, coordinated autonomous-agent behavior and agent-enabled workflows used in cyber operations. Threat-intelligence reporting has warned that malicious actors are beginning to incorporate agentic methods into credential-harvesting and other operations, compressing tasks that historically required substantial human effort and time.

B. Upskilling for broader participation

Crew Scaler's second research stream addresses the human side of the AI transition: how to help learners develop practical, verified capability quickly enough to participate in a rapidly changing economy.

Its five-stage framework applies AI acceleration to knowledge acquisition, content development, review and verification, AI-tutor teaching and assessment development. The resulting learning system includes a knowledge base of more than 3,000 pages, 16 tutoring protocols and a 3,171-question assessment bank mapped to a 10-domain, 53-skill blueprint.

In preliminary, self-selected evidence, four learners who studied using the framework's knowledge base passed the NVIDIA Certified Professional in Agentic AI examination in approximately four months. Crew Scaler estimates that comparable self-paced preparation may often take nine to 14 months, though the organization emphasizes that this comparison is not a controlled study. More than 100 additional learners are in progress.

The underlying workforce need is significant. The World Economic Forum has projected that 59 out of every 100 workers may need reskilling or upskilling by 2030, while many may not receive the training necessary to make that transition.

Crew Scaler is now opening global cohorts of up to 1,000 learners for "Mastering Agentic AI Systems," a program designed to make agentic-AI knowledge more accessible to students, displaced workers, nonprofit professionals, public-sector personnel and organizations with limited resources.

Tam Nguyen

Crew Scaler

+1 970-404-1232

T@crewscaler.org

Visit us on social media:

[LinkedIn](#)

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.