

July 26, 2026

What is Your Plan for Kimi K3?

In case you are not aware of this recent activity, Kimi K3 is a new AI model which claims to be the largest open-weight AI model with trillions of parameters. It is also Chinese. But, it is also incredibly less expensive than US closed models. AND, you can (or will be able to on July 27) download it and run it on your own hardware if you have powerful enough hardware. All of this means that as a company you need to figure out your risk strategy. This is not going to be the last AI model that your employees ask about so figuring out a strategy is forward thinking. Check out what one of our law firm partners, Fisher Phillips, has to say about this, [here](#).

Please check out our blog at <https://www.cybercecurity.com/cyblog>

You can also find copies of the weekly newsletter at <https://cybercecurity-mitch-tanenbaum-blog.com/SNU>

We have a YouTube Channel with a lot of videos. Check it out at: [Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube](#)

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCeurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at <https://cybercecurity.us>. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

Security/Privacy Alerts

Report Says Ransomware Victims Fail to Fix Flaws

Security firm Black Kite says that many ransomware victims remain vulnerable even after a cyberattack. The report highlights what victims fail to do and provides data on the ransomware ecosystem. But let's assume you have not fallen victim to a ransomware attack. How confident are you that you are totally buttoned up? When was your last penetration test? Did you mitigate all the findings? The findings in this report are deeply concerning. If you have concerns, give us a call. Credit: [Cybersecurity Dive](#)

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#). If you are a government employee, check out our AI Governance for Govies at the same site.

Want to stay on top of the news about AI - Check out our news feed on the AIGIP web site at <https://aigip.ai/news/latest-ai-news>

Hugging Face Hit by Fully AI Driven Breach

AI is good. AI is bad. Depends on who is driving it. In this case hackers broke into Hugging Face, a repository for all sorts of AI tools, using those same AI tools. They don't think that the models were compromised, but credentials certainly were. Learn more [here](#).

What is Your Plan for Kimi K3?

In case you are not aware of this recent activity, Kimi K3 is a new AI model which claims to be the largest open-weight AI model with trillions of parameters. It is also Chinese. But, it is also incredibly less expensive than US closed models. AND, you can (or will be able to on July 27) download it and run it on your own hardware if you have powerful enough hardware. All of this means that as a company you need to figure out your risk strategy. This is not going to be the last AI model that your employees ask about so figuring out a strategy is forward thinking. Check out what one of our law firm partners, Fisher Phillips, has to say about this, [here](#).

Why Are AI Companies Buying Tons of OLD Books?

As AI companies search for more training data to improve their models, one company is offering old, printed books as an ideal source because they are guaranteed to be free of the very AI slop AI companies are producing. Books are curated, reviewed and contain human knowledge. Old books are not full of AI slop. Kind of humorous if it wasn't sad. Credit: [404 Media](#)

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to. We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

How do we Use AI and Remain Compliant with CMMC?

It does take some work, but it definitely is possible. Just don't expect to do it without any policies or governance. Check out our educational piece on this at <https://turnkeycyber.us/resources/using-ai-safely-in-a-cmmc-environment>

Q: Now that CMMC Phase 2 is Suspended, We Don't Have to Worry About 3rd Party Assessments - Right?

A: Not quite. DIBCAC assessments, both medium (remote) and high (in person) are still going on - witness the most recent DoJ settlement under the FCA. That is how that one happened (A DIBCAC review). Even the DoD CIO said in the memo that suspended Phase 2 for 60 days that DoD has other authorities - most notably DFARS 252.204-7020 - to do an assessment at any time.

Reference

Want to Know Where the Nearby Flock Surveillance Cameras Are?

Like almost everything today, you can find maps to all of the Flock surveillance cameras anywhere in the world on the web. Put in an address and magic, you can see the cameras. The site is an open-source, volunteer supported project and as of this writing they have mapped

121,000 cameras. This is going to become a problem as they migrate to drone based cameras and that is probably not far off. For the moment, you can check things out at deflock.org .

Software and Hardware to Check Out

AMD Launches Helios Rack System to Rival Nvidia

Microsoft says it is going to deploy AMD Helios racks in Azure data centers. Other AMD customers for Helios racks are Meta, OpenAI and Oracle. It is AMD's first rack system and will ship in the next couple of months. It will compete against Nvidia's Grace Blackwell and Vera Rubin systems. This is an indication of how desperate these cloud vendors are for AI capacity. The chips don't even exist yet and they are getting ready to deploy them. Credit: [CNBC](#)

Important Issues/Patches

If You Thought Microsoft's 600+ Patches was a Lot; Oracle Dropped 1,449!

Oracle just released over 1,400 patches as part of the company's quarterly security fixes. Like Microsoft, Oracle is using AI to find bugs and, apparently, there is no shortage of them. Credit: [The Register](#)

Legislative and Legal Activities

France Greenlights Social Media Ban for Under 15s

Both houses of the French Parliament passed a complete ban on social media access for kids under 15, making France the first European country to do this. The ban takes effect on September 1 when kids won't be able to create new social media accounts. The ban on existing accounts takes effect in January. The law also outlaws the use of cell phones in high schools. The devices are already banned in elementary and middle schools. Platforms are reportedly required to have their age verification methods approved by the French government. That doesn't mean the ban will actually work; most of the time it does not. Credit: [The Record](#)

Education

Nothing to report

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.

Ernst & Young Data Breach Affects Personal, Financial Information

Hackers stole names, addresses, social security numbers, credit card numbers and other information. The incident, discovered in April, involves third party management software that EY uses to support tax-related work for its clients. EY is not releasing details of the attack, but I am sure this will change once the lawsuits start. Credit: [Security Week](#)

Estee Lauder Discloses Data Breach From Oracle e-Business Software

Estee Lauder says hackers exploited a bug in Oracle e-business suite that they use for HR. Information stolen includes the normal HR data: names, addresses, emails, birth date, socials, passports, banking information, health information and other HR info. We are likely to see more announcements like this as the window closes in on companies to avoid penalties for not reporting a breach. Credit: [Bleeping Computer](#)

Hugging Face Says Autonomous AI Agent Breached it

Fully automated cyberattacks - they are here. Today. Do you think you can defend your company against an attack that runs at AI speed? Learn more [here](#).

The President Wants US to Dominate AI - That is Highly Unlikely to Happen

China has pretty much caught up with us in terms of AI. In spite of what the US has done to try and slow that down. The Chinese company Moonshot released Kimi K3, which, while not as powerful as Mythos, is only a little bit behind. The possibility that the US is going to **dominate** AI is, at best, a myth, and at worst, a real problem for the IPOs of OpenAI and Anthropic. Learn more [here](#).

AI Image Fraud Estimated to Cost \$40 Bil Next Year

Deepfake fraud is getting really expensive. Deloitte estimates it to be around \$12 billion in 2023. They predict it will grow to about \$40 billion by next year. As AI gets harder to detect, that number is only going to go up. Are you prepared? Are your employees? Learn more [here](#).

Security News for the week ending July 24, 2026

This week's news: gaps in security hamper US's aviation cybersecurity regulators, a hacker wiped Romania's entire land ownership database - could it happen here, I have often wondered about this, Cisco launches low cost AI models for source code security and New York bans smart glasses in some places. Learn more [here](#).

AI is doing lots of things including making scams more believable. Deloitte says they expect AI driven Deepfake fraud to reach \$40 billion next year just in the US. If you are concerned that you might not be ready for this, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663