

May 3, 2026

AI wiped out an entire company in 9 seconds

One thing we can say about AI is that it is very efficient. The other thing we can say is that it exposes existing policy and procedure problems that were always present. So, in fairness, this one is not AI's fault. See how AI exposed existing non-AI problems [here](#).

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

You can also find copies of the weekly newsletter at <https://cybersecurity-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@CyberCecurity.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://cybersecurity.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

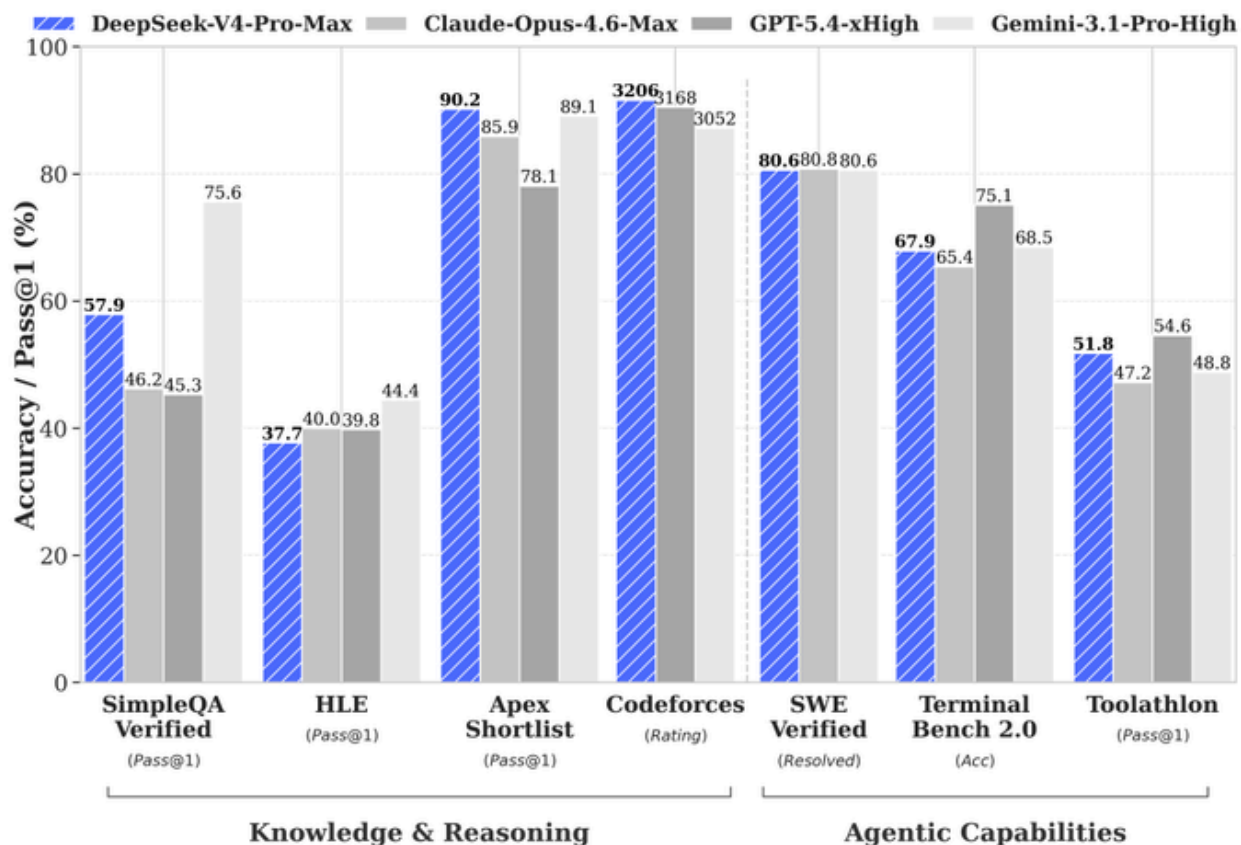
Nothing to report

AI Alerts

Check out our Certified AI Governance Leader Course at [AIGIP.AI](#).

China's DeepSeek V4 Ups the Ante for US Companies

China has released a new version of DeepSeek, it's competitor to OpenAI and Anthropic. It has 1.6 trillion parameters total, enhanced agentic capabilities, outperforms other open models in reasoning and coding. There is a smaller version, called Flash, with only 284 billion total parameters which is smaller and cheaper to run. The model costs \$3.48 per million tokens compared to \$25 for Claude Opus 4.6 and \$15 for GPT 5.4. And, it is based in China – what could go wrong?



Credit: [The Deep View](#)

Google announces up to \$40 Billion investment in Anthropic; Amazon Invests \$25 billion

Google is starting with investing \$10 billion in one of their biggest competitors, Claude, based on Anthropic's current \$380 billion valuation. The remaining \$30 billion is tied to Anthropic meeting specific contract requirements. If you are asking why Google is potentially investing \$40 billion in a competitor rather than in Gemini, good question. This follows Amazon/AWS investing up to \$25 billion in the company. From Anthropic's end, both of these companies have amazing cloud infrastructure for them to leverage. Credit: [TIKR](#)

AI wiped out an entire company in 9 seconds

One thing we can say about AI is that it is very efficient. The other thing we can say is that it exposes existing policy and procedure problems that were always present. So, in fairness, this one is not AI's fault. See how AI exposed existing non-AI problems [here](#).

Google Fixes a 10/10 Gemini Bug

Google fixed a 10.0 grade bug in the Gemini CLI npm package and google-github-actions workflow. The bug allows a hacker to force their own malicious content to load as the Gemini configuration which triggered command execution directly on the host, bypassing security before the sandbox was even initialized. The vulnerability is limited to certain use cases and requires manual review and fix. Credit: [The Hacker News](#)

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.

Q: What if I get a letter from DIBCAC?

A: DIBCAC is the Pentagon's CMMC auditor and their audits are not voluntary and are more comprehensive than even a CMMC Level 2 third party assessment. If you get one of these and you are not prepared, you are not going to have a fun week when they arrive on site. You are much better off if you are prepared. And this is not something where you can say "we are not ready, can you check back in a few months".

Reference

CISA and its Partners Release "Careful Adoption of Agentic AI Services"

CISA and Australia's Cybersecurity Center along with the similar agencies in Canada, New Zealand and the UK issued this guidance on carefully deploying agents. No one is saying do not deploy them, but the smart people are saying be careful. Learn more from [CISA and its Partners](#)

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

732 Byte Exploit Can Take Over All Linux Kernels Released After 2017

You know those people who say that open source is secure because, well, it is open source. Have them read this and then ask them if they still believe that. Open source is software and software has bugs. This one is very compact. Only 732 characters of Python and you can own the Linux kernel. It has been tested to work in Ubuntu, Amazon Linux, Red Hat and Suse, but it likely works in Debian, Fedora and others. Now there are multiple versions of the exploit in different languages. The exploit may even allow an attacker to escape the container it is in.

Credit: [Cybernews](#)

Legislative and Legal Activities

Asia for Asia - Blocks Foreign Takeovers

The United States is not the only country to disapprove of foreign investments. While their reason is unknown, this could be in response to US moves to stop foreigners from purchasing US companies and real estate. This is similar to the move by China to block Meta's takeover of Manus as a national security threat. In this case, the proposed buyout of milling machine maker Makino by Asian investment firm MBK Partners was squashed by the government. These are only two recent examples of governments blocking foreign investment in critical industries. Is this a trend? I guess we will have to wait and see. These moves by governments are making the venture capital companies a bit nervous as they often want a quick exit if that is profitable for them. Credit: [Japan News](#)

Education

The IT Behind Epstein's Empire - Camera Systems, Mystery Manager and the DoJ

Normally I would put this in the tin foil hat crowd's realm, but apparently this came out of the DoJ's release of Epstein documents. What does fall into the conspiracy theory realm is what Epstein did with the video footage he collected. He apparently, based on DoJ documents, had a world class video surveillance system that covered his entire island. Initially, the system was pretty basic, but later, it became very sophisticated. You can draw your own conclusions about what he did or threatened to do with the video he collected. Credit: [The Register](#)

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.

Eurail admits 1.3 TB of data including passports stolen in December breach

By the time they got their arms around the problem in February, the breach was much larger than they said originally. 308,000 travellers, 1.3 TB, passport and identity documents stolen, bank account details, health information source code and full backups. As of now, some travellers are being told to replace their passports. Credit: [Breached Company](#)

Supremes not fans of geofence warrants

A geofence warrant is one where an agency asks a provider like a phone company to tell them about everyone who was in a particular area during a particular time window. Almost all of these people did nothing wrong other than being in an area that some agency is interested in. The Supremes are about to decide whether they are constitutional and under what conditions. Learn more [here](#).

California's new do not email law - fines are company ending

The law itself is complex and, if it applies to you, gives you a forever responsibility. The fines, which can be as high as \$200 per day per consumer affected can easily bankrupt a company. If you buy or sell contact contact information, you should understand what this law means. Get educated [here](#).

Anthropic Code Security

This is AI at its best. Or worst. This is the publicly available version of Mythos and it is pretty powerful. If you choose not to use it, it does not mean that hackers won't use it against you. This is definitely something that needs to be on your radar. Learn more [here](#).

Security News for the week ending May 1, 2026

This week's news: China blocks Meta's takeover of Manus, officials consider 72 hour deadline for patching federal systems, Congress does what it does best - punt on Section 702, Toronto hackers go mobile and hack thousands at once and White House asks industry about their security practices. Learn more [here](#).

Do you have a strategy about using AI? The subject is moving so far that it is hard to stay current, but if you don't, that doesn't mean the hackers are going to cut you any slack. If you are not confident that you are doing better than the hackers are, contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663