July 12, 2026

AI is a Great Scapegoat for Firing People

There are two ways to use AI - to increase revenue or decrease costs. Which one a company uses will separate the great from the rest. Microsoft spent billions on AI this year but shares are down 23%. So what do you do? Fire almost 5,000, which, in fairness, is only around 2% of their workforce. But since, apparently, based on their stock price, the market is not impressed with their results, you fire some people to make it look like AI is great. The smart companies are keeping the people that AI frees up to increase revenue. Credit: **Cybernews**

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@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://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

Even Meta Sometimes Does the Right Thing

Last week Meta announced that it released a tool that allowed anyone to use any other user's public Instagram pictures with a new AI tool called AI Muse to create AI images that included details from other's images. The default, of course, was enabled. Would you expect anything else from Meta? If you were smart enough you might be able to find the option squirreled away in an obscure menu three levels deep to turn it off. Two days ago Meta discovered that there is such a thing as bad press and they were on the receiving end of it. A lot of it. For the moment the feature is gone but don't assume that Meta won't bring it back after putting some lipstick on it. Credit: **Pymnts**

AI Alerts

Check out our Certified AI Governance Leader Course at AIGIP.AI.

AI is a Great Scapegoat for Firing People

There are two ways to use AI - to increase revenue or decrease costs. Which one a company uses will separate the great from the rest. Microsoft spent billions on AI this year but shares are down 23%. So what do you do? Fire almost 5,000, which, in fairness, is only around 2% of their workforce. But since, apparently, based on their stock price, the market is not impressed with their results, you fire some people to make it look like AI is great. The smart companies are keeping the people that AI frees up to increase revenue. Credit: **Cybernews**

China to Ban Claude Code as "National Security Risk"
Sound familiar? I think it is President Trump's own words coming back against an American company to ban Claude in China. Anthropic admitted the tracking code the Chinese found was theirs and they said it was an experiment, but now that they were found out, the tracking code will be removed in the next release. Credit: **Data Breach Today**

Companies Need to Manage AI Costs - Use AI intelligently
One company - not identified - blew $500 million on Claude Code in a month. Intelligent companies (I thought) like Adobe, Amazon, Citi and others are seeing AI related spending triple and are being forced to reduce AI spend. **Microsoft reports** that using the tech is more expensive than paying human employees. Does that mean you should ignore AI and go back to using a pocket calculator and a paper encyclopedia? ***No. Absolutely not***. It means that you need to have an AI governance strategy (shameful plug: contact us to assist you in creating and managing this). The companies that are reigning in AI use are the same ones that told employees "go spend money … we don't have a strategy, but go spend money". That is NOT a plan for success in any field.

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.

What is the impact if we retain consultants, law firms and other vendors with ties to China?
Starting this month the Pentagon is enforcing Section 851 of the FY25 National Defense Authorization Act. This section prohibits the Pentagon from awarding contracts to companies (including parents and subsidiaries) that use consultants, law firms or PR firms that also lobby for organizations with ties to the Chinese military. Information on the Section 1260H list can be found **here** and the list itself can be found **here**. The ban applies to both current and future contracts.

Q: What does it mean that a C3PAO has to be accredited after it is authorized?
A: Once a C3PAO is authorized by the CyberAB, meaning that it has enough assessors, it has passed its own Level 2 assessment by the DIBCAC, passed the Foreign Ownership test and other requirements, it has, by regulation, 27 months to get accredited under ISO 27020. This involves audits of quality systems, assessment procedures and personnel qualifications. In order for this to happen, the Cyber AB itself has to be accredited under ISO 17011, the standard for bodies to accredit other organizations, but there are some political challenges that the Cyber AB and Pentagon are working on. One requirement was to divest from training people. Moving CyberAB's training arm to ISACA meets that requirement, but since ISO is an international organization and they need to watch a live assessment, that presents some legal challenges

that are being worked out. In the meantime, the Pentagon told the Cyber AB that they are waiving that requirement. Geopolitics. What fun.

Reference

Lone Attacker Uses AI to Breach AWS in 72 Hours
This attack was not against all of AWS but a single customer's environment. Still, we rarely publicly see the post-mortem. Definitely worth reading. No surprise - the attacker used agentic AI to accelerate the recon, tool development, command structure and all adaptations. The speed is the scary part. Learn more at **Dark Reading**

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Another Antique Linux Bug Found
This bug is 15 years old. It is a critical kernel vulnerability (CVE-2026-43499) that allows an attacker to reliably elevate their privilege. It exists in nearly all Linux distributions. The name it has been given is ***GhostLock*** because it is a "lock" (Mutex for you geeks) that is cleared when it should not have been. It does require some sophistication to exploit, but with AI, that is probably not hard. Credit: **gbhackers**

Legislative and Legal Activities

Nothing to report

Education

AI Agent Autonomously Hacked a Network, Adapted on the Fly and Demanded a Ransom
JadePuffer exploited a vulnerable Langflow server, harvested credentials, moved laterally and encrypted more than 1,300 database records, marking what Sysdig describes as the first documented end-to-end agentic ransomware operation. It executed over 600 different payloads that were coordinated by it. AGENTIC RANSOMWARE. Are you ready? This did not require any earth shattering new techniques, but it did require an AI that tested thousands of possibilities a second. Credit: **CSO Online**

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.

3 Year Old Linux Kernel Bug Hands Any User Root
The Bad Epoll Linux vulnerability hits servers, desktops and even Android. Epoll isn't some optional Linux feature; it is the I-O event controller at the heart of how Linux handles concurrency. There is no workaround; the only solution is to patch. While the bug has been fixed, each distribution has to integrate it into their code. If you have a Linux host supporting

VMs, you need to patch the host first because that makes all VMs vulnerable. Credit: **Breached Company**

Accenture Confirms Breach - After Hackers Offer Data for Sale
For a company the size of Accenture, the breach is small - 35 gigabytes of source code and other data. It includes RSA and SSH keys, Azure access tokens, Azure storage tokens and configuration files. IF - and this is a big if - Accenture knows what was stolen they can, with significant work, mitigate the damage. If they don't know what was stolen and they have to revoke all keys, that is a REALLY big task. Credit: **Bleeping Computer**

Bug in Oracle Software Impacts Many Companies; Millions of People
ShinyHunters exploited a bug in PeopleSoft ERP software to create havoc. For the National Association of Insurance Commissioners alone, they lost 105,000 files including regulatory documents, customer records, payment data and production credentials. Others impacted are Nissan and Medtronic, although Medtronic apparently paid a ransom. Add to that 14+ million emails compromised in Japan. Also Kubota. I suspect more to come. Apparently hackers were in there for a month before being discovered. Let the lawsuits begin. Credit: **My Privacy Blog**

- -

AI means you can forge documents in minutes
Here is another "feature" of AI and if you count on documents being legitimate, this means you need to rethink how you validate that a document is real. You can no longer trust that what you see is real because it may not be. What is even more concerning is that government agencies like county recorders say they have no responsibility to verify that a document is real. They just record it and give it validity. Learn more **here**.

Chinese firms plans to build Nvidia competitor in months
Will US firms buy Chinese AI chips? What if they cost a quarter of what Nvidia charges? Bytedance, the creator of TikTok, is the one doing this and they certainly have the money. They will optimize their applications to work with their chip also. Learn more here.

Gigawiper Windows backdoor
Gigawiper is a malware tool that has bolted together several other tools to make a really dangerous piece of malware. Among other features is a ransomware-style encryption tool that encrypts your files with a random key that it does not save, so there is no way to decrypt your data. Learn more **here**.

Security News for the week ending July 10, 2026
This week's news: Facebook data center contaminates city's water treatment plant, Supremes allow Texas app store accountability act to go into effect while the law is being appealed, Meta paid workers to pose as teens to test rivals' security, are license plate cameras next target by Supremes and Apple sues [former?] AI partner OpenAI. Details **here**.

JadePuffer executed a fully automated ransomware attack, even including demanding a ransom. *The attack involved running more than 600 resources, dynamically adjusted the process, moved laterally inside the network and demanded a ransom. Are you ready? If not, you should probably contact us.*

Mitch
www.CyberCecurity.com
www.TurnkeyCybersecurityAndPrivacySolutions.com
Mitch@CyberCecurity.com
720-891-1663