

May 31, 2026

AI Reality - The Tools You Used Yesterday Won't Protect You Tomorrow

With hackers using tools like Mythos finding tens of thousands of bugs, if you are not protecting yourself using AI, you are going to fall victim to the hackers. Like it or not, hackers are already using AI to figure out how to break in and that is only going to get worse. The message is that you need to use AI to protect yourself to try and level the playing field.

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

Ransomware Actors Show Up in Person to Steal Law Firm Data

Call me stupid, but if someone you don't know walks into your office and says that they are here to work on your non-broken computer, with no advance warning, should you give them access? Apparently folks at some law firms think the answer is yes. I will say that hackers that come in person and socially engineer lawyers are either extremely clever or under arrest. They have been doing this successfully since 2023. BEWARE!!! Credit: [Dark Reading](#)

AI Alerts

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

AI Reality - The Tools You Used Yesterday Won't Protect You Tomorrow

With hackers using tools like Mythos finding tens of thousands of bugs, if you are not protecting yourself using AI, you are going to fall victim to the hackers. Like it or not, hackers are already using AI to figure out how to break in and that is only going to get worse. The message is that you need to use AI to protect yourself to try and level the playing field.

CNN Sues Perplexity AI Over Copyright

Perplexity says you cannot copyright facts. This is true, but you can copyright the way they are presented. Courts are all over the landscape on their findings and the appeals and Supremes have not ruled on all of this yet, so, for now, the AI companies kick the legal can down the road and hope they are rich enough later to pay the bill if and when it comes due. Credit: [CNET](#)

GCHQ, The UK's Version of NSA, is Using Agentic AI to Protect Critical Infrastructure

The new system is intended to be operational within five years. It is being designed to detect and alert to threats across critical national infrastructure, airlines, telecoms firms and other "major" companies like Jaguar Land Rover, whose breach in March last year was the most expensive ever recorded in the UK. **THIS IS THE FUTURE.** Actually, this is the now for hackers. Get on board. Need help? Contact us. Credit: [Computing](#)

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 I know if my Managed Service Provider is a Cloud Service Provider?

NIST SP 800-145 lists five criteria and they ****ALL**** have to be met in order to be considered a cloud provider. 800-145 is available on the NIST site, just Google it.

Can we have phones and tablets in our CMMC world and contain CUI?

The short answer is yes. The longer answer is that you dramatically increase your cost and time and, with regard to personally owned phones, probably not because you **MUST** fully manage those phones. There are ways to include even BYOD devices that are less painful/expensive than full management. Contact us for details.

Is it just new contracts that will have to be CMMC compliant after November?

No. Reports are that many/most contract extensions for next year will have some form of CMMC requirement. Expect it and be prepared.

Are there any AI tools to transcribe meeting notes like [Read.ai](#) that are compliant for CUI?

Make a distinction between CUI and ITAR; the rules for ITAR are more complicated. For CUI, tools like Microsoft Gov Teams and Gov Zoom work, but most tools need to be banned. If you add ITAR to the mix, the problem gets even harder. Most likely, your favorite tool is **NOT COMPLIANT AND CANNOT BE USED**. Contact us for assistance.

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Ubiquiti Patches Three Max Severity Vulnerabilities in their Firewalls

Ubiquiti has released security updates to patch three maximum severity vulnerabilities in UniFi OS that can be exploited by remote attackers without privileges. The first flaw ([CVE-2026-34908](#)) enables attackers to make unauthorized changes to targeted systems by exploiting an Improper Access Control weakness in UniFi OS, while the second ([CVE-2026-34909](#)) allows them to access files on the underlying system by abusing a Path Traversal vulnerability, which could be manipulated to access an underlying account. Learn more [here](#).

Another 14 Year Old Linux Bug Discovered

And this one did not even require AI to find. Deutsche Telecom's Red Team discovered it and it affects the RPM software package installation manager. The bug allows packages to be installed as ROOT, even if the user does not have Root permissions. Linux distributions affected include Ubuntu Desktop 18.04, 24.04, 26.04, Ubuntu Server 22.04-24.04, Debian Desktop Trixie, Rocky Desktop 10.1, Fedora 43 Desktop and others. Likely, all distributions that ship with PackageKit (which is most) are vulnerable. Credit: [Security Week](#)

Legislative and Legal Activities

California Governor Signs EO Aiming to Soften AI Blow to Workers

We know that AI is going to have an impact on the business world. It will be both good and bad. The gov's EO tells state agencies to study potential workforce disruptions and make recommendations about what the state might do to soften the blow. Credit: [Fisher Phillips \(law firm\)](#).

Education

Amazon Thinks the Future of Data Centers Depends on This

Amazon knows a thing or two about networks and for any of our readers who have wrestled with stacking network switches, you know that generates latency. Well, some of Amazon's brain trust thinks they have a solution to this. One that dramatically improves latency. And, it improves energy efficiency. Unfortunately, it won't make me young. But, we can take what we can get. Credit: [Wired](#)

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.

UK Private Visa Management Service Didn't Protect Customer Data

This is not a breach. For there to be a breach there must be security in place that was compromised. I am not sure what you call it when a company can't be diligent enough to protect their customers' data in the first place. Oh, wait, I do. GUILTY! Credit: [Tech Crunch](#)

Charter Communications Breached - 42 Million Records Compromised

Hacking group ShinyHunters told Bleeping Computer on April 1st that it hacked Charter. Almost two months later, Charter admits they were hacked. They claim no "sensitive personal data" was stolen. The data came from their Salesforce instance and contained names, emails, phone numbers, plan information and other data. Credit: [Bleeping Computer](#)

Mike Lindell (MyPillow) has Something Else to Worry About Besides Million Dollar Lawsuits

The Company appears on Play ransomware's breach site with a date of May 24 and a pay by or we leak your data date of May 29th. The claim the stolen data includes private and confidential data, client documents, budget, payroll. IDs, taxes, finance information and more. If true, that is not the kind of media coverage Lindell needs. Credit: [The Register](#)

Trump's AI executive order vaporizes on day of signing

The White House had already leaked the contents of the EO to the press and then, apparently, even something as lightweight of an EO like this - where companies could voluntarily share their new releases with the government before releasing them was, I guess, a bridge too far for his campaign donors, so the status quo remains. The states are doing their thing and the feds are sleeping. Details [here](#).

Anthropic - the supply chain risk that isn't

In a massive power play that failed, Hegseth declared that Anthropic was a supply chain risk and as a result, Anthropic's revenue launched past OpenAI. Now, apparently, the NSA told the White House that they needed that software and somewhat quietly, the White House says that the supply chain risk is not a problem for the most secure agency in the nation. Details [here](#).

The Secure Data Act - is it theatre?

Well, according to the Electronic Frontier Foundation, the answer is yes. This is the latest iteration of the feds trying to pass a national privacy law while at the same time nuking 20+ state privacy laws. That is not an easy task and that process is not simple and requires a lot of compromises. Such as: (a) too many companies exempted, (b) limited enforcement and (c) it preempts laws that Congress will have to explain to the people who elect them. Meaning, it is not likely to become law. But, you never know. Details [here](#).

Security News for the week ending May 29, 2026

This week's news: Florida has a new law to force data centers to pay for utility costs, oops, someone sent 107 bitcoin to the shredder, what is good for the goose is ..., as the prez cancels the AI EO, NIST begs companies to play with them and the FBI claims it recovered \$8 billion in crypto; gangs achieve a similar goal differently. Details [here](#).

The feds can't seem to figure out what they should do when it comes to governing the use of AI. But that doesn't mean that you can set back and watch. If you need help figuring this out, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663