

June 7, 2026

Court allows Texas to implement age law

The Texas legislature passed a bill which mandates age verification requirements for Internet access without giving website owners any guidance on how to do that other than to make a "good faith effort". This will make lawyers rich and websites very cautious. It also allows anyone who has a beef with you to sue you. You get to defend yourself at your cost and likely cannot recover legal fees, even if you win. If you run a website you need to watch this closely because anyone who gets angry with you can sue you and you get to defend yourself.

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.

This week there is a new video on AI - it is here to stay. Lead. follow or get out of the way, because it is coming for you.

Security/Privacy Alerts

Standard & Poors Global Says Poor AI Governance Puts Credit Rating at Risk

So you say that you are not worried about AI fueled cyberattackers hacking you so AI governance is not a problem. S&P Global says that without strong AI governance, companies are putting their credit ratings at risk. This impacts both borrowing costs and reputation. Are you concerned about those factors? Contact us for assistance. Credit: [Cybersecurity Dive](#)

AI Alerts

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

President signs even more slimmed down AI executive order

After cancelling the signing ceremony of a different version of an AI executive order a few weeks ago, the president signed an even more slimmed down version this week. The previous version was supposed to have an audience of AI executives witness the signing. Not this time. The new EO tells the government to develop a benchmarking process for understanding an AI's capabilities. It also asks AI developers to, pretty please, let us see what you are about to release. The EO hopes that those companies might give the government up to 30 days advance access. [The EO](#) is very thin on details. For example, it says that the Committee on National Security Systems and the Secretary of Defense should, within 30 days, prioritize the cyber defense of their information systems by taking appropriate and expeditious action. Okay, I guess. Besides the one voluntary request to industry, virtually all of the EO is about getting the government off the dime about responding to the risk represented by AI used by hackers, which is a good thing. Of course, there is no money made available since EOs can't authorize funds. Everything has to be done with existing money and staff. Credit: [MSN](#)

Claude eBook on Zero Trust for AI Agents

We are beginning to get our arms around zero trust, but Anthropic has come out with a guide of zero trust for AI agents. Definitely needed. Check out their blog post [here](#).

AI Vendors Are Getting Sued - Are You Doing the Needed Due Diligence?

OpenAI has a target on its back but they are far from the only AI vendor getting sued. As AI is incorporated into all sorts of products, do you just trust the result? Hopefully not. Your due diligence regime has to be different - different questions and different contract language. Are you prepared? Need help?

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.

Leonardo DRS Says Get a Third Party CMMC Certification or Goodbye

Another day, another defense prime is telling their subs to get certified or we are not going to sub to you. Check out the details at <https://tcps-blog.com/cmmc-reqs/>

How long do I have to get recertified after a significant change?

The DoD is not saying, so it is going to be up to your organization's risk tolerance. Your prime or customer could have an "opinion" about this and it could be sooner than you might like.

Reference

SpaceX Sells Compute to Competitors Anthropic and Google

Apparently Musk really doesn't care much about the AI business as long as he makes money. He is selling data center compute power to Google for \$920 million a month and to Anthropic for \$1.2 billion a month. Both can cancel with 90 days notice. Still, \$2 billion a month is a nice round number. Credit: [Tech Crunch](#)

Software and Hardware to Check Out

IBM and RedHat to Fund \$5 Bil and 20,000 Engineers to Secure Open Source Software

While this is not really new software, it is something to closely watch if you use open source software. Project Lightwell is an effort to help find and fix vulnerabilities in open source software. IBM will create a “trusted enterprise Clearinghouse” with a LOT of engineers and using AI, will fix vulnerabilities at scale. IBM has been testing this with some of its clients like Bank of America, Chase, Mastercard and Visa, among others. The project will provide a secure space to discuss security issues with open source software. The goal is to speed the detection and resolution of bugs. Hopefully, once this is in operation, it will eventually reduce the number of 10, 15 and 20 year old vulnerabilities discovered. Credit: [Cybersecurity Dive](#)

Important Issues/Patches

Cisco Finds 7th Zero Day in SD-WAN Just This Year

This one is being exploited in the wild. It is tracked as CVE-2026-20245. THERE IS NO PATCH AND NO WORKAROUND EITHER. It does take an authenticated local user, so that means that your system has to be compromised at some level for this attack to work. If a hacker can exploit it, they can push configuration changes to edge devices. Watch for a patch, hopefully soon. They do have indicators of compromise. Credit: [Security Week](#)

Legislative and Legal Activities

Congress Can't Agree on What to do About FISA Section 702

Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows the intelligence agencies to spy on Americans without a warrant with just a few restrictions. Even the most right wing Republicans don't trust the government to be appropriate. That is why 702 expires every few years even though the intelligence community would like it to be permanent. 702 expired in April and Congress has been renewing it for a couple of weeks here and a month or two there, hoping they could come to some agreement about what to do. So far, they have not figured that out and it is about to expire again (June 12). Expect them to kick the can down the road again. Credit: [Politico](#)

Education

NIST Releases to “Responding to and Recovering from a Cyber Attack for Manufacturing

Manufacturing uses a lot of computer controlled equipment, otherwise known as industrial control systems (ICS). These computers are very different from your office computers. ICS computers are targets for hackers because they are not hardened like other computers are. This is a draft, so NIST is looking for feedback. Note that at 186 pages, it is not a light read. Learn more [here](#).

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.

Carnival Cruise Corp. Breach Exposes 6 Million. Or 8 Million. Or more

The official number is 5.9 million but others say it is as high as 10 million plus terabytes of corporate data. ALL FROM ONE EMPLOYEE BEING PHISHED. Why did that employee have access to all of that data? Sounds like an access control rights issue separate from the phishing. Data stolen includes PII like name, address, email and phone, but also identity

information like passport and drivers' license. This is going to be expensive for the largest cruise ship operator (90+ ships). Credit: [Bleeping Computer](#)

Attackers Grab Password Vaults From Dashlane

At least the vaults are encrypted. The attack was low tech and used a high volume brute force attack attempting to register new devices of existing users. The company says that fewer than 20 vaults were compromised. Once they got the vault they need to figure out your master password, so if that is strong, they still have a big problem. Choose your master password carefully. Credit: [Helpnet Security](#)

Court allows Texas to implement age law

The Texas legislature passed a bill which mandates age verification requirements for Internet access without giving website owners any guidance on how to do that other than to make a "good faith effort". This will make lawyers rich and websites very cautious. It also allows anyone who has a beef with you to sue you. You get to defend yourself at your cost and likely cannot recover legal fees, even if you win. If you run a website you need to watch this closely because anyone who gets angry with you can sue you and you get to defend yourself. Details [here](#).

Anthropic expands Mythos to more "Trusted" organizations

Anthropic says that they will give a few more companies (about 200 total out of 30 million businesses) access to Mythos. Given that is about 0.06% of all businesses, that probably won't include you, but maybe. Learn more [here](#).

AI EO, AI Bill, Oh My!

The Washington crowd definitely wants people to think that they are doing something about AI while doing absolutely nothing. Typical Washington. The AI EO says agencies should do something soon. The AI bill wants to preempt dozens of state laws because, well, because. Stay tuned as this could impact you and probably won't be well thought out. Learn more [here](#).

Security News for the week ending June 5, 2026

This week's news: Tennessee is the second state to ban cryptocurrency ATMs, do you patch your users' personal phones - 124 Android patches this month, Markwayne has a plan - we will see if it works, Meta's smart glasses have facial recognition software built in and Supreme Court upholds fines against AT&T and Verizon over selling your data. Learn more [here](#).

Carnival will spend tens of millions after ONE employee fell for a phishing scam. I don't know, but I suspect that the user's account had way too many permissions. Need help designing the correct permissions for your users? Contact us. .

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663

