

August 30, 2026

The News About Last Month's Attacks on Water Systems Just Keeps Getting Worse

Initially we were told that a water system in Minnesota was hacked. Then a few of them. The president said, basically, what do you expect, it's Minnesota, they are incompetent. Then that turned into water systems in a half dozen states. Now the feds are admitting that more than a hundred systems were targeted. These states were all over the country. Supposedly the feds are planning to help water systems protect themselves. We have no idea what that might look like or who is going to pay for it. Stay tuned for what the feds come up with to see if it is helpful or just for show. Credit: [The Register](#)

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

Cities Ditching Flock for ?Who? Verkada

As Flock's brand becomes radioactive and they work to spin what they are doing, cities are moving to other, less politically lethal, brands. One is Axiom, but another player is Verkada. Their play is that the data is 100% under the city's control. That should sell a lot better to voters than Flock's big brother strategy. We shall see. Learn more at [Cybernews](#).

The News About Last Month's Attacks on Water Systems Just Keeps Getting Worse

Initially we were told that a water system in Minnesota was hacked. Then a few of them. The president said, basically, what do you expect, it's Minnesota, they are incompetent. Then that turned into water systems in a half dozen states. Then a dozen states, about 30 water systems. Now the feds are admitting that more than a hundred systems were targeted. These states were all over the country. Supposedly the feds are planning to help water systems protect themselves. We have no idea what that might look like or who is going to pay for it. There is a very small group of techies that spun out of the security conference Defcon that has been

helping a handful of water systems, but they are volunteers and have no money to buy stuff or replace tech. Stay tuned for what the feds come up with to see if it is helpful or just for show. Credit: [The Register](#)

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>

OpenAI Says Jalapeno Beats Nvidia Blackwell

In fairness, this is very preliminary and under the control of OpenAI, so take it with a dose of skepticism. Jalapeno is their new AI chip. They have been touting this as being created in record time, but as more information comes out, maybe not so. For you chip nerds, they are implementing this as an ASIC, apparently, and those always are quicker to make than traditional chips. Also, the chip is at the “tape out” stage of development, so you can’t go to your favorite Best Buy and get one. Still, according to a testing lab that OpenAI hired, it beats Nvidia Blackwell in a number of ways using different vendor’s LLMs. Key is the “**performance per watt**” or the amount of results you get for a watt of power consumed. That is a big deal in the data center world right now and these numbers are good. Multiple benchmarks, multiple models, low power consumption. All good things and will heat up the competition once they actually have a chip they can put in a computer. Credit: [Semiconductor Analysis](#)

Ukraine to Give Britain Access to Battlefield Data to Train AI

Ukraine will give Britain access to a vast trove of battlefield data collected during the war with Russia, allowing U.K. companies and researchers to use it to train and test artificial intelligence systems. The agreement, signed Monday by Ukrainian President Volodymyr Zelensky and British Prime Minister Andy Burnham, will make the U.K. the first foreign partner to gain access to Ukraine's Avengers AI Labs, a defense platform built around millions of images and other data gathered from the battlefield.

Federal Judge Says DoD Anthropic Supply Chain Designation is Illegal

U.S. District Judge Rita F. Lin granted Anthropic summary judgment on its First Amendment, Fifth Amendment due process, and Administrative Procedure Act (APA) claims against the federal government, rejecting the designation that had followed a months-long dispute between the company and the Trump administration. The administration presented a very weak case for why Anthropic was a supply chain risk and instead, the judge sided with Anthropic’s claim that this was revenge for Anthropic criticizing the government. Credit: [Meritalk](#)

When is Child Porn Legal?

No, this is not a trick question. The prevailing wisdom is never. But, according to the Seventh Circuit Court of Appeals, AI-generated porn of fictional children is legal under the constitution. If this holds, it opens a door that cannot be easily closed. Neither state nor federal laws could make it illegal. The court also said that distributing it is a different matter and that is illegal, so if you create it yourself and don’t distribute it, your perversion is legal, at least according to the seventh circuit. Credit: [Cybernews](#)

130 Companies Warn of Risk of AI

These are, of course, the companies that are integrating AI into their products. Among them are CrowdStrike, Palo Alto Networks, Fortinet, Sentinel One and others. They say that existing technical debt - like excessive permissions and weak authentication - leave these systems exposed and AI is going to run amok if we don't do something. They want, among other things, the government to coordinate and strengthen cyber defenses (does that mean money, human power, regulation or something else). If you are part of critical infrastructure like water, big banking or power, maybe - possibly - the government might help. Likely, however, everyone else is on their own. I would not count on the government to rescue you. Credit: [Metacurity](#)

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.

CMMC is a bit unsettled right now. While some are saying they want to reduce the cost, others are saying it doesn't provide the needed security. And then AI reared its ugly head making security even harder. We don't know what the DoD is going to do, but here are some thoughts on the problem. Details at <https://tcps-blog.com/the-the-cmmc-pause-a-compliance-break-or-a-trust-fall-without-a-net/>

**** REMINDER** NEW SPRS/PIEE System Access Requirements**

This is not a change to CMMC, but PIEE is now requiring that you log in at least every 34 days to keep your account active, so make sure you put this on your recurring task list.

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Ubiquiti in the Spotlight Again

Ubiquiti is patching three max severity security vulnerabilities. They allow a hacker to exploit remotely. Ubiquiti also patched 18 more critical security issues. If you have these devices, now would be a good time to patch them. Credit: [Bleeping Computer](#)

Legislative and Legal Activities

UK Gov Wants to be Able to Ban Risky Tech and Do So in Secret

The British government wants to be able to ban tech vendors on national security grounds from selling to critical infrastructure and bar those companies from saying anything about it. Under the proposed law ministers would not have to publicly designate the vendor as a security risk before banning them. The government would even be able to force companies to remove

existing equipment. They would not even have to tell the vendor that they have been banned. Not exactly transparent, but governments, worldwide, love opacity. Credit: [The Record](#)

Education

CISA Insights From Two “Red Team” Exercises

CISA released an alert this week on two red team exercises. Red teaming is when friendly hackers attempt to compromise a network. In this case, both are critical infrastructure. In one case, the attackers lived in the network undetected. In the other case, they were detected and blocked in less than 20 minutes and while they did compromise the network, the attack was contained. There are lessons to be learned. If you are responsible for the security of your company, this is a must read. Credit: CISA [here](#) and [Bing](#).

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.

Employee Benefits Platform Paylogix Hacked

They say that hackers stole data on tens of thousands of people. LAST YEAR. Information includes what you might expect - date of birth, social security number, benefit information. In some cases, also, credentials, SIGNATURES, banking information, health insurance information, passport and more. Why did this take close to a year? I don't know but we will find out due to the MULTIPLE class actions pending. Credit: [The Record](#)

Workwear Retailer Carhartt Hacked; Loses Data on 12 Million

ShinyHunters claimed they stole double that. I guess you can't trust hackers not to lie. ShinyHunters dumped 50 gig of data in response because, they claimed, Carhartt hired a very unskilled and incompetent negotiator. The demand was initially \$3.3 million, not a lot for Carhartt. The data stolen is pretty vanilla, which is probably why Carhartt was trying to negotiate the price down. Credit: [The Register](#)

Distributed Finance (DeFi) Protocol Moonwell Hit for \$8.7 Million

This is one of the fundamental weaknesses in DeFi protocols. This is more like a pump and dump scheme. Jack up the price of a token, borrow against it and then let the token crash. In the meantime the hacker (who didn't actually “hack” anything”) and his money are long gone. This is the third attack they have had this year and they are still paying back contract holders on an earlier one. This one is more than 4 times the size, so, while unknown, it is likely that everyone gets to take a haircut, meaning (a) the price of the token is down so that is one loss and (b) when you withdraw, you won't get 100% of your tokens out. This is why this stuff is risky. Credit: [The Block](#)

McKesson Discloses Breach of 284 Million

Healthcare and pharmaceutical distribution giant McKesson has disclosed a cybersecurity incident involving unauthorized access to third-party applications and data theft, with the ShinyHunters extortion group claiming it stole 284 million patient data records. The company says they are still investigating and have not disclosed details. Credit: [Bleeping Computer](#)

Hackers shut down UK power plant for four days

While the story was kept quiet for a few days, it did eventually surface. In this case it took them four days to recover power. Since this was not a big power plant, it was not deemed critical, but what if this was a test case (it probably was). Learn more [here](#).

Has OpenAI figured out how to stop hemorrhaging red ink?

At some point the investors are going to want a return on their investment. Maybe OpenAI has figured it out, but you may not like the answer. It involves your data. Learn more [here](#).

The CMMC pause: a compliance break, or a trust fall without a net?

In July the DoD paused third party CMMC assessments. It is totally unclear what their plan is. They say they are concerned about cost, but it seems like they want to add new controls, which certainly won't reduce cost. And, some of the controls they want to add would be very expensive. But, it is important to know that your legal exposure did not pause. In fact, it increased. And then we have AI to deal with. Learn more [here](#).

Security News for the week ending August 28, 2026

This week's news: this is not a surprise - fingerprint security is not foolproof, Microsoft discloses Entra ID flaw, ServiceNow patches three max severity bugs, 130 companies warn of risk of AI and president say communities opposing data centers are making a mistake. Learn more [here](#).

AI is changing everything. A judge just declared that child porn is not illegal if it is AI porn. Do you have your arms around AI? Ignoring it will not make it go away. If you need assistance building your AI governance program, contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663