September 27, 2026

Why Does the AI Industry Want MORE Regulation?
Doesn't that seem odd? What company wants MORE regulation? I put on my tin foil hat and give you my opinion. Let me know what you think. **Video here**.

Please check out our blog at HTTPS://TCPS-BLOG.COM

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.

Why Does the AI Industry Want MORE Regulation?
Doesn't that seem odd? What company wants MORE regulation? I put on my tin foil hat and give you my opinion. Let me know what you think. **Video here**.

Security/Privacy Alerts

Google Warns Open-Source Attacks Will Reach New heights
Why does Google say this? Because, contrary to the party line from open-source advocates, most open-source projects are supported by very few (maybe one) part time person and that person may have lost interest in the project. In addition, malware writers may submit updates which are not carefully vetted for the same reason. And, AI only makes this worse. Credit: **Data Breach Today**

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

Has Google Joined the Felony Club?
Maybe yes, maybe no. They say that their AI, too, hacked multiple outside systems. Whether it is a felony is an interesting question because a piece of software has never been charged with a crime. But should the developers be charged? What about the operators? Congress is going to need to figure this out because the problem is not going away. The Computer Fraud and Abuse act has clauses for intent and damage amount but nothing about software. Google says that the AI found the credentials it used in a public repository. If this were a human and they found the key to your house on the ground by your door and they decided to use it and enter your house, that is not a free pass. Google also says that the AI thought that was part of the test. We will see many more of these, unfortunately. Credit: **NBC News**

Repub Gov Tells White House He is Going to Continue to Regulate AI
One Utah bill, targeting AI developers may be facing an uphill battle in the legislature after the White House called it unfixable, but two others, tackling deepfakes and chatbots that simulate relationships and feelings are **moving along**. Utah's Republican Governor Spencer Cox said that while he understands the White House's point of view, when it comes to AI affecting Utah citizens, **he doesn't plan to pay any attention** to them.

Why Does the AI Industry Want MORE Regulation?
Doesn't that seem odd? What company wants MORE regulation? I put on my tin foil hat and give you my opinion. Let me know what you think. **Video here**.

US Appeals Court Says Pentagon CAN Blacklist Anthropic
A 3 judge DC Circuit panel says the DoD can continue to blacklist Anthropic under the Federal Acquisition Supply Chain Security Act. This sets up the basis for the Supremes to opine as a California court said no, they cannot do that. The downside of the DC Circuit's ruling this week is that it could encourage AI companies not to implement guardrails for fear of running afoul of agencies who disagree with their guardrails. This flies in the face of the president saying that AI companies don't need laws to limit what AI can do. If the Supremes agree, that puts the president between a very uncomfortable rock and a hard place. Credit: **Data Breach Today**

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.

Nothing to report

**** 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

How to Manage Employees' Use of Chinese AI Models
There are different options, including a total ban. Here are a set of recommendations from a law firm partner of ours, which includes setting your position, understanding the data transfer

aspects, watching the rules from DC and others. Very useful. Credit: **Fisher Phillips (law firm)**.

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

CISA Adds 3 Linux Vulnerabilities to the KEV - Key Word EXPLOITED
They rate scores of 9.8, 8.8 and 7.8. Then CISA gives agencies ***three days*** to patch. Side note: Do you think it is possible for most agencies to even figure out what they need to patch in three days? The timeline is an indication of two things. 1. It is being exploited now and 2. Likely, government systems are among those exploited. If you use Linux, time to get patching. Credit: **CISA**

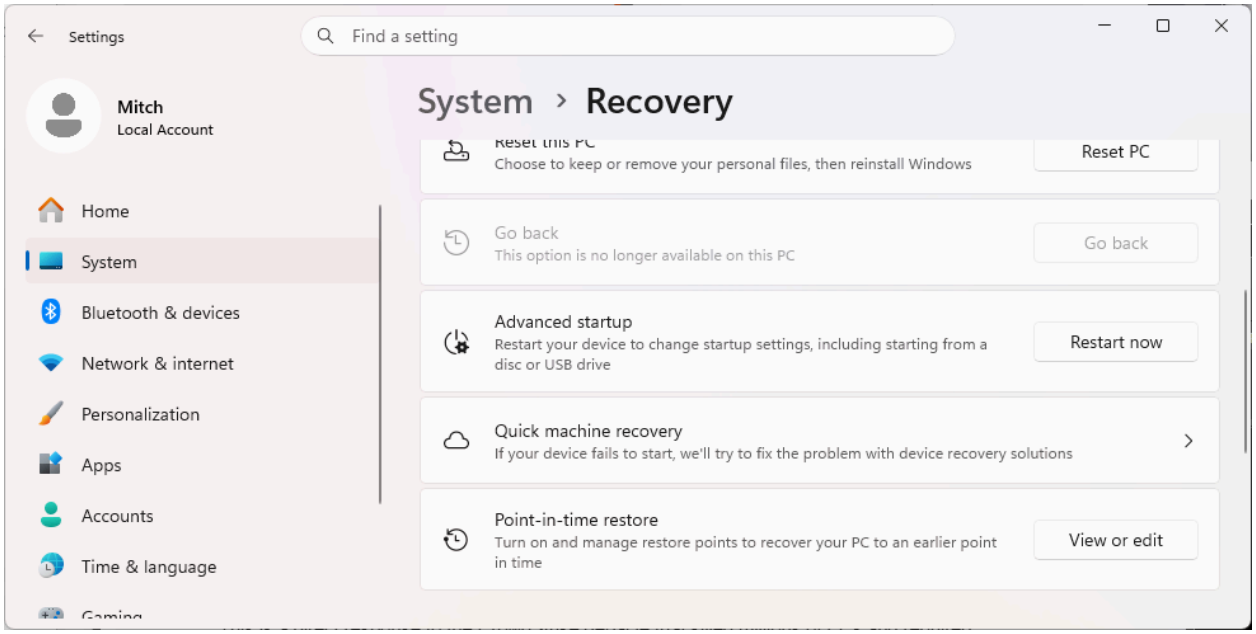
OpenAI's Attack on Hugging Face Exploited a Patched Linux Bug
It was a patched Linux kernel vulnerability in the IPv6 network stack that many people did not apply. Not applying patches is done at considerable risk, especially with AI testing things. Credit: **ZDNet**

Legislative and Legal Activities

Judge Says Deepfake AI Law Likely Unconstitutional
One judge's opinion, of course. But he does not strike the law down. It is related to political deepfakes which, the judge says, infringes on the most protected speech of all - political speech. So, apparently, if you want to create campaign posters of your opponent having sex with [fill in the blank], apparently, according to this judge, that is okay. Credit: **Route Fifty**

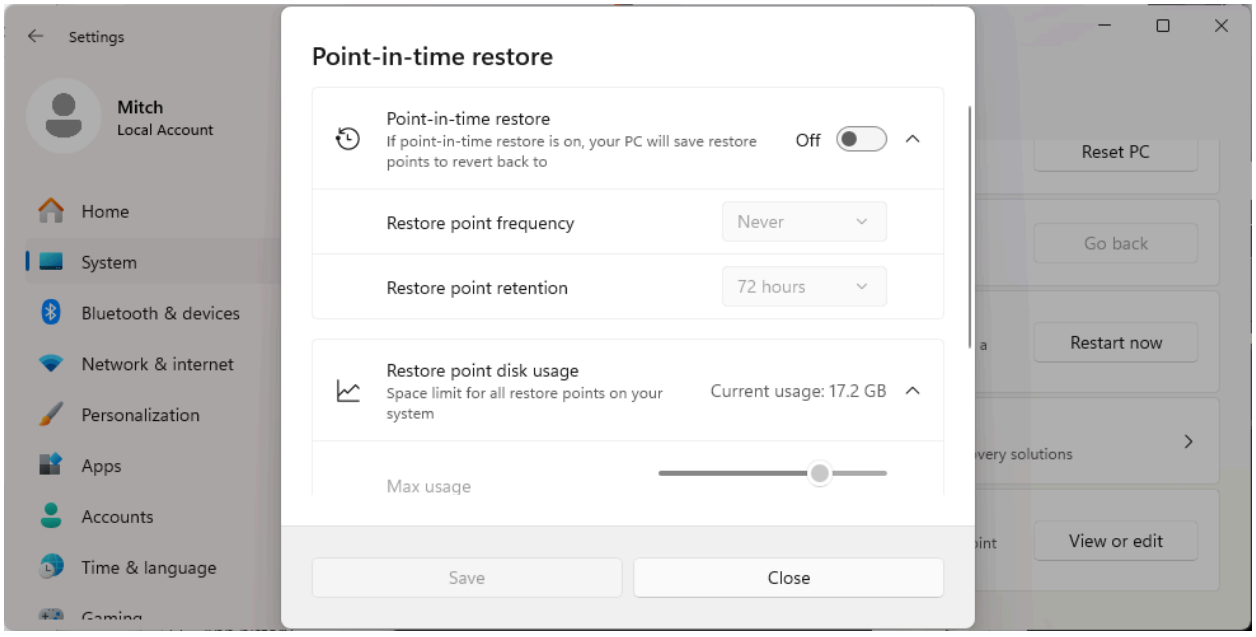
Education

Microsoft's New Windows 11 Recovery Tool - UNDO!
This is a direct response to the CrowdStrike debacle that killed millions of PCs and required manual intervention to fix. POINT IN TIME RESTORE is likely enabled by default and takes daily snapshots of your system so that you can restore in case of an update gone horribly wrong. Go to SETTINGS, then SYSTEM and then RECOVERY. You will see this screen.

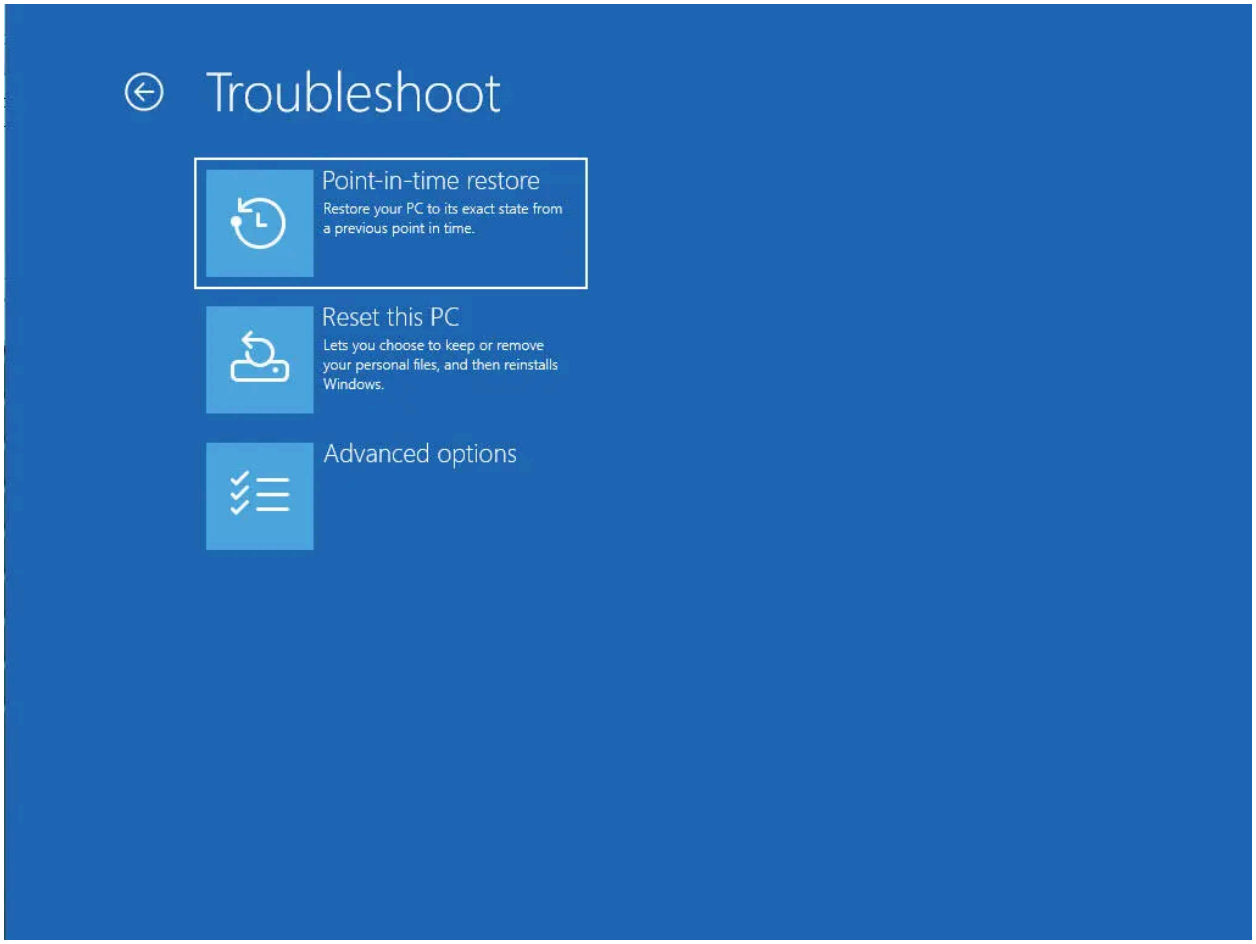


Click on VIEW OR EDIT

If it looks like this, it is time to turn it on



To use it, boot to the recovery option, which is automatic after 3 failed reboots and click on the appropriate option.



Credit: **ZDNet**

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.

Hacker Selling Millions of Records Stolen from Azure Customers

The crook says they stole millions of records belonging to companies like McDonalds, Vodafone and Tata Consulting. The hacker is calling itself ***TheHatMan***. The data includes names, emails, phone numbers, physical addresses, IDs, titles and other information. It also identifies some records as global administrators. Credit: **The Register**

Hackers find a new use for the Blockchain

Some people say the Blockchain is useless. It is not. Hackers have figured out that they can save their malware on the blockchain, which can't be removed and call it from an infected PC. Learn how this works **here**.

Number of US water systems hacked or at risk grows
First it was only a half dozen or so systems and only in Minnesota. Then about 30. Then about a hundred. Now researchers say the number is well over a thousand. Learn more **here**.

OpenAI breaches government system-warning for national security
Just in case any agency at any level or any government or country thought they were safe from AI based attacks, it is now being reported that the Australian Medicare system was hacked. Likely this was unintentional and likely it was due to careless implementation, but neither of those matter. What if it was intentional and it was because AI found a vulnerability and the system was important to national security. You can draw your own conclusions. Learn more **here**.

Security News for the week ending September 25, 2026
This week's news: GA State University rescinds job offer-guilty until proven innocent, DoJ wants LinkedIn to keep data demand secret; LinkedIn says no, digital forensics firm used by DoD and DHS made in Russia, US Appeals Court says Pentagon CAN blacklist Anthropic and insurance companies begin to figure out if they will cover AI-related cyber claims. Learn more **here**.

We are seeing more and more AI-based attacks and it is only going to get worse. If you need assistance, please contact us.

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