

Apr 5, 2026

Quantum Computing and Encryption - I Forgot to Mention One Thing

When I was ranting last week about Q-Day, when quantum computers were powerful enough to break traditional encryption, which Google says will happen by 2029 - I forgot to mention one thing. Besides your bank accounts being unprotected, the entire cryptocurrency world will be toast. And the blockchain - You might as well be writing on it with a number 2 pencil with an eraser on the end. Both of those depend on encryption and cryptographic checksums. Is this guaranteed? No. But are you feeling lucky punk? The crypto folks are working on upgrading to quantum RESISTANT cryptography, but no one thinks that will be quantum PROOF and anything that is already on the blockchain is going to be toast.

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

Quantum Computing and Encryption - I Forgot to Mention One Thing

When I was ranting last week about Q-Day, when quantum computers were powerful enough to break traditional encryption, which Google says will happen by 2029 - I forgot to mention one thing. Besides your bank accounts being unprotected, the entire cryptocurrency world will be toast. And the blockchain - You might as well be writing on it with a number 2 pencil with an eraser on the end. Both of those depend on encryption and cryptographic checksums. Is this guaranteed? No. But are you feeling lucky punk? The crypto folks are working on upgrading to quantum RESISTANT cryptography, but no one thinks that will be quantum PROOF and anything that is already on the blockchain is going to be toast.

So Far Attacks on Tech Companies Have Been Limited to the Middle East



On April 1, Iranian missiles struck the headquarters of Batelco — Bahrain's largest telecommunications company. The facility houses Amazon Web Services infrastructure, and the strike triggered a massive fire, structural damage, and rendered portions of the complex inoperative. Credit: [Breached Company](#)

Microsoft Now FORCES Upgrades to Windows 11

Starting this week Microsoft began forcing users of both Windows Home and Pro that are running Windows 11 24H2 to update to 25H2. This is true even though 24H2 has not yet reached end-of-life (but it will in October). If the PC is managed by your IT department, they will not be forced to upgrade. Credit: [Bleeping Computer](#)

AI Alerts

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

New York Passes Comprehensive AI Safety Law

New York and California are at the forefront of this, but not alone. These two states alone represent 60 million residents. While not as strong, Texas, Colorado, and Utah also have AI safety laws. Together, these states represent almost a third of the US population. 45 states also have some form of anti-deep fake laws. The NY law, called the Responsible AI Safety and Education Act (RAISE), requires large AI platforms to publish their safety protocols and report to

the state within 72 hours qualifying incidents. The initial fine is \$1 million. While the president would like a national AI law, likely by design very weak so that AI companies can do whatever they want, the states seem less inclined to support that. The more states that have their own AI laws, the harder it is going to be for the Republican controlled House and Senate to usurp states rights and pass a weaker national law, but you never know when it comes to politics. Credit: [Morrison Foerster](#)

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.

Q: How can we use AI and still be CMMC compliant?

A: It is possible but you have to make sure that you are doing it correctly (contact us if you need assistance). The safest but most complex solution is to run the LLM in your own CMMC compliant (like GCC High) environment. That way you can control the outcome completely. It is possible to use AI, including CoPilot WHICH IS HOSTED INSIDE GCC/GCC HIGH, but you always need to have policies and procedures. Also, contract language. We can assist you with this.

Q: I have a contract renewal that is coming up at the end of this year. Will that renewal require a third-party (C3PAO) certification?

A: There are no guarantees here, but if the renewal is due after this November there is a good chance that the renewal will require a third-party certification. The question is are you willing to risk not getting the renewal? If the renewal is important then you need to be working on getting certified yesterday because it will take you all of the time between now and then to get this done.

Q: Is there a shortage of CMMC assessors?

A: Not at the moment. Here are the numbers as of Tuesday. 1,074 third-party certified organizations, 103 C3PAO organizations and over 500 C3PAO applicants. 759 Certified assessors PLUS another 484 Lead assessors, so right now, the shortage is in organizations ready to be certified. There are currently only 116 organizations in the process of getting certified. So, I don't think the number of assessors is the tall pole in the tent.

Q: When is CUI not CUI - Take 2!

A: Last week I said it was really weird that the Army is marking all emails as CUI whether they are really CUI or not and I said this is probably not legal or at least in the spirit of the regulation. Ryan Bonner said that absent the CUI tombstone it isn't really CUI. I am not sure that I agree with that, but Ryan is a usually very reliable source. He does not, of course, represent the opinion of the government. That means that if you are using Purview or the like to bounce emails, seeing JUST the letters CUI is probably not the best filter. It will certainly work and if it causes senders to push more email to your enclave that might not be all bad, but it does mean that you may get some non-real-cui mail in your enclave, which is certainly not a compliance problem.

Reference

Nothing to report

Software and Hardware to Check Out

Nothing to report

Important Issues/Patches

Another Fortinet Exploit

This time it is in Fortinet Endpoint Management Server (EMS). The bug allows unauthenticated hackers to execute arbitrary code via specially crafted HTTP requests. FortiClient EMS provides centralized management, deployment, and monitoring for FortiClient endpoint agents across numerous platforms. Credit: [CSO Online](#)

Legislative and Legal Activities

Nothing to report

Education

North Korean Hackers Drained \$285 Million from Drift in 10 Seconds

In fairness, they did set things up in advance, but still, once they pressed the GO button, it only took them a few seconds to make this distributed finance organization's wallet a lot lighter.

Learn how they did it. Credit: [Security Week](#)

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.**

Balancer Labs Shuts after \$110 Million Hack

Last November Balancer, a "defi" app, lost \$110 million to hackers. That caused users to flee which caused the total value locked to plummet from around \$775 million to around \$300 million and continue to decline, now hovering around \$150 million. They have come up with a new legal structure to run it which they think will allow them to dodge the legal liability from losing more than \$100 million dollars of other people's money. Hope you didn't have any contracts with them, but this is the nature of unregulated finance. They will protect themselves, not you.

Credit: [Web 3 Is Going Great](#)

Hackers Claimed to Have Breached Cisco Systems

The hackers, ShinyHunters, claim to have breached Cisco in three different ways including Salesforce, Github and AWS. According to the hackers, the breach includes 3 million Salesforce records which include PII, Github repositories and AWS buckets, along with other corporate data. They have given Cisco until April 3 to pay up. Bleeping Computers say they have reports that the hackers cloned over 300 Github repositories. A portion, they say, belongs to corporate customers including banks, BPOs and US government agencies. NOT GOOD. It is tempting to say that if Cisco can't protect itself, how can we, but in reality, if you have a hundred thousand employees or whatever Cisco has, you have 100,000 points of attack, making protecting the company actually harder. Credit: [Cyber News](#)

Drift Loses \$280 Million to Hackers

The Drift Protocol is a distributed finance (DeFi) trading platform on the Solana blockchain. They are now shy about \$280 million as a result not of a platform bug but rather hackers becoming platform administrators by understanding a weakness in the underlying platform design. They are now trying to recover the stolen funds. Another day another blockchain software hack. When will they learn? Credit: [Bleeping Computer](#)

Will forcing routers to be assembled in the US make them secure?

The short answer is no. The longer answer is there are none made in the USA. Zip. Zero. None. But there are bigger issues besides that. Learn more [here](#).

Axios npm package with 100 million weekly downloads compromised

The package was the victim of a single developer getting compromised and the result is that tens of millions of developers are now at risk of compromise. Learn more [here](#).

Critical Claude bug discovered after code accidentally released

Maybe there is some good out of Claude's mistake in releasing 500,000 lines of source code by mistake. A bug was found by a good researcher and Claude can now fix it. But if it was a hacker who found it, it would not be so good. Learn more [here](#).

Security News for the week ending April 3, 2026

This week's news: Hong Kong just made it a crime to refuse to unlock your phone, California to require AI companies seeking state contracts to meet safety+ rules, hackers leverage Claude Code leak to attack you, Microsoft's LinkedIn is watching you and when tech and the real world collide. Learn more [here](#).

New York and other states have passed AI safety laws. Many of these laws impact your suppliers but others impact users. Either way, you need to understand what the requirements are. If you are not ready for this, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663