

Mar 29, 2026

First, do you know what a Q-Bit is? It is a measure of capability of a quantum computer and, in this case, its ability to crack all existing (RSA) encryption. In 2019 they thought it would take 20 million Q-Bits and that is a long way away. Last year they thought it would only take a million due to better cracking algorithms. Last month researchers figured it would only take 100,000 Q-Bits.

Microsoft, Amazon and Google will be driving when you have to convert. Some things will be backward compatible; many won't. To remind you, the problem is that once someone gets a capable computer, any data (of yours) they saved will be decryptable, so it is in your best interest to convert now. Google says the deadline is now 2029. Credit: [CSO Online](#)

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](mailto: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

Nothing to report

### AI Alerts

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

### Pennsylvania Teens Get Probation for Creating CSAM of Schoolmates

Two Pennsylvania teens used AI to create deepfake nudes of their classmates at Lancaster Country Day School. The teens were 14 at the time. The teens got off very lightly, in my

opinion, since even the possession of CSAM is a felony. They were sentenced to six months of juvenile probation, 60 hours of community services and \$12,000 in restitution. This was the outcome of facing 59 felony charges. They had created deepfake porn of more than 50 students, using the students' Instagram photos as the input. A lawsuit has also been filed against the school for not dealing with the initial Safe2Say alert they got. Credit: [WHTM Lancaster](#)

### **Judge Enjoins Pentagon in Anthropic Case**

A federal judge granted Anthropic's request for a preliminary injunction in the case of the Pentagon calling Anthropic a supply chain risk and ordering federal agencies and all contractors to stop using their software. Judge Rita Lin said "Punishing Anthropic for bringing public scrutiny to the government's contracting position is classic illegal First Amendment retaliation". Stay tuned for more scenes of our next episode. Credit: [CNBC](#)

### **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: What does Stryker Medical attack tell us about CMMC controls?**

**A:** The attack that, we think, wiped 200,000 devices at the company was not due to exploiting some crazy unknown zero-day. It was bad password management and lack of effective MFA. Simple, basic stuff that CMMC is working to get companies to implement. Not all attacks require a genius. In fact, most do not.

### **Q: Iran linked hackers claim to have stolen 375 TB of Data from Lockheed including F35 Prints - is this real?**

**A:** As of the time of writing this Lockheed says that they have seen the reports but are claiming for the moment that they are confident in defensive systems. We shall see how that holds up. The group claims to have copies of the blueprints for the F-35 and other corporate data. Again, we don't know, but I do suspect that this will likely increase the Pentagon's focus on CMMC. Oh, yeah, they want \$400 million in exchange for not selling the blueprints. This is one to watch to see if they are telling the truth and what the Pentagon's response is, if it is true. One plausible possibility is that this is actually a supply chain attack. The F-35 program has well over a thousand suppliers, many of whom might have access to shared document repositories.

### **Q: Is there a hard deadline of November 2026 for CMMC compliance?**

**A:** Not in the way you may be thinking. That date is the start of CMMC phase 2 when the appropriate (key word) CMMC requirements are going to start being included in NEW contracts. Appropriate could be Level 1, Level 2 (self) or Level 2 (C3PAO), depending on what information you have as part of the contract. For anyone getting a new contract that contains CONTROLLED TECHNICAL INFORMATION (which is a high percentage of contracts), that means that you likely will have to have a third party CMMC certification in order to be awarded the contract. For most companies from start to certification, the timeline is likely 12 months or more, so if you think that requirement is going to be yours and you have not started your CMMC journey, you are definitely behind and you should contact us right away.

### **Q: When is CUI not CUI or is UII?**

**A:** The services are definitely having some problems dealing with CUI. The Army sent out a message saying that they mark all outgoing messages CUI, whether they are or not and just because they mark an email CUI doesn't mean it is CUI. The Navy created a new marking, UUI, meaning Uncontrolled Unclassified Information (which does not exist) and is controlled to only be delivered to .MIL addresses. The Army claims "the presence of an automated CUI banner does not, by itself, indicate that the message or attachments contain CUI". Assuming that is even legal, I am not sure how a contractor is to determine what is and is not CUI. In fact, a contractor is not legally allowed to downgrade CUI. If you are in this situation contact us for our recommendation for dealing with this.

## **Reference**

### **How Many Q-Bits Do You Need to Break All Traditional Encryption?**

First, do you know what a Q-Bit is? It is a measure of capability of a quantum computer and, in this case, its ability to crack all existing (RSA) encryption. In 2019 they thought it would take 20 million Q-Bits and that is a long way away. Last year they thought it would only take a million due to better cracking algorithms. Last month researchers figured it would only take 100,000 Q-Bits.

Microsoft, Amazon and Google will be driving when you have to convert. Some things will be backward compatible; many won't. To remind you, the problem is that once someone gets a capable computer, any data (of yours) they saved will be decryptable, so it is in your best interest to convert now. Google says the deadline is now 2029. Credit: [CSO Online](#)

## **Software and Hardware to Check Out**

### **Apple Dips it Toes into the Business World**

Apple started out as a computer company but then, with iPhones, it turned into a consumer marketing company, selling other people's stuff and getting a cut of the money. I suspect that growth has become a challenge both because the market is getting saturated and there are other competitors. SO, they are trying to get into the business world to compete with Microsoft and Google. Apple Business will be available next month. It includes a device management software and bring your own domain and a few other things. For now, it is free. It is only really useful if your company is only a Mac shop as, unlike Google and Microsoft, it has no cross platform capability. This is likely because they don't have the internal expertise to do that. I would say that this is good for fully Mac shops, but for anyone else, probably not. Details at [Apple Insider](#)

## **Important Issues/Patches**

### **Citrix NetScaler Hole Similar in Severity to CitrixBleed2**

The bug allows an unauthenticated remote attacker to leak potentially sensitive information from the Netscaler's memory. Companies that use Citrix Netscalers need to patch now. In the CitrixBleed attack unauthenticated attackers could steal credentials. Once you have credentials, it is all over. Credit: [CSO Online](#)

## **Legislative and Legal Activities**

### **Google and Meta Found Liable by LA Jury for Addiction**

A jury found Google and Meta liable for social media addiction. This could impact thousands of other pending cases, so you can guarantee this will get appealed to the Supremes. IF this stands and that is a big if, the social media companies will be liable for billions. The jury awarded the victim \$3 million in compensation and another \$3 million in punitive damages.

Credit: [MSN](#)

### **Meta Loses Addiction Trial in New Mexico, Fined \$375 Million**

It has not been a good week for social media. This was the first of two verdicts that they didn't like. These trials have taken a different approach to get around the Section 230 immunity defense that shields social media from being liable for user submitted content. Instead, it focuses on the algorithms that keep people scrolling and that is NOT something that is protected under the Communications Decency Act Section 230. Hence they lost. But mostly, Zuckerberg, Musk and others are worried about the 1,000 lawsuits (and more being filed) that will come behind these and use these as ammunition in their attacks against the addictive properties of social media. Credit: [My Privacy Blog](#)

### **Dutch Court Fines Musk 100,000 Euros a Day for Failing to Stop CSAM Creation**

While the court only has jurisdiction in the Netherlands, if Musk ignores the ruling it is likely that it will not play well in the ongoing investigations and litigation in the EU and UK. It is estimated that 3 million such pictures, including non-consensual child nudity, were created in just 11 days after the feature was turned on. Credit: [Politico](#) and [MSN](#)

## **Education**

### **Why Did OpenAI Kill Sora and What Does it Mean?**

I think we are going to see a lot of crashing and burning. Sora was costing OpenAI \$15 mil a day. And it allowed users to easily make brand killing content - copyright theft and misinformation for starters. At scale. As the regulations tighten the noose around the platforms, they may be at a realization that they need to clean up their acts. Learn more [here at Cybernews](#)

## **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.**

### **DoJ Confirms Iran Hacked FBI Director Patel's Personal Gmail - Stole 836 Meg of Data**

It is important to note that this was his PERSONAL email, not the FBI's email. 8 days ago he goaded Iran. Now they have published his personal photos, documents and mail. Purely to embarrass him. The 836 megabytes is after compressing it, so it is a lot more in reality. I am not clear how much harm this will do (were there nude selfies in there?) but it certainly is embarrassing both to him personally and to the Bureau. Credit: [Breached Company](#)

### **Blueleaks 2.0 Exposes Millions of Law Enforcement Anonymous Tips**

This is the type of leak that can get people killed. These are anonymous tips about crimes like the type that get submitted to Crimestoppers. With names, contact information, etc. Organizations that use the system include the Air Force, DoJ, IRS criminal investigations. The leak includes this comment: ***“Remember folks, don't do the dirty work for the pigs.*”**

***Investigating crime is their job, not yours. They don't care about you, they want convictions and prisoners to fuel the for-profit prisons.*** Credit: [DDoS Secrets](#)

### **HackerOne, Mazda, Infinite Campus and Dutch Ministry Hit by Data Breach**

All four breaches target the organization's employees. The Dutch breach was detected by the ministry. Infinite Campus acknowledged the breach but not how much data was stolen. It appears this MAY BE another Salesforce breach, where the hackers compromised the victim organization's credentials rather than hacking Salesforce. The HackerOne breach may be related to the Navia breach I reported about last week. The Mazda leak is small and related to some warehouse management software that was compromised. The sheer number of these breaches is amazing. Credit: [Hackread](#)

-----

### **Department of Energy Announces Cybersecurity Pipedream**

They announced a five year plan to dramatically reduce the cyber attacks on private companies in the energy sector. With no funds. And no regulations. And no laws. DoD learned the hard way that this doesn't work and has been working very hard to fix that with a massive new regulation called CMMC (well, actually, Congress forced them to do that in the NDAA, but that is another story). DoE has not explained how this is going to work. Learn more [here](#).

### **FCC Bans Import of NEW Consumer Routers Not Made in the USA**

This is a great idea but, again, with no plan. There are zero consumer routers made in the USA. And just like we are seeing with PC memory (those companies just said the hell with consumer memory; we are going to ONLY sell to companies), this is likely what we are going to see with routers. There is a loophole in the regulation that doesn't exactly say that if you get on the good side of the administration you can get an exception, but that is what it strongly implies. We know how you get on the administration's good side. Learn more [here](#).

### **Chinese Hackers STILL Deep Inside US Telecoms**

These sleeper cells did not get extracted when we admitted to Salt Typhoon in 2024 according to Rapid 7. The security firm says the Chinese are still deeply embedded in our critical telecom infrastructure. Learn more [here](#).

### **Security News for the week ending March 27, 2026**

This week's news: Jeffrey Epstein's schedule now available online, British lawmaker asks why Meta/Google/X didn't take down ruinous deep fake, how many Q-Bits do ya need, FBI admits under oath it is tracking you and doesn't need a warrant and Gen AI has turned fraud into a \$400 billion + business. Details [here](#).

***I am repeating this multiple times this week. Quantum computing will allow hackers to decrypt anything you have encrypted that they were able to save. More importantly, the timeframe in which they are going to be able to do that keeps getting earlier. It was 2035. Now it is 2029. It will likely get sooner. If you don't have a plan for dealing with it, assume you no longer have any secrets. If you need assistance, please contact us.***

**Mitch**

[www.CyberCecurity.com](http://www.CyberCecurity.com)

[www.TurnkeyCybersecurityAndPrivacySolutions.com](http://www.TurnkeyCybersecurityAndPrivacySolutions.com)

[Mitch@CyberCecurity.com](mailto:Mitch@CyberCecurity.com)

720-891-1663