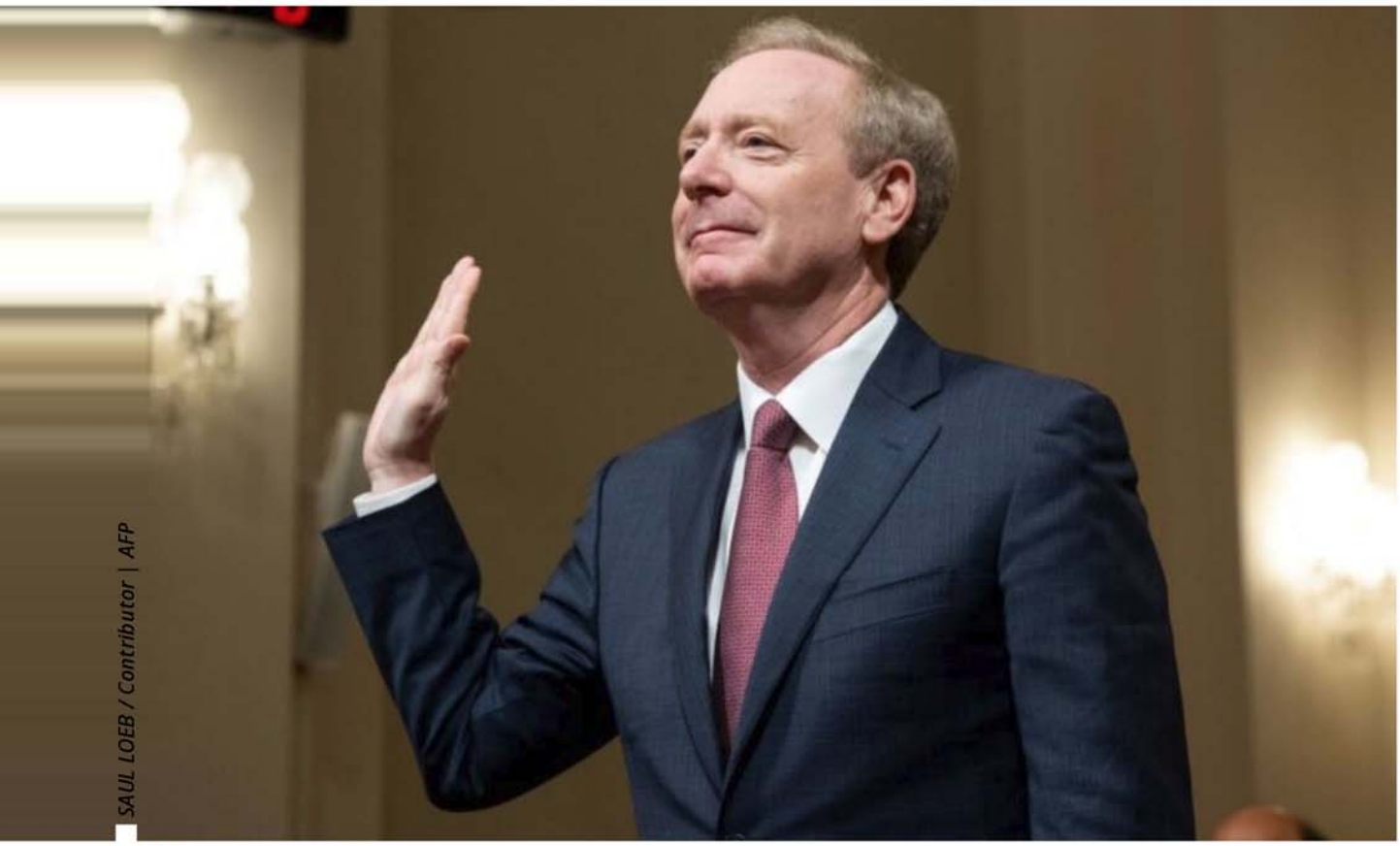
"DO BETTER" —

Microsoft in damage-control mode, says it will prioritize security over AI

Microsoft CEO Satya Nadella is now personally responsible for security flaws.

ASHLEY BELANGER - 6/13/2024, 10:38 PM



SAUL LOEB / Contributor | AFP

Enlarge / Brad Smith, vice chairman and president of Microsoft, is sworn in before testifying about Microsoft's cybersecurity work during a House Committee on Homeland Security hearing on Capitol Hill in Washington, DC, on June 13, 2024.

Microsoft is pivoting its company culture to make security a top priority, President Brad Smith testified to Congress on Thursday, promising that security will be "more important even than the company's work on artificial intelligence."

Satya Nadella, Microsoft's CEO, "has taken on the responsibility personally to serve as the senior executive with overall accountability for Microsoft's security," Smith told Congress.

His testimony comes after Microsoft admitted that it could have taken steps to prevent two aggressive nation-state cyberattacks from China and Russia.

According to Microsoft whistleblower Andrew Harris, Microsoft spent years ignoring a vulnerability

while he proposed fixes to the "security nightmare." Instead, Microsoft feared it might lose its government contract by warning about the bug and allegedly downplayed the problem, choosing profits over security, ProPublica reported.

This apparent negligence led to one of the largest cyberattacks in US history, and officials' sensitive data was compromised due to Microsoft's security failures. The China-linked hackers stole 60,000 US State Department emails, Reuters reported. And several federal agencies were hit, giving attackers access to sensitive government information, including data from the National Nuclear Security Administration and the National Institutes of Health, ProPublica reported. Even Microsoft itself was breached, with a Russian group accessing senior staff emails this year, including their "correspondence with government officials," Reuters reported.

"We acknowledge that we can and must do better," Smith told Congress today, according to his prepared written testimony. "As a company, we need to strive for perfection in protecting this nation's cybersecurity. Any day we fall short is a bad day for cybersecurity and a terrible moment at Microsoft."

To reinforce the shift in company culture toward "empowering and rewarding every employee to find security issues, report them," and "help fix them," Smith said that Nadella sent an email out to all staff urging that security should always remain top of mind.

"If you're faced with the tradeoff between security and another priority, your answer is clear: Do security," Nadella's email said. "In some cases, this will mean prioritizing security above other things we do, such as releasing new features or providing ongoing support for legacy systems." To ensure everyone's on board, Microsoft has also started tying executives' salary to meeting security goals.

Microsoft to adopt all the government's recommendations

Smith was the only witness testifying at a House Committee on Homeland Security hearing, titled, "A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security."

He told Congress that Microsoft was following through on all 16 recommendations that the Cyber Safety Review Board (CSRB) made in a report that "identified a series of Microsoft operational and strategic decisions that collectively points to a corporate culture that deprioritized both enterprise security investments and rigorous risk management."

As part of those obligations, Microsoft has committed to stop charging for key security-related features like more granular logging that the CSRB said should be a core part of their cloud service. (Last July, Microsoft started shifting that culture by expanding cloud logging accessibility and flexibility to give customers "access to wider cloud security logs" at no additional cost.)

Smith also said that Microsoft was "pursuing new strategies, investing more resources, and fostering a stronger cybersecurity culture." That includes adding "another 18 concrete security objectives" beyond the CSRB recommendations and "dedicating the equivalent of 34,000 full-time engineers to what has become the single largest cybersecurity engineering project in the history of digital technology," Microsoft's Secure Future Initiative (SFI).

Microsoft also beefed up its security team, Smith said, adding "1,600 more security engineers this fiscal year" and planning to "add another 800 new security positions" in the next fiscal year.

Additionally, the company's Chief Information Security Officer (CISO) will now run an office with senior-level deputy CISOs "to expand oversight of the various engineering teams to assess and ensure that security is 'baked into' engineering decision-making and processes."

Smith described the SFI as "a multiyear endeavor" focusing all of Microsoft's efforts developing products and services "on achieving the highest possible standards for security." He warned that online threats are always evolving but said that Microsoft was committed to grounding projects in core cybersecurity tenets that would prioritize security in product designs and ensure that protections are never optional and always enabled by default.

This initiative is part of Microsoft's plan to win back trust after Smith and Microsoft previously did not seem to accept full responsibility for the Russian cyberattack. In 2021, Smith told Congress that “there was no vulnerability in any Microsoft product or service that was exploited” in that cyberattack, while arguing that "customers could have done more to protect themselves," ProPublica reported.

In an exchange with Senator Marco Rubio (R.-Fla.), Smith specified that customers could have paid for "an antivirus product like Microsoft Defender and securing devices with another Microsoft product called Intune," ProPublica reported.

Now, Smith told Congress Thursday, "Microsoft accepts responsibility for each and every one of the issues cited in the CSRB’s report. Without equivocation or hesitation. And without any sense of defensiveness."

Page: 1 2 Next →

READER COMMENTS 105

ASHLEY BELANGER
Ashley is a senior policy reporter for Ars Technica, dedicated to tracking social impacts of emerging policies and new technologies. She is a Chicago-based journalist with 20 years of experience.

Reader Comments (105)

View comments on forum

1 2 3 Next ›

Sort by date Sort by votes

Nilt *Ars Legatus Legionis* 18y 20,150

Popular

"Personally responsible" huh? I'll buy that when he gets canned or this guy is charged with lying to Congress.

216 (221 / -5) Yesterday at 4:41 PM

D

deus01 *Ars Praefectus* 10y 3,184

Popular

It's a good thing microsoft didn't just recently announce any AI features that are a security nightmare or anything

328 (330 / -2) Yesterday at 4:41 PM

Paulie *Ars Tribunus Militum* 21y 1,514

Popular

KEK. LMAO even.

28 (40 / -12) Yesterday at 4:43 PM

B

bignick243 *Wise, Aged Ars Veteran* 7y 130

Popular

I wonder if this had anything to do with the total recall of recall.

112 (112 / 0) Yesterday at 4:45 PM

A

akw0088 *Smack-Fu Master, in training* 3y 67

Popular

Southpark We're sorry gif

59 (61 / -2) Yesterday at 4:45 PM

M

Maton *Smack-Fu Master, in training* 2y 69

Popular

Every time there is a security incident, Microsoft should be required to invest $1,000,000 into its on-premise products. That would really be punishment for Nadella.

96 (96 / 0) Yesterday at 4:45 PM

Popular

VaireWeaver *Ars Centurion* 7y 371

What's funny to me is that they seem shocked by the blowback. Tells me they have zero people paying attention to, or interacting with, their customers. They are only paying attention to the wall street hype trains.

158 (161 / -3) Yesterday at 4:45 PM

Popular

Podginator *Ars Centurion* 8y 246

It is actually insulting for him to claim he is personally responsible. Absolutely insulting.

152 (155 / -3) Yesterday at 4:46 PM

Popular

ArsScene *Ars Centurion* 2y 331

i wonder how much these security "initiatives" will cost relative to the costs associated with the ongoing "ai" initiative. that's a metric of relative importance.

54 (54 / 0) Yesterday at 4:46 PM

Popular

Minty Beets *Smack-Fu Master, in training* 2y 53

> Satya Nadella, Microsoft's CEO, "has taken on the responsibility personally to serve as the senior executive with overall accountability for Microsoft's security," Smith told Congress.

Personally, as in "Here's Satya's home address to send bills and lawsuits?"

105 (108 / -3) Yesterday at 4:46 PM

Popular

bignick243 *Wise, Aged Ars Veteran* 7y 130

> VaireWeaver said:

> What's funny to me is that they seem shocked by the blowback. Tells me they have zero people paying attention to, or interacting with, their customers. They are only paying attention to the wall street hype trains.

Kinda sounds like a certain airplane manufacturer...or pretty much any corporation these days.

102 (104 / -2) Yesterday at 4:47 PM

Popular

murixbob *Smack-Fu Master, in training* 2y 20

Given the actually history behind the saml / AD FS issue, they clearly don't give any fucks about security and will likely continue to give none. Not until actual law is put in place that puts companies and CEOs / CSOs criminally on the line.

68 (69 / -1) Yesterday at 4:49 PM

Popular

UserIDAlreadyInUse *Ars Praefectus* 11y 3,586

They'll do the right thing...when forced to do the right thing. Where on earth are companies like Microsoft finding sociopaths for the upper executive levels? Is there, like, an agency that specializes in recruiting self-serving, antisocial tendencies or what?

60 (61 / -1) Yesterday at 4:50 PM

Popular

Callias *Ars Praetorian* 11y 546

Technically, as the CEO and an officer of the corporation, he already had personal accountability so I'm not sure I see this as anything other than blowing warm smoke up the arses of customers and shareholders.

It's not like he's actually going to be doing any of the work, signing off on new code, change control forms, etc. So what actually is this saying? On the day-to-day level?

96 (98 / -2) Yesterday at 4:53 PM

Popular

UserIDAlreadyInUse *Ars Praefectus* 11y 3,586

> Callias said:
>
> Technically, as the CEO and an officer of the corporation, he already had personal accountability so I'm not sure I see this as anything other than blowing warm smoke up the arses of customers and shareholders.
>
> It's not like he's actually going to be doing any of the work, signing off on new code, change control

> forms, etc. So what actually is this saying? On the day-to-day level?

"Can we push to prod?"
"No, not until Nadella approves the latest commits."

104 (105 / -1) Yesterday at 4:55 PM

Popular

yippiekayakotherbuckets *Ars Centurion* 1y 304

Chairman of the committee, I'm afraid I can't recall.

27 (28 / -1) Yesterday at 4:58 PM

Popular

Sajuuk *Ars Tribunus Angusticlavius* 10y 9,220

> UserIDAlreadyInUse said:
>
> They'll do the right thing...when forced to do the right thing. Where on earth are companies like Microsoft finding sociopaths for the upper executive levels? Is there, like, an agency that specializes in recruiting self-serving, antisocial tendencies or what?

If I remember correctly a number of studies have shown that the "dark triad" is statistically over-represented in management and leadership positions.

Why? Well, because those are the traits we incentivize for when it comes to making billions of dollars at the expense of anything and everything else.

73 (73 / 0) Yesterday at 4:59 PM

Popular

MagicDot *Ars Scholae Palatinae* 10y 722

> ...while lawmakers weigh whether the cloud service provider can be trusted with safeguarding national security.

LOL - no for-profit organization should ever be trusted with national security.

43 (48 / -5) Yesterday at 4:59 PM

randomcat *Ars Tribunus Militum* 5y 2,867

At least this gives something solid for well-intentioned MS employees to point to when they bring up issues or suggest security improvements. "Yeah, security's great, we value security and everything, blah blah blah.... but seriously, we actually do or we'll lose specific contracts."

10 (10 / 0) Yesterday at 5:05 PM

Popular

jhodge *Ars Tribunus Angusticlavius* 13y 7,896

I read this:

"In some cases, this will mean prioritizing security above other things we do, such as releasing new features or providing ongoing support for legacy systems."

...and translate it to:

"This gives us the perfect excuse to push customers from on-prem to Azure."

Maybe I'm just cynical, but I think MS would absolutely love it if everyone worked off an Azure "Cloud PC" talking to MS365 service and Azure infra all in the name of security.

58 (58 / 0) Yesterday at 5:05 PM

Popular

yippiekayakotherbuckets *Ars Centurion* 1y 304

> MagicDot said:
>
> LOL - no for-profit organization should ever be trusted with national security.

I'll never dispute that profit is a bad motivator, but almost everything DoD and civilian government agencies use is produced by a for-profit company, apart from free open source software. Jets, tanks, satellites, network gear, laptops, radios, ammunition, everything. There just isn't a mechanism in most countries to produce things by non-profit organizations.

Last edited: Yesterday at 5:11 PM

44 (47 / -3) Yesterday at 5:05 PM

Popular

JoeJohnJackson *Wise, Aged Ars Veteran* 1y 151

> Microsoft CEO Satya Nadella is now personally responsible for security flaws.

So he'll personally recompense anyone affected by the security flaws, lose stock options or be fired over the next security flaws? If not, how exactly is he taking any responsibility other than some empty statement saying he does?

Last edited: Yesterday at 5:11 PM

51 (51 / 0) Yesterday at 5:06 PM

JoeJohnJackson *Wise, Aged Ars Veteran* 1y 151

> yippiekayakotherbuckets said:
>
> is produced by a for-profit company, apart from open source software

Since when do for-profit companies not produce open source software?

I don't remember Red Hat, IBM, Intel, AMD, Novell, etc. being non-profit companies. 🤔

-3 (13 / -16) Yesterday at 5:09 PM

Popular

omf *Ars Scholae Palatinae* 22y 680

I remember the last time Microsoft very publicly made security their number one priority. It seemed to last a year or two before they went back to very obviously prioritizing profit over all else.

78 (78 / 0) Yesterday at 5:11 PM

yippiekayakotherbuckets *Ars Centurion* 1y 304

> JoeJohnJackson said:
>
> Since when do for-profit companies not produce open source software?
>
> I don't remember Red Hat, IBM, Intel, AMD, Novell, etc. being non-profit companies. 🤔

Edited

-15 (1 / -16) Yesterday at 5:11 PM

Popular

mmorales *Ars Praetorian* 21y 404

> UserIDAlreadyInUse said:
>
> They'll do the right thing...when forced to do the right thing. Where on earth are companies like Microsoft finding sociopaths for the upper executive levels? Is there, like, an agency that specializes in recruiting self-serving, antisocial tendencies or what?

Yes, they're called Executive Search Firms and they are very well compensated for finding people with these traits.

41 (41 / 0) Yesterday at 5:11 PM

JoeJohnJackson *Wise, Aged Ars Veteran* 1y 151

> yippiekayakotherbuckets said:
>
> Edited

Your edit is still false. All those for-profit companies I mention have all created and contributed GPL code to quite a few projects which are FOSS. Unless you have some alternate defintion of FOSS? 🤔

-1 (8 / -9) Yesterday at 5:14 PM

yippiekayakotherbuckets *Ars Centurion* 1y 304

> JoeJohnJackson said:
>
> That's still false. All those companies I mention produce(d) GPL code which is FOSS.

Ease up man, this is a minor point in my comment.

-4 (7 / -11) Yesterday at 5:15 PM

forkspoon *Ars Centurion* 14y 339

They're mostly saying a lot of great things in this planned cultural shift. Very different than when shit was openly hitting the fan.

Makes me wonder if MS have recently been assured that if they take internal financial responsibility, they won't face legal responsibility. That or someone (maybe in USG) spoke softly with a big stick? In any event, it's generally a safe bet to assume the execs won't wind up in court for their own gross negligence.

9 (9 / 0) Yesterday at 5:15 PM

UserIDAlreadyInUse *Ars Praefectus* 11y 3,586

> mmorales said:
>
> Yes, they're called Executive Search Firms and they are very well compensated for finding people with these traits.

*Real*ly....I honestly would not have imagined that to be the case.

6 (8 / -2) Yesterday at 5:16 PM

Popular

Danellicus *Ars Scholae Palatinae* 12y 712

> Maton said:
>
> Every time there is a security incident, Microsoft should be required to invest $1,000,000 into its on-premise products. That would really be punishment for Nadella.

$1M is sofa change for Microsoft. This kind of a breach-leak should have real financial penalties, starting with B. Or else somebody like Brad Smith or Satya Nadella can see the inside of a Club Fed for 6 months. Otherwise they just pay the penalty and move on.

41 (41 / 0) Yesterday at 5:16 PM

Popular

Maestro4k *Ars Scholae Palatinae* 14y 1,163

> UserIDAlreadyInUse said:
>
> They'll do the right thing...when forced to do the right thing. Where on earth are companies like Microsoft finding sociopaths for the upper executive levels? Is there, like, an agency that specializes in recruiting self-serving, antisocial tendencies or what?

In addition to what mmorales said, sociopaths tend to move up the ladder quickly in most businesses, because that's what businesses select for: unethical assholes who'll put making money over everything else.

35 (35 / 0) Yesterday at 5:17 PM

charliebird *Ars Tribunus Militum* 14y 1,878

Microsoft claims to pivot to security. It must be a day that ends in 'y'.

14 (15 / -1) Yesterday at 5:19 PM

Popular

dlux *Ars Legatus Legionis* 18y 25,337

For all you youngsters out there, Microsoft went through all this before in the early 2000s when Windows was getting hammered almost weekly with big security breaches. Gates finally had to admit the scale of the problem and turned all their resources inward to tackle this deeply-rooted problem.

It's good to know they learned so much from that period.

79 (79 / 0) Yesterday at 5:22 PM

vought1221 *Ars Praetorian* 16y 468

What the hell is a "senior level deputy CISO"?

Jesus. They're just making shit up at this point to keep those sweet, sweet services contracts coming.

19 (19 / 0) Yesterday at 5:25 PM

Popular

fuzzyfuzzyfungus *Ars Tribunus Angusticlavius* 11y 9,403

> deus01 said:
>
> It's a good thing microsoft didn't just recently announce any AI features that are a security nightmare or anything

It seems specifically worth noting that 'recall' happened *after* "If you're faced with the tradeoff between security and another priority, your answer is clear: Do security," Nadella's email said.

Which opens a fun game of "completely for show? Unable to actually tackle dysfunctional culture? Or 'that is them prioritizing security, god help us.'?"

37 (37 / 0) Yesterday at 5:26 PM

MVCarpenter *Smack-Fu Master, in training* 22h 1

Curious if anyone else thinks that all that MS Recall BS is related to the rise in employee surveillance.

Ars Tech Article for Reference: "Simulation of keyboard activity" leads to firing of Wells Fargo employees

Basically MS building in all that recall crap so that user activity can be surveyed.

I didn't see anywhere that recall info could be accessed by 'network admins' or anything like that.... buuuuut I wonder.

Also, software like Hubstaff -- makes me ill just thinking about it.

13 (14 / -1) Yesterday at 5:26 PM

volcano.authors *Smack-Fu Master, in training* 6y 72

Let me know when any of the large orgs, you know which ones, when they suffered due to Microsoft's continuing anti-social behavior, pivoted to any of the other options?

Vote with your wallet, all you smart guys in suits in the government and in industry.

The same government who, through DARPA, can fund a whole new initiative, can change the industry completely. Don't act like you can't do a thing except make a big show of hauling Satya onto the carpet, and questioning him.

Fool me once, shame on you. Fool me twice, shame on... well, you know.

11 (11 / 0) Yesterday at 5:28 PM

Popular

cyloncat *Smack-Fu Master, in training* 6m 4

I guess they've forgotten about the "Trustworthy Computing" initiative, when back in 2002 Bill Gates emailed all employees and called on them to deliver products that are "as available, reliable, and secure as standard services such as electricity, water services, and telephony." Microsoft actually cleaned up their act on security, at least for a while.

31 (31 / 0) Yesterday at 5:40 PM

1 2 3 Next ›

You must log in or register to reply here.

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

Thousands of servers infected with ransomware via critical PHP vulnerability

Meta halts plans to train AI on Facebook, Instagram posts in EU

Retired engineer discovers 55-year-old bug in *Lunar Lander* computer game code

Apple punishes women for same behaviors that get men promoted, lawsuit says

Tesla investors sue Elon Musk for diverting carmaker's resources to xAI

Huge telehealth fraud indictment may wreak havoc for Adderall users, CDC warns

To kill the competition, bacteria throw pieces of dead viruses at them

How the "Nutbush" became Australia's unofficial national dance

STORE
SUBSCRIBE
ABOUT US
RSS FEEDS
VIEW MOBILE SITE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox. Sign me up →