Carl Szabo
Vice President & General Counsel, NetChoice
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

A CASCADE OF SECURITY FAILURES: ASSESSING MICROSOFT's CYBERSECURITY SHORTFALLS AND THE IMPLICATIONS FOR HOMELAND SECURITY

Letter for the Record

June 7, 2024

Dear Chairman Green, Ranking Member Thompson, and members of the Committee on Homeland Security:

NetChoice[1] is a trade association of leading e-commerce and online companies promoting the value, convenience, and choice of internet business models. Our mission is to make the internet safe for free enterprise and for free expression.

We work to promote the integrity and availability of the global internet and are significantly engaged in issues in the states, in Washington, and in international internet governance organizations.

We commend the House Committee on Homeland Security for holding a hearing with Brad Smith, Vice Chair and President of Microsoft, about "A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security."

Summary

For years, flaws in Microsoft's approach to cybersecurity have enabled devastating cybersecurity attacks that have compromised the public and private sectors alike. The U.S. Department of Homeland Security Cyber Safety Review Board's (CSRB) recent report, "Review of the Microsoft Online Exchange Incident from Summer 2023,"[2] draws long overdue attention to Microsoft's persistent and severe security shortcomings.

Microsoft poses an especially acute national security risk given it has a dominant 85 percent market share in the U.S. government's productivity software market,[3] which makes the government dependent

[1] NetChoice is a trade association of e-Commerce and online businesses, at www.netchoice.org The views expressed here do not necessarily represent the views of every NetChoice member company.
[2] Review of the summer 2023 Microsoft Exchange online intrusion, CISA (Mar. 20, 2024), https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf
[3] Monoculture and market share: The state of communications and collaboration software in the US government (Sept. 21, 2021), https://omdia.tech.informa.com/-/media/tech/omdia/marketing/commissioned-research/pdfs/monoculture-and-market-share-the-state-of-communications-and-collaboration-software-in-the-us-government-v3.pdf?rev=8d41cc2d16de491b9f59d2906309fdaa

on Microsoft products including Outlook email, Word, Excel, Teams instant messaging, and the Azure cloud platform.

As you prepare for this hearing, we kindly ask that you consider Microsoft's recent commitment to put security "above all else" against their business, past commitments and priorities. A sober look at the facts shows that we simply cannot trust Microsoft to do better.

Insecure Monopolist

Recent reports that the U.S. Department of Defense is doubling down on Microsoft's insecure software[4] reveal a disturbing fact: Microsoft has locked in federal agencies and faces little competition.[5] Increasing competition for federal contracts and diversity among federal IT vendors will do more to improve Microsoft's cybersecurity than its executives' commitments to do better.

Today, the overwhelming reliance on Microsoft software has resulted in an IT "monoculture" across government. This creates a single attack surface for hackers and a single point-of-failure during outages that leaves the U.S. government unnecessarily vulnerable to cybersecurity threats.

Just last year, Microsoft's cyber defenses failed on two separate occasions to stop foreign adversaries from accessing its networks and compromising government data. These incidents include last summer's attack by Chinese hackers—the focus of the CSRB report—as well as Russia-sponsored Nobelium's breach of Microsoft corporate systems, which granted the hackers access to federal agencies' emails with company executives.[6]

And yet, despite these security concerns, the U.S. government continues to award Microsoft new federal contracts because it has become dependent on the company. For example, in the seven weeks following the disclosure of last summer's Chinese hack, Microsoft was awarded five contracts by the Department of Defense worth a combined $45 million.[7] [8] [9] [10] [11]

Microsoft has no incentive to improve the security of its products because it faces no real competition for public sector contracts and no financial consequences for providing the government with insecure products. Instead, it relies on restrictive licenses to make it difficult and expensive for customers to switch technology providers or run multiple systems. Rather than fixing the problem, Microsoft has built a $20 billion dollar a year security business.[12] Microsoft has federal agencies and taxpayers caught in a

[4] Pentagon's Microsoft monopoly raises concerns in Congress, Shaun Waterman, Newsweek (Jun. 7, 2023), https://www.newsweek.com/pentagons-microsoft-monopoly-raises-cybersecurity-concerns- congress-dod-defense-1804884

[5] The US government has a Microsoft problem, Eric Geller, WIRED (Apr. 15, 2024), https://www.wired.com/story/the-us-government-has-a-microsoft-problem/

[6] CISA directs federal agencies to immediately mitigate significant risk from Russian state-sponsored cyber threat, CISA (Apr. 11, 2024), https://www.cisa.gov/news-events/news/cisa-directs-federal- agencies-immediately-mitigate-significant-risk-russian-state-sponsored-cyber

[7] Contract summary, https://www.usaspending.gov/award/CONT_AWD_HC102823F1148_9700_ HC102817D0001_9700

[8] Contract summary, https://www.usaspending.gov/award/CONT_AWD_HC105023F0019_9700_ HC105023D0003_9700

[9] Contract summary, https://www.usaspending.gov/award/CONT_AWD_HC105023F0021_9700_ HC105023D0003_9700

[10] Contract summary, https://www.usaspending.gov/award/CONT_AWD_HC105023F0018_9700_ HC105023D0003_9700

[11] Contract summary, https://www.usaspending.gov/award/CONT_AWD_HC105023F0017_9700_ HC105023D0003_9700

[12] Microsoft still dominates cybersecurity business after hacks, Andrew Martin, Bloomberg (Apr. 17, 2024), https://www.bloomberg.com/news/newsletters/2024-04-17/microsoft-still-dominates-cybersecurity-business-after-hacks

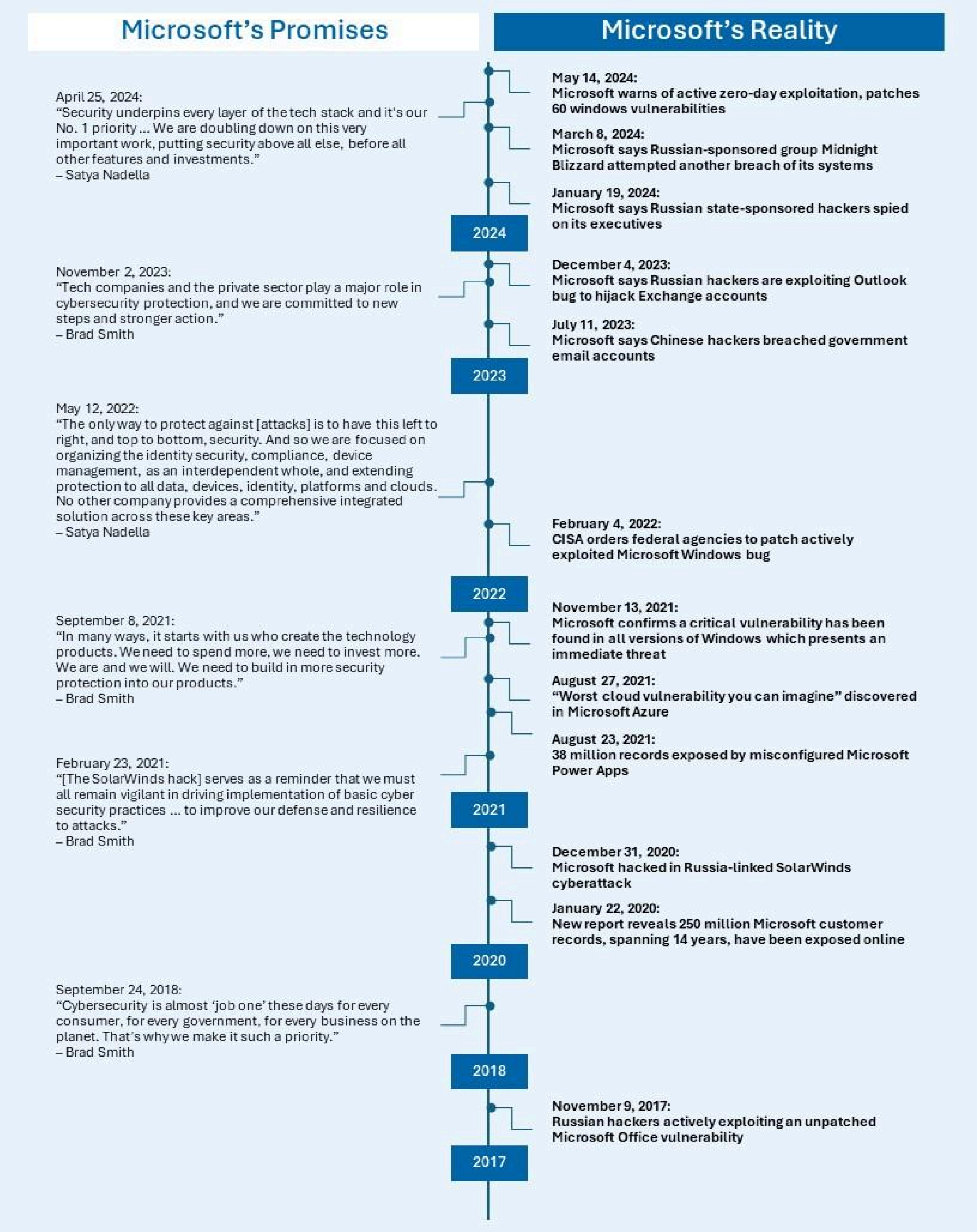
lucrative trap: sell software that isn't secure, watch hackers exploit those products, and then charge even more money to protect products it should have secured in the first place.

Promises Made, Promises Kept?

Microsoft's recent promise to put security "above all else" fits into a long pattern of watching government systems getting breached, promising to do better until the storm blows over, and then going back to the status quo.

Shortly after the CSRB's report was released, Charlie Bell, Microsoft's Executive Vice President, Security, wrote in a blog post, "We are making security our top priority at Microsoft, above all else—over all other features."[13] This statement follows years of what have turned out to be other empty promises from Microsoft executives, including Smith, to prioritize cybersecurity after major attacks. We should not believe Microsoft's promises to do better this time.

[13] Security above all else—expanding Microsoft's Secure Future Initiative, Charlie Bell, Microsoft (May 3, 2024), https://www.microsoft.com/en-us/security/blog/2024/05/03/security-above-all-else-expanding- microsofts-secure-future-initiative/



Microsoft's Promises

Microsoft's Reality

May 14, 2024:
Microsoft warns of active zero-day exploitation, patches 60 windows vulnerabilities

April 25, 2024:
"Security underpins every layer of the tech stack and it's our No. 1 priority ... We are doubling down on this very important work, putting security above all else, before all other features and investments."
– Satya Nadella

March 8, 2024:
Microsoft says Russian-sponsored group Midnight Blizzard attempted another breach of its systems

January 19, 2024:
Microsoft says Russian state-sponsored hackers spied on its executives

2024

December 4, 2023:
Microsoft says Russian hackers are exploiting Outlook bug to hijack Exchange accounts

November 2, 2023:
"Tech companies and the private sector play a major role in cybersecurity protection, and we are committed to new steps and stronger action."
– Brad Smith

July 11, 2023:
Microsoft says Chinese hackers breached government email accounts

2023

May 12, 2022:
"The only way to protect against [attacks] is to have this left to right, and top to bottom, security. And so we are focused on organizing the identity security, compliance, device management, as an interdependent whole, and extending protection to all data, devices, identity, platforms and clouds. No other company provides a comprehensive integrated solution across these key areas."
– Satya Nadella

February 4, 2022:
CISA orders federal agencies to patch actively exploited Microsoft Windows bug

2022

November 13, 2021:
Microsoft confirms a critical vulnerability has been found in all versions of Windows which presents an immediate threat

September 8, 2021:
"In many ways, it starts with us who create the technology products. We need to spend more, we need to invest more. We are and we will. We need to build in more security protection into our products."
– Brad Smith

August 27, 2021:
"Worst cloud vulnerability you can imagine" discovered in Microsoft Azure

August 23, 2021:
38 million records exposed by misconfigured Microsoft Power Apps

February 23, 2021:
"[The SolarWinds hack] serves as a reminder that we must all remain vigilant in driving implementation of basic cyber security practices ... to improve our defense and resilience to attacks."
– Brad Smith

2021

December 31, 2020:
Microsoft hacked in Russia-linked SolarWinds cyberattack

January 22, 2020:
New report reveals 250 million Microsoft customer records, spanning 14 years, have been exposed online

2020

September 24, 2018:
"Cybersecurity is almost 'job one' these days for every consumer, for every government, for every business on the planet. That's why we make it such a priority."
– Brad Smith

2018

November 9, 2017:
Russian hackers actively exploiting an unpatched Microsoft Office vulnerability

2017

[14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31]

[14] Microsoft warns of active zero-day exploitation, patches 60 windows vulnerabilities, Ryan Naraine, Security Week (May 14, 2024), https://www.securityweek.com/microsoft-patches-60-windows- vulns-warns-of-active-zero-day-exploitation/

[15] Microsoft "doubling down" on cybersecurity, Sam Sabin, Axios (Apr. 26, 2024), https://www.axios.com/ 2024/04/26/microsoft-earnings-cybersecurity-hacks

Follow the Money

"Security underpins every layer of the tech stack and it's our No. 1 priority. We are doubling down on this very important work, putting security above all else, before all other features and investments." - Microsoft CEO Satya Nadella, April 25, 2024

Microsoft has made bold commitments to put security above everything else, including presumably AI, and to tie top executives' pay to cybersecurity.[32] But the only way to determine if Microsoft truly puts security above all else is to "follow the money." Consider the following:

[16] Microsoft says Russian-sponsored group Midnight Blizzard attempted another breach of its systems, Kyt Dotson, SiliconANGLE (Mar. 8, 2024), https://siliconangle.com/2024/03/08/microsoft-says-russian- sponsored-group-midnight-blizzard-attempted-another-breach-systems/

[17] Microsoft says Russian state-sponsored hackers spied on its executives, Zeba Siddiqui and Christopher Bing, Reuters (Jan. 19, 2024), https://www.reuters.com/technology/cybersecurity/microsoft- says-it-was-hacked-by-russian-state-sponsored-group-2024-01-19/

[18] Russian hackers exploiting Outlook bug to hijack Exchange accounts, Bill Toulas, Bleeping Computer (Dec. 4, 2023), https://www.bleepingcomputer.com/news/microsoft/russian-hackers-exploiting-outlook- bug-to-hijack-exchange-accounts/

[19] A new world of security: Microsoft's Secure Future Initiative, Brad Smith, Microsoft (Nov. 2, 2023), htt ps://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/

[20] Chinese hackers breached government email accounts, Microsoft says, Julian E. Barnes, Maggie Haberman and Jonathan Swan, The New York Times (Jul. 11, 2023), https://www.nytimes.com/2023/07/11/us/politics/china-hack-us-government-microsoft.html

[21] Microsoft CEO Nadella: 'Zero trust is at the foundation of security transformation,' Jay Fitzgerald, CRN (May 12, 2022), https://www.crn.com/news/security/microsoft-ceo-nadella-zero-trust-is-at-the- foundation-of-security-transformation

[22] CISA orders federal agencies to patch actively exploited Windows bug, Sergiu Gatlan, Bleeping Computer (Feb. 4, 2022), https://www.bleepingcomputer.com/news/security/cisa-orders-federal-agencies- to-patch-actively-exploited-windows-bug/

[23] All Windows versions impacted by new zero-day hack, 0patch buys time, Gordon Kelly, Forbes (Apr. 21, 2022), https://www.forbes.com/sites/gordonkelly/2021/11/13/warning-issued-for-millions-of-microsoft-windows-10-windows-11-users/?sh=2a52b68e49c0

[24] Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem, Eric Rosenbaum, CNBC (Sep. 8, 2021), https://www.cnbc.com/2021/09/08/microsofts-20-billion-and- cybersecuritys-big-spending-problem.html

[25] "Worst cloud vulnerability you can imagine" discovered in Microsoft Azure, Jim Salter, Ars Technica (Aug. 27, 2021), https://arstechnica.com/information-technology/2021/08/worst-cloud-vulnerability- you-can-imagine-discovered-in-microsoft-azure/

[26] 38 million records exposed by misconfigured Microsoft Power Apps. Redmond's advice? RTFM, Thomas Claburn, The Register (Aug. 23, 2021), https://www.theregister.com/2021/08/23/power_shell_records/

[27] Strengthening the nation's cybersecurity: Lessons and steps forward following the attack on SolarWinds, Brad Smith, Senate Select Committee on Intelligence Open Hearing on the SolarWinds Hack (Feb. 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-bsmith-022321.pdf

[28] Microsoft hacked in Russia-linked SolarWinds cyberattack, Robert McMillan, The Wall Street Journal (Dec. 31, 2020), https://www.wsj.com/articles/microsoft-hacked-in-russia-linked-solarwinds-cyberattack- 11609437601

[29] Microsoft security shocker as 250 million customer records exposed online, Davey Winder, Forbes (Apr. 14, 2022), https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=60e9cea94d1b

[30] Microsoft president Brad Smith on AI for humanitarian concerns, cybersecurity, CBS (Sep. 24, 2018), https://www.youtube.com/watch?v=hmyYnZ7TcfU

[31] Russian 'Fancy Bear' hackers using (unpatched) Microsoft Office DDE exploit, Swati Khandelwal, The Hacker News (Nov. 9, 2017), https://thehackernews.com/2017/11/apt28-office-dde-malware.html

[32] A Microsoft under attack from government and tech rivals after 'preventable' hack ties executive pay to cyberthreats, Trevor Laurence Jockims, CNBC (May 22, 2024), https://www.cnbc.com/2024/05/22/after-a-big-hack-microsoft-is-tying-top-executive-pay-to-cyberthreats.html#:~:text=One%20change%20Microsoft%20is%20now,started%20conversations%20at%20other%20companies

- In the month since Nadella's declaration, Microsoft has announced at least $11.2 billion in AI investments across Indonesia,[33] Malaysia,[34] France[35] and the United States.[36]

- At Microsoft Build, which started May 21, Microsoft announced "Recall." This product takes a screenshot of a user's computer screen every few seconds and stores that image on their laptop.[37] Security experts have described it as a "security nightmare" and "an affront to user privacy and an assault on best practices for both security and privacy."[38]

- Microsoft announced a CoPilot AI bot in the Telegram messaging app on May 28,[39] an AI partnership with Khan Academy on May 21,[40] and more.

These are not the actions of a company that puts security "*above all else, before all other features and investments.*" The reality is that the culture of insecurity the CSRB warned about is alive and well at Microsoft.

In 2021, Microsoft committed to investing $20 billion in cybersecurity over the next five years, or $4 billion annually.[41] Compare this investment to Microsoft's annual security revenue, which reached $20 billion last year alone—5x what Microsoft publicly stated it would spend to secure customers that same year.[42]

Simply look at Microsoft's other investments to see where its priorities are: A proposed supercomputer to jumpstart AI,[43] the acquisition of Activision Blizzard Inc. to expand its gaming business,[44] and stock buybacks to boost share price.[45]

[33] Microsoft will invest $1.7 billion in AI and cloud infrastructure in Indonesia, Edna Tarigan, Associated Press (Apr. 30, 2024), https://apnews.com/article/indonesia-microsoft-satya-nadella-invest-ai-a2e53b4a 3872ac80b9c56c53187c4890

[34] Microsoft to invest $2.2 bln in cloud and AI services in Malaysia, Danial Azhar and Rozanna Latiff, Reuters (May 2, 2024), https://www.reuters.com/technology/microsoft-invest-22-bln-malaysias-digital- transformation-2024-05-02/

[35] Microsoft and Amazon to invest $5.6 billion into France as Macron courts tech giants, Ryan Browne, CNBC (May 13, 2024), https://www.cnbc.com/2024/05/13/amazon-and-microsoft-to-invest-5point6-billion-into-france.html#:~:text=Microsoft%20says%20it%20is%20committing,support%20for%20France%27s%20technology%20industry

[36] Microsoft to invest over $3 billion to build AI in Wisconsin, Tom Dotan and Ken Thomas, The Wall Street Journal (May 8, 2024), https://www.wsj.com/tech/ai/microsoft-to-invest-over-3-billion-to-build-ai-in- wisconsin-64f7b6e3

[37] Microsoft announced "Recall." This product takes a screenshot of a user's computer screen every five seconds, Thomas Brewster, Forbes (May 28, 2024), https://www.forbes.com/sites/thomasbrewster/2024/ 05/28/microsoft-recall-feature-is-always-watching/?sh=47a0bb808bfc

[38] Microsoft's 'Recall' feature draws criticism from privacy advocates, Jai Vijayan, Dark Reading (May 24, 2024), https://www.darkreading.com/data-privacy/microsofts-recall-feature-draws-criticism-from-privacy- advocates

[39] After Windows 11, Copilot is coming to messaging apps, starting with Telegram, Mayank Parmar, Windows Latest (May 28, 2024), https://www.windowslatest.com/2024/05/28/after-windows-11-copilot-is- coming-to-messaging-apps-starting-with-telegram/

[40] Microsoft, Khan Academy provide free AI assistant for all educators in US, Eric Rosenbaum, CNBC (May 21, 2024), https://www.cnbc.com/2024/05/21/microsoft-khan-academy-launch-free-ai-assistant- for-all-us-teachers.html

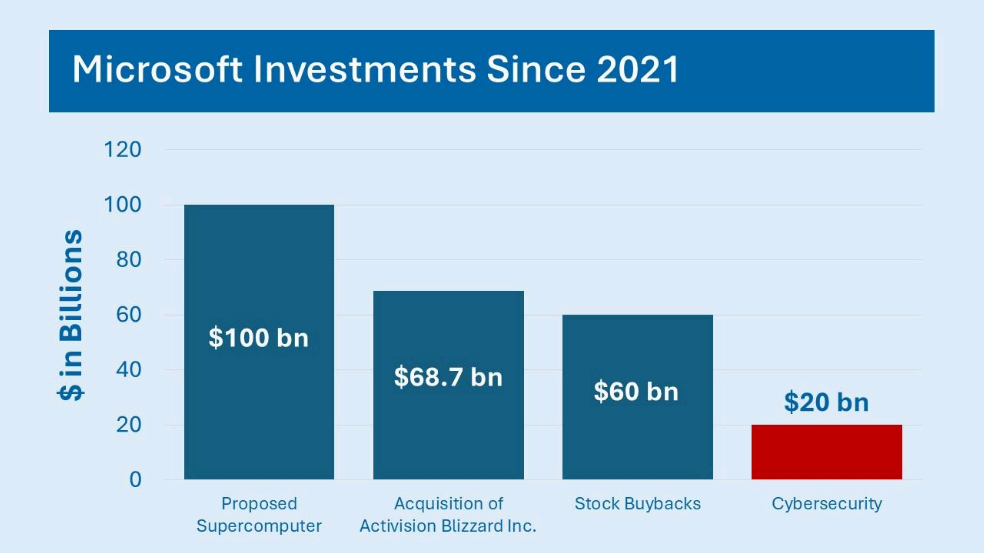
[41] Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem, Eric Rosenbaum, CNBC (Sep. 8, 2021), https://www.cnbc.com/2021/09/08/microsofts-20-billion-and- cybersecuritys-big-spending-problem.html

[42] Microsoft still dominates cybersecurity business after hacks, Andrew Martin, Bloomberg (Apr. 17, 2024), https://www.bloomberg.com/news/newsletters/2024-04-17/microsoft-still-dominates-cybersecurity-business-after-hacks

[43] Microsoft and OpenAI plot $100 billion Stargate AI supercomputer, Anissa Gardizy and Amir Efrati, The Information (Mar. 29, 2024), https://www.theinformation.com/articles/microsoft-and-openai-plot- 100-billion-stargate-ai-supercomputer

[44] Microsoft to acquire Activision Blizzard to bring the joy and community of gaming to everyone, across every device, Microsoft (Jan. 18, 2022), https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/

[45] Microsoft hikes dividend and unveils $60 billion stock buyback program, Eric J. Savitz, Barron's (Sep. 15, 2021), https://markets.businessinsider.com/news/stocks/big-tech-stock-buybacks-apple- google-meta-microsoft-tesla-buffett-2023-8



It is clear that Microsoft is more concerned with its market share, AI and market cap-not security. As a free market organization, we support Microsoft's growth and expansion, but taxpayers shouldn’t pay billions for insecure software so that Microsoft can boost its stock price.

Conclusion

NetChoice commends the Committee for holding Microsoft accountable for its cascade of security failures that have compromised the U.S. government and threatened Americans’ safety. We support the Committee’s efforts to fulfill its cybersecurity oversight responsibilities by examining Microsoft's supposed commitment to addressing its cybersecurity challenges.

As always, we offer ourselves as a resource to discuss these issues in further detail. We greatly appreciate your attention to this important matter.[46]

Sincerely,

Carl Szabo
Vice President & General Counsel, NetChoice

NetChoice is a trade association that works to protect free expression and promote free enterprise online.

[46] The views of NetChoice expressed here do not necessarily represent the views of NetChoice members.