Microsoft's Work to Strengthen Cybersecurity Protection

Written Testimony of Brad Smith
Vice Chair and President, Microsoft Corporation

U.S. House Committee on Homeland Security

Submitted on June 11, 2024
for the Committee's Hearing on June 13, 2024

Chairman Green, Ranking Member Thompson, and Members of the Committee, thank you for the opportunity to appear to discuss Microsoft's commitment and ongoing work to strengthen cybersecurity protection. As you know, this work comes in part in response to the Cyber Safety Review Board's (CSRB) report on the Microsoft Exchange Online cyber intrusion in 2023 by malicious actors referred to as Storm-0558, affiliated with the People's Republic of China.

Let me first note my appreciation for the critical role this Committee plays in protecting the homeland security of the United States. In the world today, America's homeland cannot be secured without protecting the cyber domain. Cybersecurity has become a collective duty that spans both the public and private sectors. Given this Committee's responsibilities, I appreciate the importance of your oversight not only of the executive branch, but of tech companies.

Before I say anything else, I think it's especially important for me to say that 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. But rather with a complete commitment to address every recommendation and use this report as an opportunity and foundation to strengthen our cybersecurity protection across the board.

We are taking action to address every one of the CSRB's recommendations applicable to Microsoft. To put this in context, the CSRB's report provides 25 recommendations, 16 of which apply to Microsoft. Four of these are directed to Microsoft specifically and the remaining 12 recommendations are addressed to all cloud service providers (CSPs). We are acting on all 16 of these recommendations.

But we are not stopping there. We have added another 18 concrete security objectives, reflecting the work we started last summer after we assessed the shortfalls we identified from the Storm-0558 intrusion from China. As a result, last November we launched a company-wide initiative, called the Secure Future Initiative (SFI), to act on this learning. We expanded this work in January after an aggressive attack by the Russian Foreign Intelligence Agency, or SVR, and then expanded it again in March after the CSRB report.

We recognize that Microsoft plays a unique and critical cybersecurity role. Not only for our customers, but for this country. And not only for this country, but for this nation's allies. This role reflects the wide range of products and services Microsoft provides to individuals and organizations, including cloud services that operate through datacenters located in 32 countries around the world. It also reflects the broad cybersecurity work we undertake every day, including for and in close collaboration with the U.S. and numerous allied governments.

This role brings with it tremendous responsibility. Expanding and intensifying geopolitical conflicts have created a more dangerous cyberworld. It's no accident that the first shots fired in the war against Ukraine were malicious cyberattacks by the Russian military. And it's no coincidence that the first people to detect these attacks were located not in Ukraine, but near Seattle working in Microsoft's Threat Intelligence Center.

In the 28 months since that war began and as tensions have grown elsewhere, we have seen more prolific, well-resourced, and sophisticated cyberattacks by four countries – Russia, China, Iran, and North Korea. By any measure, lawless and aggressive cyber activity has reached an extraordinary level. During the past year, Microsoft detected 47 million phishing attacks against our network and employees. But this is modest compared to the 345 million cyber attacks we detect against our customers every day. Too often these actions take place without effective reprisals or deterrence, reflecting in part the degree to which international law and norms of conduct are incomplete or lack meaningful enforcement.

For those of us who work at Microsoft, the implications could not be clearer. At one level, the CSRB's recommendations speak to everyone who works at any company providing cloud services and in technology positions more broadly. But more than anything, they are a clarion call for stronger action for every employee who works at Microsoft.

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. While perfection in the face of aggressive nation-state cyberattacks is difficult to achieve, we always must be the first not only to recognize but to accept responsibility and apologize when attacks penetrate our network like the two from China and Russia did this past year, especially when, as the CSRB noted, stronger steps would have prevented them.

That is what we are doing here. We acknowledge that we can and must do better, and we apologize and express our deepest regrets to those who have been impacted. This is the message I have conveyed personally when talking with individuals impacted in our government, as well as elsewhere. It's something for all our employees to embrace. As I often say inside Microsoft, "no one ever died of humility." To the contrary, a willingness to acknowledge our shortcomings and address problems head-on inspires us to learn from our mistakes and to apply the lessons we learn so we constantly can get better.

In sum, we accept responsibility for the past and are applying what we've learned to help build a more secure future. We are pursuing new strategies, investing more resources, and fostering a stronger cybersecurity culture. We have reallocated resources and have assigned technical and engineering employees across the company to this endeavor, 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. And we are identifying new opportunities not just for ourselves, but for all our customers and for greater collaboration across the private and public sectors.

Let me share some of the details.

Microsoft's Secure Future Initiative

As I described above, we launched our Secure Future Initiative as a multiyear endeavor to evolve the way we design, build, test, and operate our products and services. It is focused on achieving the highest possible standards for security and is grounded in three core cybersecurity tenets that apply across Microsoft:

- **Secure by Design**: Make security the first priority when designing any product or service.
- **Secure by Default**: Ensure that security protections are enabled and enforced by default, require no extra effort, and are not optional.

- **Secure Operations**: Ensure that security controls and monitoring will continuously be improved to meet current and future threats.

This approach will enable us to establish stronger multi-layered defenses to counter the most sophisticated and well-resourced nation-state actors. To implement these tenets, Microsoft has defined specific engineering goals and key performance indicators divided into the following six pillars:

- **Protect Identities and Secrets**: Reduce the risk of unauthorized access to any data by implementing and enforcing best-in-class standards across our infrastructure that manages identities and sensitive information such as passwords ("secrets"), to ensure that only the right people and applications access the right resources.

- **Protect Tenants and Isolate Production Systems**: Use consistent, best-in-class security practices and continuously validate isolation of production systems – including those upon which we operate the Microsoft Cloud.

- **Protect Networks**: Continuously improve and implement best-in-class practices to protect Microsoft production networks.

- **Protect Engineering Systems**: Continuously improve our software supply chain and the systems that enable Microsoft engineers to develop, build, test, and release software, thereby protecting software assets and improving code security.

- **Monitor and Detect Threats**: Continuously improve coverage and automatic detection of ever-evolving threats to Microsoft production infrastructure and services, accelerating actioning against those threats.

- **Accelerate Response and Remediation**: Enhance our response and remediation practices when we learn of vulnerabilities in our offerings or our infrastructure, to be even more comprehensive and timely and better prevent exploitation of those vulnerabilities.

Perhaps most importantly for purposes of this hearing, we worked this spring to map all 16 of the CSRB's recommendations applicable to Microsoft to ensure that we are addressing them as part of the Secure Future Initiative. For example, we are actively in the process of transitioning both our consumer and enterprise identity systems to a new hardened key management system that leverages hardware security modules for the storage and generation of keys. We are rolling out proprietary data and corresponding detection signals at all places where tokens are validated. And we have made significant progress on Automated and Frequent Key Rotation, Common Auth Libraries, and Proprietary Data used in our token generation algorithm.

We have invited the Cybersecurity and Infrastructure Security Agency (CISA), on behalf of the CSRB, to Microsoft's headquarters for a detailed technical briefing on these and all our other engineering objectives, including the specific ways we are implementing the CSRB's recommendations. We also will keep the Committee fully informed on our progress in addressing all 16 recommendations, plus our other steps.

It is important to note that we do not see the CSRB's recommendations nor our additional 18 SFI objectives as a "to do" list that we tick off, so that we can declare eventually that our job is complete. Security does not work that way. Threat actors will always attack with the full breadth of human ingenuity. Our cybersecurity will never be complete. Rather, **these steps are emblematic of a corporate-wide and permanent shift to ensure that we place security above all else in a world in which there is constant combat in cyberspace.**

The Importance of Culture

There is a well-known business adage that “culture eats strategy for breakfast.” Business history unfortunately is littered with companies that had a brilliant strategy but a weak culture. From the moment we learned that the CSRB urged Microsoft to address our cybersecurity culture, we concluded almost instinctively that this is a critical facet that we need to embrace rather than resist.

Culture of course starts with the “tone from the top” and ultimately needs to be lived by every employee. When I first discussed the CSRB’s focus on our security culture with Satya Nadella, Microsoft’s Chairman and CEO, he embraced the culture point immediately. As he said, we each needed to make this the most important thing we do as leaders of the company. It is more important even than the company’s work on artificial intelligence. And we needed to sit down with Microsoft’s Senior Leadership Team[1] to work on this together.

Both as a Senior Leadership Team and with Microsoft’s Board of Directors, we have spent considerable time the past two months focused on reviewing the security culture we have and re-defining the world-class security culture we want to foster. As with anything this important, this has required a lot of discussion and careful thought. Culture change always requires multiple facets, and the difficulty of achieving real and lasting success should not be underestimated.

The good news is that we have substantial experience in this area. Few companies in the past decade have done as much work as Microsoft to reinvent themselves by redefining their culture. In 2014, when Satya became Microsoft’s CEO, he led the company through a cultural transformation based on a north star focused on developing a “growth mindset,” unleashing curiosity and innovation at every level by encouraging employees to become “learn-it-alls” instead of “know-it-alls.”

We are calling on our capabilities for cultural change to strengthen our security culture, starting with a north star that we’ve communicated across the company to make security the top priority at Microsoft, above all else. To help make this concrete, Satya wrote to every employee:

> “If you’re faced with the tradeoff between security and another priority, your answer is clear: **Do security**. 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.”[2]

While this clarity is critical, it’s only the start of what is needed for a broad-based and effective security culture. As our Senior Leadership Team discussed this cultural evolution, we concluded that it makes sense to treat security as the most important attribute of product quality. And in so doing, there is a lot

[1] Microsoft’s Senior Leadership Team or SLT is comprised of 16 executives with the following titles: Chairman and Chief Executive Officer; Vice Chair and President; Executive Vice President and Chief Financial Officer; Executive Vice President and Chief Technology Officer; Executive Vice President and Chief Human Resources Officer; Executive Vice President, Cloud & AI; Executive Vice President and Chief Executive Officer, Microsoft AI; Executive Vice President, Experiences & Devices; Executive Vice President, Microsoft Security; Executive Vice President and Chief Commercial Officer; Executive Vice President and Chief Marketing Officer; Chief Executive Officer, LinkedIn; Chief Executive Officer, Microsoft Gaming; Executive Vice President, Strategic Missions + Technologies; Executive Vice President, Business Development, Strategy and Ventures; Executive Vice President and Consumer Chief Marketing Officer.

[2] See Prioritizing security above all else - The Official Microsoft Blog.

we can apply from business learning both across Microsoft and around the world in building high quality products.

Some of the most creative and effective work in this regard brought together post-World War II American business thinking with new innovations in the 1980s that enabled Toyota and other Japanese auto companies to build a global reputation for reliable, high-quality cars. The resulting Total Quality Management (TQM) system has continued to evolve in ensuing decades, and many of the most successful American companies apply a form of it today.

A TQM system focuses on customer needs and continuous Improvement, recognizing that there is always room for improvement, no matter how small. Critically, it involves total participation across a company, with every employee participating in the process of quality improvement.

At the heart of these various approaches is something we believe will become a vital part of Microsoft's security culture – empowering and rewarding every employee to find security issues, report them, help fix them, and encourage broader learning from the process and the results. This requires that we incorporate this security work as an indispensable and integrated element in every aspect of the company's engineering processes, as you can see reflected in the three core tenets of the Secure Future Initiative.

An added aspect we've learned from our prior work is that culture change requires constant practice and role modeling. This is one of the many reasons that our Senior Leadership Team has been devoting part of its weekly meeting for a standing deep dive into one of the six SFI pillars, as well as a discussion of other specific security issues and an assessment of how we are doing overall. We're replicating this focus across the company, while making a point of talking explicitly about the role of our SFI tenets in both internal and external product discussions – as we did last Friday when we announced a feature change to our upcoming Copilot+ PCs.[3]

Effective culture change also requires the resources needed for success. This is why we have added 1,600 more security engineers this fiscal year, and we will add another 800 new security positions in our next fiscal year.

We've coupled this expansion of resources with important changes in the company's security governance. In addition to the critical longstanding role of the company's Chief Information Security Officer, or CISO, we have created the Office of the CISO 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.

Ultimately, culture change requires accountability. This is something all our senior leaders understand, starting with Satya as the company's CEO. Rather than delegate overall security responsibility to someone else, he has taken on the responsibility personally to serve as the senior executive with overall accountability for Microsoft's security.

This is also why we announced on May 3 that part of the compensation of the company's Senior Leadership Team will be based on our progress in meeting our security plans and milestones. Since that time, we've worked to refine these compensation and other accountability steps for the next fiscal year, which begins on July 1. Tomorrow, Microsoft's Board of Directors will review and finalize this program, and I look forward to reporting on the Board's decisions and discussing them with you at the hearing on Thursday.

[3] See "Update on the Recall preview feature for Copilot+ PCs," Microsoft Windows Blog, June 7, 2024.

A More Dangerous Threat Landscape

We also recognize that we must continue to adapt to a dynamic and intensifying threat landscape. Today, Microsoft tracks more than three hundred nation-state actors. We report what we see through frequent cybersecurity technical blogs, podcasts, and other resources,[4] and we summarize all that we track across the company annually in our Microsoft Digital Defense Reports.[5]

Recent years have brought sobering cybersecurity developments that, if anything, get less public attention and discussion than they deserve. Unlike attacks from tanks, planes, or ground troops, cyberattacks are invisible to the naked eye. But they move across the internet at the speed of light, crossing borders and attacking domestic infrastructure on American soil, too often destroying property and putting American citizens' lives at risk.[6]

Geopolitical tensions since Russia invaded Ukraine have led to more dangerous conflict in cyberspace. The two successful attacks by Russian and Chinese actors against Microsoft in fact reflect broader changes that are sweeping in their reach. As we take stock not only of these recent attacks but of all the data we see, a few key conclusions emerge.

First, the pace of attacks has increased to the point where there is now constant combat in cyberspace. Not just every day, but literally *every second*. Microsoft alone detects almost 4,000 password-based attacks against our customers every second of every day.

We're also seeing a steady increase in attacks by state-based cyber actors in Russia, China, Iran, and North Korea. These have increased steadily not only against Microsoft but against individuals and organizations around the world.

Second, nation-state adversaries are becoming more aggressive. We are seeing a higher level of technical sophistication that almost certainly reflects the investment of more resources and expanded work to strengthen technical know-how. But more disconcerting still is the more aggressive nature of nation-state attacks. To take two examples:

- One year ago, Microsoft detected a Chinese nation-state actor compromising and pre-positioning "web-shell" back doors in the networks of a wide range of critical infrastructure in the United States and Guam using very sophisticated techniques. This included routing their attacks through compromised home routers. We disclosed this to the U.S. government and the public and worked with government agencies to continue to investigate these attacks. This activity put civilians and civilian infrastructure at risk, including our electricity and water supplies and air traffic control systems.
- The Russian Foreign Intelligence Agency, or SVR, continues to be one of the best resourced and most sophisticated cyber agencies in the world. This past year, we have seen it become more aggressive as well. For example, in the past the SVR's hackers typically would withdraw from a computer environment once their intrusion was discovered. The past six months, we have seen them pour

[4] See, e.g., Threat Intelligence Thought Leadership | Security Insider (microsoft.com); Microsoft Security Response Center; Microsoft Security Blog | Digital Security Tips and Solutions.

[5] Intelligence Reports (microsoft.com)

[6] See, e.g., DEFENDING-OT-OPERATIONS-AGAINST-ONGOING-PRO-RUSSIA-HACKTIVIST-ACTIVITY.PDF (defense.gov), May 1, 2024

more resources once discovered into what in effect is hand-to-hand combat to control a computer environment.

Third, we're seeing a more direct relationship between nation-state activity and cybercrime, especially in Russia and North Korea. While the latter's government ministries have long self-funded parts of their budgets through cyber-based financial theft, the Russian activity has taken a new turn. We believe the SVR in part is retaining its top engineers by enabling them to take what they learn during the day and use the same tools to work with impunity in criminal ransomware operations at night and on the weekends. This is creating a vicious cycle reinforcing nation-state and ransomware activity.

Ransomware has become a particularly heinous form of cybercrime, as it threatens the destruction of computers and disruption of critical services to increase the prospects of recovering the ransom they demand. Perhaps most sobering, ransomware has become a plague on the healthcare sector, including in the United States. The FBI estimated in its 2023 Internet Crime Report that healthcare has become the sector most frequently targeted by ransomware. The number of such attacks last year against U.S. healthcare providers increased by 128 percent, claiming 389 healthcare organizations as victims.[7]

The impacts of these attacks are real and frightening. For example, last Thanksgiving, a cyberattack on Ardent Health Services, a Tennessee-based company owning more than two dozen hospitals across at least five states, caused ambulances to be diverted from hospitals in East Texas and forced hospitals in New Jersey, New Mexico, and Oklahoma to reroute ambulances. During such attacks, hospitals lose access to electronic medical records, medical imaging systems fail, and some patients must be transported to other facilities. Experts from the University of Minnesota School of Public Health have linked cyberattacks between 2017 and 2021 to the deaths of 67 Medicare patients in the United States, a number they believe is likely underestimated.

On February 21, 2024, UnitedHealth Group was targeted by the Russian-speaking BlackCat (ALPHV) ransomware group. The attack shut down the largest healthcare payment system in the United States, which processes nearly 40 percent of all medical claims. This created a backlog of unpaid claims, causing serious cash flow problems for doctors' offices and hospitals and threatening patients' access to care. The UnitedHealth CEO estimated one-third of Americans could be impacted to some extent by the attack.

Fourth and finally, we must prepare for the likelihood that America's nation-state adversaries will collaborate more closely in cyberspace. Russia and China are already working together when it comes to other forms of military and intelligence activity, and they are more closely connected with North Korea and Iran as well. We must work on the assumption that the geopolitical trends we see in the physical world will manifest themselves in cyberspace as well.

This is grave at multiple levels. It's one thing to engage in cyber combat with four separate nation-state adversaries, but quite another scenario if two or all four of these countries work in tandem.

This mounting danger is qualitative as well as quantitative. This is because each of the four countries – and especially Russia and China – are well-resourced and highly capable on their own. But they have capabilities in different areas, from software engineering to machine learning to computational resources to social science. The greater danger for the United States and our allies is that these countries will not just combine forces but build up each other's cyber-attack capabilities as they do so.

Unfortunately, this is where the future is likely going.

[7] Ransomware_Attacks_Surge_in_2023.pdf (dni.gov)

This makes all the CSRB's 25 recommendations more important. Not just the 16 that speak to Microsoft or the 12 directed at other cloud service providers. But also, the other nine addressed to the government and to public-private collaboration.

We All Live in the Same Connected World

Make no mistake, we are all in this together. The CSRB report was sparked by a successful Chinese attack on Microsoft, and we understand every day that we have by far the first and greatest responsibility to heed its words. We're committed to doing so and to playing an indispensable leadership role in defending not just our customers, but this country and its allies. But no single company can protect a country and other nations from what is emerging as a cyberwar waged by four aggressive governments. Cybersecurity protection requires a whole-of-industry and whole-of-society mission across multiple countries. Each of us can and must learn from each other and work together to protect cybersecurity for our nation and the world.

A huge part of the problem today is that our adversaries are operating on an uneven playing field, benefitting from at least two attributes:

- Nation-state attackers too often attack without meaningful reprisal, consequence, or deterrence. International law or norms of conduct are incomplete and lack meaningful enforcement.
- Like all threat actors, nation-state attackers have the first mover advantage. Private sector parties like Microsoft can only play defense. This is a huge advantage to the attacker. During the past 18 months, when the two attacks from China and Russia occurred, resources on our network were, conservatively, targeted more than 80 million times. By this measure, our defense is both successful and yet not good enough.

I want to express enormous gratitude to all those who are fighting to defend our country in this war in cyberspace. This includes our customer organizations, including their CISOs. This also includes our competitors and *their* CISOs. Yes, our companies compete fiercely, and we negotiate for our respective interests fiercely. But we also recognize that there is a higher calling, a common bond that knits us all together, and that is to keep our organizations, our people, our country, and our allies safe and secure.

The federal government in the United States has made many important strides in recent years in strengthening cybersecurity protection. But as with everyone else, we will need the government to do even more. For your consideration, we include some ideas below of how the government – and this Committee – can do more in support of cyber defense.

- Enhance effective deterrence and heighten accountability by attributing malicious cyber activity. Today, public attribution remains inconsistent and much of the malicious cyber activity remains in the shadows. Deter nation-state threat actors by imposing appropriate punishment so that the actions of nation-state actors are not without a cost. To accomplish this Congress should assess whether additional steps are needed to strengthen countermeasures against nation-state threat actors.
- Embrace the CSRB report's government-focused recommendations and move quickly to implement them just as the private sector should adopt the set of 12 recommendations directed to it. The overarching recommendation is for the U.S. government to "updat[e] both the FedRAMP program itself as well as the supporting frameworks that implement the Federal Information Security Modernization Act (FISMA) such as the NIST RMF." Recommendations 21 through 25 provide greater specifics. Other recommendations, such as Recommendation 18 which calls for a cyber

threat notification system such as an “Amber Alert”, will require government and private sector partnership and Microsoft stands ready to contribute.

- Reduce the overall attack surface through deterrence by denial, i.e., improving the defensive cybersecurity of our critical infrastructure through new funding or critical programs.

We have an enormous amount to accomplish in 2024, starting with Microsoft itself. But even more than this, one of the most important lessons from the past two years and the two successful Chinese and Russian attacks is that everything we do this year, no matter how successful, will not likely be sufficient for the dangers we will face a year or two from now. The cyber domain is becoming more lawless, dangerous, and hostile. And we need to plan and adapt accordingly.

We are grateful for the opportunity to speak with the Committee and to communicate our commitment to you, our customers, and the country that we will continue to strengthen our security practices. Not just to implement the CSRB’s recommendations. But more broadly and beyond.

Thank you.