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

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JUNE 13, 2024

Serial No. 118–70

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
58–996 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
SHEILA JACKSON LEE, Texas
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
THOMAS R. SUOZZI, New York
TIMOTHY M. KENNEDY, New York
YVETTE D. CLARKE, New York

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

CONTENTS

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

Thursday, June 13, 2024

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to notice, at 1:17 p.m., in room 310, Cannon House Office Building, Hon. Mark E. Green (Chairman of the committee) presiding.

Present: Representatives Green, Higgins, Gimenez, Pfluger, Garbarino, Greene, Gonzales, Ezell, D'Esposito, Lee, Luttrell, Strong, Crane, Thompson, Swalwell, Correa, Carter, Thanedar, Magaziner, Ivey, Garcia, Ramirez, Menendez, Suozzi, Kennedy, and Clarke.

Chairman GREEN. The Committee on Homeland Security will come to order.

Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to examine the Department of Homeland Security's Cyber Safety Review Board's recent report concerning the summer 2023 Microsoft Exchange on-line cyber incident.

Specifically, we'll examine Microsoft's view regarding the company's security practices and challenges encountered in preventing significant cyber intrusions by suspected nation-state actors and its plans to strengthen security measures moving forward.

I now recognize myself for an opening statement.

Each and every day, the United States depends upon Microsoft—cloud services, productivity tools, operating systems—to carry out an array of critical missions. Microsoft is deeply integrated into our Nation's digital infrastructure, a presence that carries heightened respect and heightened responsibility.

We're holding this hearing today because of the latest Department of Homeland Security Cyber Safety Review Board, CSRB, report. The report attributed last summer's Microsoft Exchange online hack by Storm–0558, which is backed by the Chinese Communist Party, to "a cascade of security failures at Microsoft".

The determinations were based on a number of findings detailed in the report. I have the report and would like to introduce it into the record.

So ordered.

[The information follows:]

REPORT SUBMITTED BY CHAIRMAN MARK E. GREEN, MD

CYBER SAFETY REVIEW BOARD

Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board

TABLE OF CONTENTS

MESSAGE FROM THE CHAIR AND DEPUTY CHAIR

It is not an exaggeration to say that cloud computing has become an indispensable resource to this nation, and indeed, much of the world. Numerous companies, government agencies, and even some entire countries rely on this infrastructure to run their critical operations, such as providing essential services to customers and citizens. Driven by productivity, efficiency, and cost benefits, adoption of these services has skyrocketed over the past decade, and, in some cases, they have become as indispensable as electricity. As a result, cloud service providers (CSPs) have become custodians of nearly unimaginable amounts of data. Everything from Americans' personal information to communications of U.S. diplomats and other senior government officials, as well as commercial trade secrets and intellectual property, now resides in the geographically-distributed data centers that comprise what the world now calls the "cloud."

The cloud creates enormous efficiencies and benefits but, precisely because of its ubiquity, it is now a high-value target for a broad range of adversaries, including nation-state threat actors. An attacker that can compromise a CSP can quickly position itself to compromise the data or networks of that CSP's customers. In effect, the CSPs have become one of our most important critical infrastructure industries. As a result, these companies must invest in and prioritize security consistent with this "new normal," for the protection of their customers and our most critical economic and security interests.

When a hacking group associated with the government of the People's Republic of China, known as Storm-0558, compromised Microsoft's cloud environment last year, it struck the espionage equivalent of gold. The threat actors accessed the official email accounts of many of the most senior U.S. government officials managing our country's relationship with the People's Republic of China.

As is its mandate, the Cyber Safety Review Board (CSRB, or the Board) conducted deep fact-finding around this incident. The Board concludes that this intrusion should never have happened. Storm-0558 was able to succeed because of a cascade of security failures at Microsoft, as outlined in this report. Today, the Board issues recommendations to Microsoft to ensure this critical company, which sits at the center of the technology ecosystem, is prioritizing security for the benefit of its more than one billion customers. In the course of its review, the Board spoke with a range of large CSPs to assess the state of their security practices, and—as is also its mandate—the Board today issues recommendations to all CSPs for establishing specific security controls for identity and authentication in the cloud. All technology companies must prioritize security in the design and development of their products. The entire industry must come together to dramatically improve the identity and access infrastructure that safeguards the information CSPs are entrusted to maintain. Global security relies upon it.

We, and all the members of CSRB, are grateful for Microsoft's full cooperation in this review. The company provided extensive oral and written submissions since November 2023, and we believe answered all of our questions to the best of its ability. We also received full cooperation from U.S. intelligence, law enforcement, and cyber defense agencies.

As we complete our third review since the Board's establishment in 2022, we are gratified more broadly to observe the track record of cooperation that CSRB has developed with industry, security researchers, the academic community, and foreign government agencies. We are more confident than ever in the Board's role as a truly public-private institution that conducts authoritative fact-finding and issues actionable recommendations in the wake of major cyber incidents.

We are grateful to Alejandro Mayorkas, Secretary of Homeland Security, and to Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency, for their continued belief in and support of this Board, including by charging us with consequential mandates like this review of the Microsoft Exchange Online incident.

We offer our thanks to the 20 organizations and individual experts who offered their experience and expertise to allow us to conduct this comprehensive review. Finally, we express deep appreciation to our colleagues on the Board for their continued commitment to our charge, and to the determined and gifted staff who helped the Board discharge its task and bring this important review to conclusion.

Robert Silvers
Chair

Dmitri Alperovitch
Deputy Chair

EXECUTIVE SUMMARY

In May and June 2023, a threat actor compromised the Microsoft Exchange Online mailboxes of 22 organizations and over 500 individuals around the world. The actor—known as Storm-0558 and assessed to be affiliated with the People's Republic of China in pursuit of espionage objectives—accessed the accounts using authentication tokens that were signed by a key Microsoft had created in 2016. This intrusion compromised senior United States government representatives working on national security matters, including the email accounts of Commerce Secretary Gina Raimondo, United States Ambassador to the People's Republic of China R. Nicholas Burns, and Congressman Don Bacon.

Signing keys, used for secure authentication into remote systems, are the cryptographic equivalent of crown jewels for any cloud service provider. As occurred in the course of this incident, an adversary in possession of a valid signing key can grant itself permission to access any information or systems within that key's domain. A single key's reach can be enormous, and in this case the stolen key had extraordinary power. In fact, when combined with another flaw in Microsoft's authentication system, the key permitted Storm-0558 to gain full access to essentially any Exchange Online account anywhere in the world. As of the date of this report, Microsoft does not know how or when Storm-0558 obtained the signing key.

This was not the first intrusion perpetrated by Storm-0558, nor is it the first time Storm-0558 displayed interest in compromising cloud providers or stealing authentication keys. Industry links Storm-0558 to the 2009 Operation Aurora campaign that targeted over two dozen companies, including Google, and the 2011 RSA SecurID incident, in which the actor stole secret keys used to generate authentication codes for SecurID tokens, which were used by tens of millions of users at that time. Indeed, security researchers have tracked Storm-0558's activities for over 20 years.

On August 11, 2023, Secretary of Homeland Security Alejandro Mayorkas announced that the Cyber Safety Review Board (CSRB, or the Board) would "assess the recent Microsoft Exchange Online intrusion . . . and conduct a broader review of issues relating to cloud-based identity and authentication infrastructure affecting applicable cloud service providers and their customers."

The Board conducted extensive fact-finding into the Microsoft intrusion, interviewing 20 organizations to gather relevant information (see Appendix A). Microsoft fully cooperated with the Board and provided extensive in-person and virtual briefings, as well as written submissions. The Board also interviewed an array of leading cloud service providers to gain insight into prevailing industry practices for security controls and governance around authentication and identity in the cloud.

The Board finds that this intrusion was preventable and should never have occurred. The Board also concludes that Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations. The Board reaches this conclusion based on:

1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;
3. the Board's assessment of security practices at other cloud service providers, which maintained security controls that Microsoft did not;
4. Microsoft's failure to detect a compromise of an employee's laptop from a recently acquired company prior to allowing it to connect to Microsoft's corporate network in 2021;
5. Microsoft's decision not to correct, in a timely manner, its inaccurate public statements about this incident, including a corporate statement that Microsoft believed it had determined the likely root cause of the intrusion when in fact, it still has not; even though Microsoft acknowledged to the Board in November 2023 that its September 6, 2023 blog post about the root cause was inaccurate, it did not update that post until March 12, 2024, as the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction;
6. the Board's observation of a separate incident, disclosed by Microsoft in January 2024, the investigation of which was not in the purview of the Board's review, which revealed a compromise that allowed a different

nation-state actor to access highly-sensitive Microsoft corporate email accounts, source code repositories, and internal systems; and

7. how Microsoft's ubiquitous and critical products, which underpin essential services that support national security, the foundations of our economy, and public health and safety, require the company to demonstrate the highest standards of security, accountability, and transparency.

Throughout this review, the Board identified a series of Microsoft operational and strategic decisions that collectively point to a corporate culture that deprioritized both enterprise security investments and rigorous risk management.

To drive the rapid cultural change that is needed within Microsoft, the Board believes that Microsoft's customers would benefit from its CEO and Board of Directors directly focusing on the company's security culture and developing and sharing publicly a plan with specific timelines to make fundamental, security-focused reforms across the company and its full suite of products. The Board recommends that Microsoft's CEO hold senior officers accountable for delivery against this plan. In the meantime, Microsoft leadership should consider directing internal Microsoft teams to deprioritize feature developments across the company's cloud infrastructure and product suite until substantial security improvements have been made in order to preclude competition for resources. In all instances, security risks should be fully and appropriately assessed and addressed before new features are deployed.

Based on the lessons learned from its review and its fact-finding into prevailing security practices across the cloud services industry, the Board, in addition to the recommendations it makes to the President of the United States and Secretary of Homeland Security, also developed a series of broader recommendations for the community focused on improving the security of cloud identity and authentication across the government agencies responsible for driving better cybersecurity, cloud service providers, and their customers.

- **Cloud Service Provider Cybersecurity Practices:** Cloud service providers should implement modern control mechanisms and baseline practices, informed by a rigorous threat model, across their digital identity and credential systems to substantially reduce the risk of system-level compromise.
- **Audit Logging Norms:** Cloud service providers should adopt a minimum standard for default audit logging in cloud services to enable the detection, prevention, and investigation of intrusions as a baseline and routine service offering without additional charge.
- **Digital Identity Standards and Guidance:** Cloud service providers should implement emerging digital identity standards to secure cloud services against prevailing threat vectors. Relevant standards bodies should refine, update, and incorporate these standards to address digital identity risks commonly exploited in the modern threat landscape.
- **Cloud Service Provider Transparency:** Cloud service providers should adopt incident and vulnerability disclosure practices to maximize transparency across and between their customers, stakeholders, and the United States government, even in the absence of a regulatory obligation to report.
- **Victim Notification Processes:** Cloud service providers should develop more effective victim notification and support mechanisms to drive information-sharing efforts and amplify pertinent information for investigating, remediating, and recovering from cybersecurity incidents.
- **Security Standards and Compliance Frameworks:** The United States government should update the Federal Risk Authorization Management Program and supporting frameworks and establish a process for conducting discretionary special reviews of the program's authorized Cloud Service Offerings following especially high-impact situations. The National Institute of Standards and Technology should also incorporate feedback about observed threats and incidents related to cloud provider security.

1 FACTS

1.1 OVERVIEW

In May 2023, a threat actor known as Storm-0558[1] compromised the Microsoft Exchange Online mailboxes of a broad range of victims in the United States (U.S.), the United Kingdom (U.K.), and elsewhere. Storm-0558, assessed by multiple sources to pursue espionage objectives and maintain ties with the People's Republic of China (PRC),[2, 3] accessed email accounts in the U.S. Department of State (State Department, or State), U.S. Department of Commerce (Commerce Department, or Commerce), and U.S. House of Representatives.[4] This included the official and personal mailboxes of U.S. Commerce Secretary Gina Raimondo; Congressman Don Bacon; U.S. Ambassador to the PRC, R. Nicholas Burns; Assistant Secretary of State for East Asian and Pacific Affairs, Daniel Kritenbrink;[5] and additional individuals across 22 organizations.[6] These senior officials have substantial responsibilities for many aspects of the U.S. government's bilateral relationship with the PRC. Storm-0558 had access to some of these cloud-based mailboxes for at least six weeks,[7, 8] and during this time, the threat actor downloaded approximately 60,000 emails from State Department alone.[9]

State Department was the first victim to discover the intrusion when, on June 15, 2023, State's security operations center (SOC) detected anomalies in access to its mail systems.[10] The next day, State observed multiple security alerts from a custom rule it had created, known internally as "Big Yellow Taxi,"[11] that analyzes data from a log known as MailItemsAccessed, which tracks access to Microsoft Exchange Online mailboxes. State was able to access the MailItemsAccessed log to set up these particular Big Yellow Taxi alerts because it had purchased Microsoft's government agency-focused G5 license that includes enhanced logging capabilities through a product called Microsoft Purview Audit (Premium).[12] The MailItemsAccessed log was not accessible without that "premium" service.[13]

Though the alerts showed activity that could have been considered normal—and, indeed, State had seen false positive Big Yellow Taxi detections in the past—State investigated these incidents and ultimately determined that the alert indicated malicious activity. State triaged the alert as a moderate-level event and, on Friday, June 16, 2023, its security team contacted Microsoft.[14, 15] Microsoft opened and conducted an investigation of its own, and over the next 10 days, ultimately confirmed that Storm-0558 had gained entry to certain user emails through State's Outlook Web Access (OWA). Concurrently, Microsoft expanded its investigation to identify the 21 additional impacted organizations and 503 related users impacted by the attack and worked to identify and notify impacted U.S. government agencies.[16]

Microsoft initially assumed that Storm-0558 had gained access to State Department accounts through traditional threat vectors, such as compromised devices or stolen credentials. However, on June 26, 2023, Microsoft discovered that the threat actor had used OWA to access emails directly using tokens that authenticated Storm-0558 as valid

---

[1] Microsoft uses its internal naming taxonomy to label threat actors based on several characteristics including country of origin, infrastructure, and objectives. *Source: Lambert, John; Microsoft, "Microsoft shifts to a new threat actor naming taxonomy," April 18, 2023, https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/*
[2] Anonymized.
[3] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[4] Anonymized.
[5] Schappert, Stefanie; CyberNews, "*Another US Congressman reveals emails hacked by China*," November 15, 2023, https://cybernews.com/news/us-congressman-emails-hacked-china-microsoft/
[6] Anonymized.
[7] Anonymized.
[8] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[9] State Department, "*Department Press Briefing – September 28, 2023*," September 28, 2023, https://www.state.gov/briefings/department-press-briefing-september-28-2023/
[10] Anonymized.
[11] Sakellariadis, John and Miller, Maggie; Politico, "*All thanks to 'Big Yellow Taxi': How State discovered Chinese hackers reading its emails*," September 15, 2023, https://www.politico.com/news/2023/09/15/digital-tripwire-helped-state-uncover-chinese-hack-00115973
[12] State Department, Board Meeting.
[13] Microsoft, "*Compare Office 365 Government Plans: Microsoft 365*," https://www.microsoft.com/en-us/microsoft-365/enterprise/government-plans-and-pricing
[14] Anonymized.
[15] State Department, Board Meeting.
[16] Microsoft, Board Meeting.

users. Such tokens should only come from Microsoft's identity system, yet these had not. Moreover, tokens used by the threat actor had been digitally signed with a Microsoft Services Account (MSA)[17] cryptographic key that Microsoft had issued in 2016. This particular MSA key should only have been able to sign tokens that worked in consumer OWA, not Enterprise Exchange Online. Finally, this 2016 MSA key was originally intended to be retired in March 2021, but its removal was delayed due to unforeseen challenges associated with hardening the consumer key systems.[18] This was the moment that Microsoft realized it had major, overlapping problems: first, someone was using a Microsoft signing key to issue their own tokens; second, the 2016 MSA key in question was no longer supposed to be signing new tokens; and third, someone was using these consumer key-signed tokens to gain access to enterprise email accounts.

According to Microsoft, this discovery triggered an all-hands-on-deck investigation by Microsoft that ran overnight from June 26 into June 27, 2023, focusing on the 2016 MSA key that had issued the token as well as the access token itself. By the end of the day, Microsoft had high confidence that the threat actor had forged a token using a stolen consumer signing key. Microsoft then escalated this intrusion internally, assigning it the highest urgency level and coordinating its investigation across multiple company teams. As a result, Microsoft developed 46 hypotheses to investigate, including some scenarios as wide-ranging as the adversary possessing a theoretical quantum computing capability to break public-key cryptography or an insider who stole the key during its creation. Microsoft then assigned teams for each hypothesis to try to: prove how the theft occurred; prove it could no longer occur in the same way now; and to prove Microsoft would detect it if it happened today. Nine months after the discovery of the intrusion, Microsoft says that its investigation into these hypotheses remains ongoing.[19]

Microsoft began notifying potentially impacted organizations and individuals on or about June 19 and July 4, 2023, respectively.[20, 21] As detailed below, this effort had varying degrees of success. Ultimately, Microsoft determined that Storm-0558 used an acquired MSA consumer token signing key to forge tokens to access Microsoft Exchange Online accounts for 22 enterprise organizations, as well as 503 related personal[22] accounts, worldwide.[23] Of the 503 personal accounts reported by Microsoft, at least 391 were in the U.S. and included those of former government officials,[24] while others were linked to Western European, Asia-Pacific (APAC), Latin American, and Middle Eastern countries and associated victim organizations.[25, 26, 27]

Microsoft found no sign of an intrusion into its identity system and, as of the conclusion of this review, has not been able to determine how Storm-0558 had obtained the 2016 MSA key; it did find a flaw in the token validation logic used by Exchange Online that could allow a consumer key to access enterprise Exchange accounts if those Exchange accounts were not coded to reject a consumer key. By June 27, 2023, Microsoft believed it had identified the technique used to access victim accounts and rapidly cleared related caching data in various downstream Microsoft systems to invalidate all credentials derived from the stolen key. Microsoft believed that this mitigation was effective, as it almost immediately observed Storm-0558 begin to use phishing to try to gain access to the email boxes it had previously compromised.[28] However, by the conclusion of this review, Microsoft was still unable to demonstrate to the Board that it knew how Storm-0558 had obtained the 2016 MSA key.

---

[17] Consumer accounts are validated by MSA consumer signing keys, and Azure AD accounts are validated through Azure AD enterprise signing keys. As these keys are from separate providers, and managed in separate systems, they should not be able to validate for the other system. *Source: SecureTeam, "Microsoft Key Used for Unauthorised Email Access," July 27, 2023, https://secureteam.co.uk/2023/07/27/microsoft-key-used-for-unauthorised-email-access/*

[18] Microsoft, Board Meeting.

[19] Microsoft, Board Meeting.

[20] Anonymized.

[21] Anonymized.

[22] The term "personal" in this context means an individual account. "A Microsoft [personal] account is the name given to the identity service that provides authentication and authorization to Microsoft's consumer services. You use a personal Microsoft account to connect to Microsoft apps, services, and devices." *Source: Microsoft, "What's the difference between a Microsoft account and a Microsoft 365 work or school account?" October 10, 2023, https://support.microsoft.com/en-au/office/what-s-the-difference-between-a-microsoft-account-and-a-microsoft-365-work-or-school-account-72f10e1e-cab8-4950-a8da-7c4533957 5b0*

[23] Microsoft, Board Meeting.

[24] Anonymized.

[25] Microsoft, Board Meeting.

[26] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[27] Microsoft, Response to Board Request for Information.

[28] Microsoft, Board Meeting.

1.2 INTRUSION DETAILS

1.2.1 TIMELINE

The Board finds that the intrusion began in May 2023 and known adversaries' techniques were remediated by the end of June 2023. A high-level timeline follows, and a more complete chronology is included in Appendix B.

May-June 15, 2023: Initial Intrusion, Before Discovery

Storm-0558 compromised Microsoft Exchange Online mailboxes of certain victims in the U.S., the U.K., and elsewhere between May and the first half of June.[29, 30] However, the Board heard that Microsoft's window of compromise may have started earlier than May 15, as it had published, based on standard 30-day log retention practices.[31]

June 15-19, 2023: Department of State Detects the Intrusion

State first detected anomalous activity on June 15, notified Microsoft on June 16, and, with support from Microsoft, investigated and analyzed the data over the course of the holiday weekend. By June 19, State determined that a threat actor had accessed six State email accounts, including those of personnel supporting the Secretary of State's upcoming trip to Beijing. State discovered that the threat actor accessed six other accounts between June 21 and June 24, and later discovered the compromise of one other account through the analysis of a seized virtual private server (VPS).[32]

June 16-26, 2023: The Investigation Broadens; Department of Commerce is Identified as a Victim

State reached out to Microsoft, the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI).[33, 34] CISA already had personnel at State conducting proactive threat hunting who began collecting data for analysis;[35] FBI shared details about the threat actor, its targets and exploitation vectors, and other indicators of compromise.[36, 37] After outreach from State, on June 16, Microsoft conducted an initial investigation, which assumed that Storm-0558 had gained entry to user emails through State's OWA.[38]

On June 19, Microsoft notified an organization in the U.K. that it was a victim; Microsoft later identified other victim organizations in the U.K.[39] On June 23, Microsoft notified Commerce Department that it, too, was a victim.[40] On or about June 26, Microsoft determined that Storm-0558 was using the stolen 2016 MSA key to issue tokens that allowed it to access both consumer and enterprise accounts.[41]

June 24, 2023: Closing the Attack Vector

On June 24, Microsoft invalidated the stolen key the threat actor was using.[42, 43] Microsoft believed that this action ended Storm-0558's access to the email accounts, as it almost immediately observed Storm-0558 attempt phishing and other methods to regain access to the email boxes it had previously compromised.[44]

July 4, 2023 and Beyond: Continue Victim Notification and Remediation

Microsoft began victim notification during its initial investigation, and this continued for weeks. Because of the nature of the intrusion, only Microsoft was able to identify most of the victims. It worked with the U.S. government to provide

[29] Anonymized.
[30] Anonymized.
[31] Anonymized.
[32] State Department, Board Meeting.
[33] FBI, Response to Board Request for Information.
[34] State Department, Board Meeting.
[35] Anonymized.
[36] State Department, Board Meeting.
[37] FBI, Board Meeting.
[38] Microsoft, Board Meeting.
[39] Anonymized.
[40] Commerce Department, Board Meeting.
[41] Microsoft, Board Meeting.
[42] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[43] Anonymized.
[44] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

victim information, and federal agencies undertook separate efforts to notify impacted individuals.[45, 46] These different efforts had varying degrees of success. Microsoft also took additional steps to ensure that the 2016 MSA key was replaced and that previously issued tokens would not work on any impacted individual customers' environments.[47]

1.2.2 THREAT ACTOR PROFILE

Storm-0558 has been active since approximately the year 2000.[48] Microsoft described Storm-0558 as "a China-based threat actor with activities and methods consistent with espionage objectives. While we have discovered some minimal overlaps with other Chinese groups such as Violet Typhoon (ZIRCONIUM, APT31), we maintain high confidence that Storm-0558 operates as its own distinct group." Microsoft historically observed the group primarily targeting U.S. and European diplomatic, economic, and legislative governing bodies; media companies, think tanks, and telecommunications and equipment services providers; and individuals connected to Taiwan and Uyghur geopolitical interests.[49] Microsoft assesses that the Microsoft Exchange Online intrusion was a targeted information-collection operation aimed at fulfilling the PRC's intelligence needs.[50]

Microsoft has developed insights into Storm-0558's activity clusters, ways in which its operational network overlaps with Microsoft's environment, and its affiliates and partnerships.[51] FBI and CISA assess that this latest campaign by Storm-0558 was also consistent with that of a nation-state threat actor with a high level of sophistication,[52] particularly with its knowledge of identity and access management (IAM) systems.[53]

Following disclosure of the Storm-0558 breach, Google's Threat Analysis Group was able to link at least one entity tied to this threat actor to the group responsible for the 2009 compromise of Google and dozens of other private companies in a campaign known as Operation Aurora,[54, 55] as well as the RSA SecurID incident.[56, 57] The threat group believed to have been behind the Operation Aurora campaign has been known to compromise cloud identity systems, steal source code, and engage in token-forging activities to gain access to targeted individuals' email accounts.[58, 59] Particularly, this threat group sought to understand the location of account login source code and the specific engineers involved in its development, ways in which organizations deploy account login systems to their production environment, and where and how organizations manage their cryptographic keys for account login cookies. In the wake of these attacks, investigators assessed that this threat group's tooling and reconnaissance activities suggest that it is well resourced, technically adept, and deeply knowledgeable of many authentication techniques and applications.[60]

---

[45] Anonymized.
[46] Anonymized.
[47] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[48] Anonymized.
[49] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[50] Microsoft, Board Meeting.
[51] Microsoft, Board Meeting.
[52] FBI, Board Meeting.
[53] CISA, Board Meeting.
[54] Google, Board Meeting.
[55] Operation Aurora was a series of cyberattacks from China that targeted U.S. private sector companies in 2010, compromising the networks of Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google, and more than two dozen other companies to steal their trade secrets. Google was the only company that confirmed it was a victim and publicly attributed the incident to China. The incident is viewed as a milestone in the recent history of cyber operations because it raised the profile of cyber operations as a tool for industrial espionage. *Source: Council on Foreign Relations, "Operation Aurora," January 2010, https://www.cfr.org/cyber-operations/operation-aurora*
[56] The 2011 RSA SecureID intrusion resulted in the compromise of sensitive information relating to its two-factor SecurID authentication system. *Source: Schwartz, Mathew; Dark Reading, "RSA Pins SecurID Attacks On Nation State," October 12, 2011, https://www.darkreading.com/cyberattacks-data-breaches/rsa-pins-securid-attacks-on-nation-state*
[57] Anonymized.
[58] O'Gorman, Gavin and McDonald, Geoff; Symantec, "*The Elderwood Project*," September 6, 2012, https://www.cs.cornell.edu/courses/cs6410/2012fa/slides/Symantec_ElderwoodProject_2012.pdf
[59] Google specifically described the attack as a highly sophisticated and targeted attack on their corporate infrastructure that resulted in theft of intellectual property and access to targeted Gmail accounts. *Source: Google Official Blog, "A new approach to China," January 12, 2010, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html*
[60] Google, Board Meeting.

1.2.3 2023 COMPROMISE OF MICROSOFT EXCHANGE ONLINE

1.2.3.1 Storm-0558's Possession of the 2016 MSA Key

Microsoft learned that, in 2021, Storm-0558 had accessed a variety of documents stored in SharePoint and assessed that the threat actor was specifically looking for information on Azure service management and identity-related information.[61] Despite Microsoft's pursuit of the 46 key-theft hypotheses,[62] the Board assesses that Microsoft does not know how Storm-0558 obtained the 2016 MSA key. Microsoft stated in a September 6, 2023 blog post that the most probable way Storm-0558 had obtained the key was from a crash dump[63] to which it had access during the 2021 compromise of Microsoft's systems. However, Microsoft had only theorized that such a scenario was technically feasible in the 2016 timeframe. While Microsoft updated this blog on March 12, 2024 to correct its assessment of these theories,[64] it has not determined that this is how Storm-0558 obtained the key.[65]

The Board further determines that Microsoft has no evidence or logs showing the stolen key's presence in or exfiltration from a crash dump. During the Board's interview with Microsoft in November 2023, Microsoft said that soon after publication, it realized that the statements in the September 6 blog were inaccurate: Microsoft had found no evidence of a crash dump containing the 2016 MSA key material.[66] While Microsoft's latest update about this incident acknowledges that it did not find a crash dump containing the impacted 2016 MSA key material,[67] the possibility that the threat actor had accessed other keys and sensitive data, in addition to the 2016 MSA key, also remains unresolved,[68] adding to the Board's concern about the full consequences of the incident and remaining uncertainty.

In its November 2023 interview, Microsoft also told the Board that it was debating when to issue a new or updated blog based on the progress of its investigation but had not made any decisions.[69] In a written response to the Board on March 5, 2024, Microsoft maintained that it "intends to publish an update to the blog in the near future."[70] Over six months after its publication of the September 6 blog, and four months after acknowledging to the Board that the blog was inaccurate, Microsoft publicly corrected its mistaken assertions in an addendum, based on its "latest knowledge."[71]

1.2.3.2 How Storm-0558 Used the 2016 MSA Key

Storm-0558 established its first identified component of external hosting infrastructure to execute the Exchange Online intrusion and gained access to email accounts on May 15, 2023.[72] After State notified Microsoft about the intrusion on June 16, 2023, Microsoft reviewed logs pertaining to the event, from the month of May, and identified that the first instance of malicious activity took place days after Storm-0558 had established its infrastructure. Microsoft also said that Storm-0558 had, in the past, used more sophisticated covert networks, but Microsoft believes that a previous disruption of the threat actor's infrastructure forced it to use a less sophisticated infrastructure for this intrusion that was more readily identifiable once discovered.[73] In this instance, Storm-0558 occasionally used infrastructure located geographically near its targets, likely to try to blend in with legitimate activity.[74, 75]

---

[61] Microsoft, Response to Board Request for Information.
[62] Microsoft, Board Meeting.
[63] A system crash (also known as a "bug check" or a "Stop error") occurs when Windows cannot run correctly. The dump file that is produced from this event is called a system crash dump. *Source: Microsoft Learn, "Generate a kernel or complete crash dump," September 2, 2022, https://learn.microsoft.com/en-us/troubleshoot/windows-client/performance/generate-a-kernel-or-complete-crash-dump*
[64] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[65] Microsoft, Board Meeting.
[66] Microsoft, Board Meeting.
[67] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[68] Anonymized.
[69] Microsoft, Board Meeting.
[70] Microsoft, Response to Board Request for Information.
[71] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[72] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[73] Microsoft, Board Meeting.
[74] Anonymized.
[75] Microsoft, Board Meeting.

Microsoft designed its consumer MSA identity infrastructure more than 20 years ago. Later, it introduced an enterprise Entra infrastructure, previously known as Azure Active Directory (AD). Initially, the consumer MSA system had no process for automated signing key rotation or deactivation and utilized a manual process instead. Over time, Microsoft automated the key rotation process in the enterprise system with the intent for the consumer MSA system to follow and use the same technology, but it had not done so in the consumer MSA system before the intrusion. Microsoft continued to rotate consumer MSA keys infrequently and manually until it stopped the rotation entirely in 2021 following a major cloud outage linked to the manual rotation process. While Microsoft had paused manual key rotation, it neither had, nor created, an automated alerting system to notify the appropriate Microsoft teams about the age of active signing keys in the consumer MSA service.[76]

Thus, possession of the 2016 MSA key—dated though it was—enabled the threat actor to forge authentication tokens that allowed it to access email systems. This access should have been limited to consumer email systems,[77] but due to a previously unknown flaw that allowed tokens to access enterprise email accounts, Storm-0558 was able to get into systems such as those at State and Commerce. The flaw was caused by Microsoft's efforts to address customer requests for a common OpenID Connect (OIDC) endpoint service that listed active signing keys for both enterprise and consumer identity systems.[78] However, Microsoft had not adequately updated the software development kits (SDKs), which Microsoft and its partners both used, to differentiate between the consumer MSA and the enterprise signing keys within the common endpoint. As a result, this allowed successful authentication to the Entra system for certain applications, such as mail, regardless of which key was used.[79]

Thus, as illustrated in Figure 1, the stolen 2016 MSA key in combination with the flaw in the token validation system permitted the threat actor to gain full access to essentially any Exchange Online account.[80, 81]

Cloud Service Vulnerabilities

Cloud service providers (CSPs) do not always register and publicly disclose common vulnerabilities and exposures (CVEs) in their cloud infrastructure when mitigating those vulnerabilities does not require customer action.[82] This lack of disclosure, which is counter to accepted norms for cybersecurity more generally, makes it difficult for CSP customers to understand the risks posed by their reliance on potentially vulnerable cloud infrastructure.[83]

Microsoft does not know when Storm-0558 discovered that consumer signing keys (including the one it had stolen) could forge tokens that worked on both OWA consumer and enterprise Exchange Online. Microsoft speculates that the threat actor could have discovered this capability through trial and error. It assessed that during this incident, the actor was researching Microsoft technologies and used this knowledge to pivot and circumvent Microsoft's security measures within test cloud tenants.[84]

[76] Microsoft, Board Meeting.
[77] Microsoft, Board Meeting.
[78] OpenID providers like the Microsoft identity platform provide an OpenID Provider Configuration Document at a publicly accessible endpoint containing the provider's OIDC endpoints, supported claims, and other metadata. Client applications can use the metadata to discover the URLs to use for authentication and the authentication service's public signing keys. *Source: Microsoft; "OpenID Connect on the Microsoft identity platform," October 23, 2023, https://learn.microsoft.com/en-us/entra/identity-platform/v2-protocols-oidc*
[79] Microsoft, Board Meeting.
[80] Anonymized.
[81] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[82] Anonymized.
[83] Anonymized.
[84] Microsoft, Board Meeting.

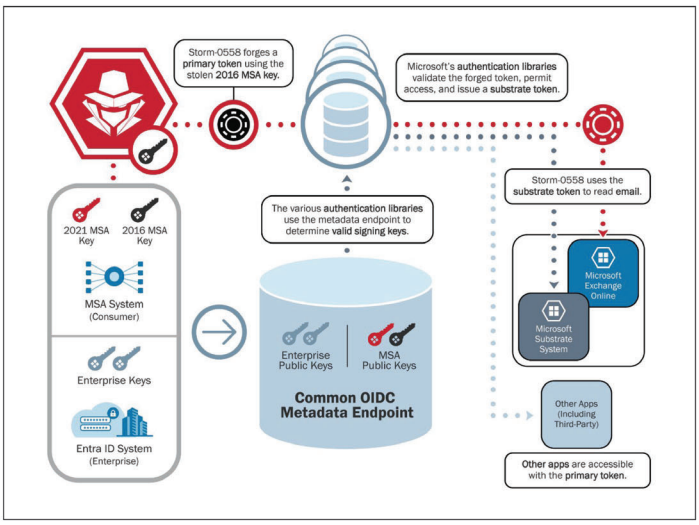


Figure 1: Storm-0558 Token Abuse with Stolen 2016 MSA Key

1.2.4 2021 COMPROMISE OF MICROSOFT CORPORATE NETWORK BY STORM-0558

Microsoft told the Board that Storm-0558 had compromised Microsoft's corporate network via an engineer's account, which occurred between April and August 2021. Microsoft believes, although it has produced no specific evidence to such effect, that this 2021 intrusion was likely connected to the 2023 Exchange Online compromise because it is the only other known Storm-0558 intrusion of Microsoft's network in recorded memory. During this 2021 incident, Microsoft believes that Storm-0558 gained access to sensitive authentication and identity data.[85]

As announced on March 26, 2020 and completed on April 23, 2020, Microsoft acquired a company called Affirmed Networks[86] that worked in 5G technology and advanced networking. Microsoft believes that prior to the acquisition, Storm-0558 targeted an engineer and compromised their device due to their experience in 5G technology and advanced networking. After the acquisition, Microsoft supplied corporate credentials to the acquired engineer that allowed access to Microsoft's corporate environment with the compromised device. Leveraging this access, Storm-0558 captured an authentication token, then replayed the token to authenticate as the Microsoft employee on Microsoft's corporate network.[87, 88]

[85] Microsoft, Board Meeting.
[86] Khalidi, Yousef; Microsoft, "*Microsoft announces agreement to acquire Affirmed Networks to deliver new opportunities for a global 5G ecosystem*," March 26, 2020, https://blogs.microsoft.com/blog/2020/03/26/microsoft-announces-agreement-to-acquire-affirmed-networks-to-deliver-new-opportunities-for-a-global-5g-ecosystem/
[87] Microsoft, Board Meeting.
[88] Anonymized.

While Storm-0558 exhibited an advanced understanding of Microsoft's network and demonstrated a particular interest in information associated with identity and engineering, Microsoft does not have direct evidence linking the two incidents. Microsoft's insider threat investigation also did not find evidence to indicate that a malicious insider was a part of the 2023 intrusion. Through its ongoing investigations, Microsoft said it believes that alternative initial access vectors, such as an insider threat, remain unlikely.[89]

Still, the 2021 compromise of Microsoft's corporate network highlights gaps within the company's mergers and acquisitions (M&A) security compromise assessment and remediation process. Microsoft told the Board that, where applicable and based on the risk profile associated with the acquisition and the terms of the agreement, Microsoft deploys telemetry and threat intelligence tools to assess whether an acquisition has been compromised, and remediation can occur pre- or post-closing. Microsoft and the acquisition target formalize a security incident response process to coordinate security incidents until close. Following the acquisition, Microsoft's internal audit team may conduct security audits of an acquisition leveraging findings from due diligence security assessments to inform the scope of these assessments.[90]

1.2.5 INCIDENT IMPACT

The Microsoft Exchange Online intrusion was significant: Storm-0558's combined possession of the 2016 MSA key and its ability to access enterprise Exchange accounts allowed the threat actor to access any Microsoft Exchange Online account. Although Microsoft expressed confidence resulting both from extensive log analysis and direct actor tracking that this intrusion only impacted Microsoft Exchange Online, the stolen key also could have been used by the threat actor to access other Microsoft cloud applications had it chosen to do so. These include both Microsoft and third-party applications reliant on Microsoft's identity provider (IDP) that were either intentionally (due to supporting consumer accounts) or unintentionally (due to using client libraries or bespoke code that failed to properly validate authentication tokens) trusting tokens signed by the stolen key.[91, 92, 93] Microsoft believes that Storm-0558 itself limited the scope of this intrusion, as it appeared to be selective in its targeting, balancing its information-gathering objectives with probabilities of detection.[94] The Board believes that the actor also prioritized high-value and time-sensitive collection missions.

Yet while the number of victims was relatively low given the breadth of the access available to the actor, they were widespread: Storm-0558 accessed the email accounts of 22 enterprise organizations,[95] including government agencies and three think tanks.[96] This intrusion also impacted the personal accounts of individuals likely associated with these organizations.[97] The non-U.S. victims included four foreign government entities, three private sector organizations, and four educational entities.[98]

Impacted U.K. Accounts
Storm-0558 compromised several U.K. organizations' email accounts and exfiltrated an unknown number of emails. Initially, Microsoft reported three affected accounts to the National Cyber Security Centre (NCSC),[99] but further investigation by Microsoft revealed additional victims. This discovery underscores both the evolving nature of this incident's impact assessment and the delayed victim identification.[100] The Board has not learned why these U.K. individuals were chosen over others.

[89] Microsoft, Board Meeting.
[90] Microsoft, Response to Board Request for Information.
[91] Anonymized.
[92] Microsoft, Board Meeting.
[93] Anonymized.
[94] Microsoft, Board Meeting.
[95] Microsoft, Board Meeting.
[96] Anonymized.
[97] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[98] Anonymized.
[99] NCSC, the U.K.'s version of FBI Cyber Division, supports the most critical organizations in the U.K., the wider public sector, industry, subject matter experts, and the general public. *Source: NCSC, "What we do," https://www.ncsc.gov.uk/section/about-ncsc/what-we-do*
[100] NCSC, Board Meeting.

Microsoft knew the identity of all of the individuals whom Storm-0558 targeted, many of whom were linked to entities associated with Western European, APAC, Latin American, and Middle Eastern countries.[101, 102] Of these accounts, the intrusion impacted at least 391 personal email accounts in the U.S,[103] including some Hotmail accounts belonging to current and former employees of an affected government organization.[104]

The threat actor compromised the official and personal mailboxes of many senior U.S. government officials, some of which likely contained information about the U.S.'s diplomatic and economic policies toward the PRC. The timing of the intrusion, just before Secretary Blinken's trip to Beijing in 2023, combined with the seniority of the officials targeted, highlights a potential partial rationale for such intrusions.[105]

1.3 INCIDENT MANAGEMENT

1.3.1 HOW STATE DEPARTMENT DISCOVERED THE INTRUSION

State Department was the first entity to detect the intrusion when on June 16, 2023, a State SOC analyst observed multiple alerts from the "Big Yellow Taxi" custom alert rule. Detecting an intrusion like this is difficult; State Department found Storm-0558 because it had purchased enhanced logging through the G5 licenses,[106] which few, if any, victims had similarly acquired.[107] As standard practice, State's SOC uses that enhanced logging to build custom alerts like "Big Yellow Taxi" in response to an evolving threat environment.[108] Just purchasing the additional logging alone would not have been enough; in fact, the Board heard that few organizations analyzed the voluminous MailItemsAccessed log in detail, and such in-depth analysis would be difficult for smaller organizations.

State, however, used the data to build custom detection rules to enable it to identify anomalous access to mailboxes such as the activity undertaken in this intrusion. State Department's SOC designed custom alerting capabilities based on three years of experience dealing with anomalous access to mailboxes. In particular, State curated log events like the MailItemsAccessed data to enumerate all applications accessing mailboxes within its infrastructure, and to trigger alerts for any anomalous events.[109] It also designed a rule to detect deviations in mailbox activity by comparing baseline interactions of applications with Exchange Online.[110] These rules provided detailed information about application IDs touching mailboxes, specific application details, and context about particular mailboxes involved, thereby enhancing State's ability to pinpoint potential issues quickly.[111]

1.3.2 INVESTIGATION AND ANALYSIS

1.3.2.1 Microsoft's Investigation

After receiving State Department's report on June 16, 2023, Microsoft began an initial investigation using its normal processes, which involved Microsoft's Detection and Response Team (DART). Microsoft attributed the intrusion to Storm-0558 after identifying infrastructure associated with the threat actor. This investigation continued until June 26, 2023. At the time, Microsoft determined the impact was larger in scope and may have involved the compromise of Microsoft's systems. Specifically, Microsoft discovered the threat actor was able to access emails directly using forged tokens signed with a consumer token signing key that was supposed to have been inactive. Once it identified and revoked the stolen 2016 MSA key, Microsoft was able to use the key to inform its hunting efforts: since the key was inactive at this point, the Microsoft identity system was not using it to sign any tokens. Thus, all signing instances using this key constituted nefarious activity. This insight helped Microsoft determine that its identity system had not issued the invalid tokens and identify threat actor activities with high confidence,[112] meaning the threat actors had an MSA

[101] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[102] Microsoft, Response to Board Request for Information.
[103] Anonymized.
[104] Anonymized.
[105] Anonymized.
[106] State Department, Board Meeting.
[107] Anonymized.
[108] State Department, Board Meeting.
[109] State Department, Board Meeting.
[110] Anonymized.
[111] State Department, Board Meeting.
[112] Microsoft, Board Meeting.

key that could be used to issue working—though fraudulently issued—tokens that could grant application access to mailboxes within the enterprise environment.[113]

In response, on June 26, 2023, Microsoft launched an overnight investigation focusing on the key and token and assessed with high confidence that the threat actor had forged a token using a consumer MSA key that should have been inactive. Upon confirming that Storm-0558 had forged the token, Microsoft began converging individual processes into its Software and Services Incident Response Plan (SSIRP), which has different urgency levels based on multiple criteria, including the number of impacted customers. On June 27, 2023, Microsoft assigned this intrusion a SEV-0 rating, the highest urgency level. This meant that the incident required robust communication, visibility, and coordination across Microsoft and up to its most senior leadership, including its Board of Directors.[114]

Microsoft's incident response plan leverages several specialty teams that coordinate response for large and small incidents. While some incidents are local, like a good faith researcher reporting a vulnerability that can be repaired without needing cross-team coordination, in this case Microsoft leveraged its standardized global security response processes, allowing it to coordinate across multiple teams and establish separate workstreams for containment, customer impact, incident notifications, and investigating the key's exfiltration. For the last workstream, it assembled team members from DART, the Microsoft Threat Intelligence Center (MSTIC), and various security teams to hypothesize potential egress points for the key. This collaborative effort generated the three sub-workstreams dedicated to investigating Microsoft's 46 hypotheses.[115]

After reexamining the 2021 compromise of the engineer and analyzing what Storm-0558 could have accessed using the stolen credentials at that time, Microsoft determined that it needed to expand its investigation to scan for the presence of the 2016 MSA key across its network. Microsoft told the Board that it continues to engage in this work. Additionally, after Microsoft put protections in place to prevent future token generation by invalidating the key, it saw the actor experiment and unsuccessfully attempt to generate new tokens.[116, 117] Storm-0558's use of the invalid key to sign authentication requests allowed Microsoft's teams to determine the scope of the threat actor's access.[118] Microsoft found no evidence of a breach in the perimeter of the signing system. During the investigation, Microsoft examined the threat actor's targeting methods, and looked for evidence of a compromise or the introduction of an external device into the corporate network as possible attack vectors. The investigation uncovered what Microsoft believes is the precise number of targeted individuals, and enabled Microsoft's acquisition of the malware that Storm-0558 used to sign tokens for accessing OWA. This discovery was pivotal in focusing the search across Microsoft's logs for any additional threat activity. Microsoft has not yet determined how Storm-0558 obtained the 2016 MSA key and says that it is continuing to investigate.[119]

1.3.2.2 Investigations by Victim Organizations

Victims found it difficult to investigate these intrusions after initial detection because Microsoft could not, or in some cases did not, provide victim organizations with holistic visibility into all necessary data. Although Microsoft activated enhanced logging for identified victims who did not have the appropriate license, Microsoft could not give historical logs to customers unless they already had the premium licenses at the time of the intrusion. Thus, customers could capture data from the time that Microsoft enabled additional logging capabilities but were unable to view past intrusion activity.

State's SOC had limited visibility into the activity but, based on the particular email accounts that the threat actor accessed, quickly determined that the targeted individuals were supporting the Secretary's upcoming trip to Beijing. This approach significantly aided State in refining its analysis of the activity. Later joined in its response by the National Security Agency (NSA), CISA, and Microsoft, State confirmed the intrusion into the mailboxes on June 19, 2023. It then began a comprehensive investigation to understand what was happening and what the actor had exfiltrated. On June 21, 2023, after issuing a legal process to the U.S.-based VPS provider that hosted the attacker's infrastructure, the government obtained a disk image from the provider that contained valuable insights into the threat actor's intrusion

[113] Anonymized.
[114] Microsoft, Board Meeting.
[115] Microsoft, Board Meeting.
[116] Microsoft, Board Meeting.
[117] Anonymized.
[118] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[119] Microsoft, Board Meeting.

attempts and follow-on activity. That same day, the FBI was notified of the intrusion and received this information. In parallel with CISA, FBI conducted an independent analysis on the disk image and made its findings available to the broader group.[120]

Microsoft first notified Commerce's Office of the Chief Information Officer (OCIO) about the intrusion into the Commerce Department's systems on June 23, 2023, one week after State Department's discovery. According to Microsoft's initial reports, Storm-0558 accessed and exfiltrated data from Commerce on June 21, 2023.[121, 122] However, later audit logs provided by Microsoft showed Storm-0558 had initially accessed Commerce data on June 6, 2023.[123]

Commerce Department's Enterprise SOC (ESOC) team immediately contacted CISA for assistance, marking the beginning of the entity's efforts to understand the intrusion.[124] It then asked Microsoft to share relevant logs, and Microsoft provided some data and activated G5 logging. However, Commerce could not view past activity as these logs only captured data from the time that Microsoft enabled the advanced logging. Microsoft told Commerce that it had derived some of its information about the incident from additional logging capabilities available to internal Microsoft teams for monitoring threat actor behavior.[125, 126] Commerce Department asked Microsoft to share these logs so that it could do its own assessment of the incident, including any potential impact to other subordinate bureaus' systems. Microsoft shared certain portions of Commerce's impacted unified audit logs and provided Internet Protocol (IP) addresses that the organization could use to search across its network. This incomplete dataset impacted Commerce Department's ability to do a complete assessment of the incident.[127]

Commerce Department collected all affected user devices, temporarily suspended impacted mailbox usage, and deployed signatures at its ESOC to monitor for and detect related activity. Commerce also shared all signatures with subordinate Bureaus to deploy. To monitor for follow-on threat activity and identify impact beyond initial reporting, Commerce activated G5 logging, but as discussed, it could not analyze historical telemetry for malicious activity because Microsoft could only provide these logs and data going forward—it had not collected and did not possess the data for earlier activity because Commerce did not have the G5 licenses then.[128]

1.3.2.3 Investigations by Government Incident Responders

On June 21, 2023, State Department notified the FBI Washington Field Office's Cyber Task Force that a threat actor had accessed official State mailboxes between June 13 and June 20, 2023. FBI told the Board that Microsoft was critically important to its ability to understand the nature of the compromise, who the targets were, and how the threat actor had exploited the vulnerability. Microsoft also helped FBI in continuing to develop proof of high-level attribution to Storm-0558 and voluntarily provided indicators of compromise (IoCs) for further investigation.[129]

CISA was a central point for information sharing related to detection, mitigation, and remediation across and between federal agencies, and with private sector partners and victims. It also shared guidance to agencies for how to detect this intrusion, specifically to examine their logs, to the extent that they had access to the G5 service level, for unexpected MailItemsAccessed events with irregular application IDs.[130] At the time of the intrusion, CISA was already providing State Department with proactive threat hunting services as part of a routine, by-request engagement. CISA shifted to incident response following State's detection of Storm-0558 activity and analyzed the pattern of threat activity. CISA also collected data and surveyed observations from other stakeholder organizations to search for compromises beyond State.[131]

CISA tried to recreate Storm-0558's activity but could not replicate the forged token as it did not possess the necessary stolen MSA key. Without the 2016 MSA key, CISA could only emulate the incident in a limited way and had to rely on its knowledge of Exchange Online and logs from State Department to conduct its investigation. Leveraging tokens it

[120] State Department, Board Meeting.
[121] Anonymized.
[122] Commerce Department, Board Meeting.
[123] Commerce Department, Board Meeting.
[124] Commerce Department, Response to Board Request for Information.
[125] Commerce Department, Board Meeting.
[126] Anonymized.
[127] Commerce Department, Board Meeting.
[128] Commerce Department, Board Meeting.
[129] FBI, Board Meeting.
[130] Anonymized.
[131] CISA, Board Meeting.

generated in OWA, similar to those used by Storm-0558, CISA conducted a test to emulate the application programming interface (API) used by the threat actor to exfiltrate email. Subsequent forensics on the threat actor's tooling validated that CISA's emulation accurately reflected Storm-0558's activities other than the initial token forgery. As a result of this emulation work, CISA assessed that the threat actor could not avoid generating the MailItemsAccessed log data during the intrusion, which meant that it could detect similar future activity if it had the relevant logs.[132]

CISA also worked with international partners; the NCSC engaged CISA during the first week of its investigation after realizing the breadth of the intrusion. The NCSC told the Board that the conversations were useful as the NCSC and CISA shared information on intrusion impacts and each organization's respective engagement with Microsoft.[133]

While Microsoft has longstanding relationships with CISA, in this instance, Microsoft delayed reaching out to CISA until it could confirm additional details of the intrusion. Microsoft did not know the root cause of the intrusion for some time and was reluctant to share data with CISA and others until it had more certainty. CISA reached out to Microsoft to share its investigative efforts, at which point Microsoft confirmed that it had observed CISA's replication of the intrusion using a test commercial tenant. As a result of this outreach, Microsoft further engaged with CISA and provided detailed briefings, disclosing how it had uncovered Storm-0558's presence within its network and providing details on the nature and methodology of the threat actor. During these discussions, Microsoft provided some of the intrusion's technical details and gave CISA limited access to its forensics about the threat actor's infrastructure.[134]

International Partners: NCSC

The U.K. victims did not have enhanced logging capabilities, which inhibited the NCSC's ability to verify Microsoft's claims of earlier threat activity. During its response, the NCSC had to balance disabling the compromised environment with leaving it operational so it could further analyze the intrusion and ensure that Storm-0558 could not regain access if the NCSC's mitigations failed to close the underlying vulnerability.[135]

Based on Microsoft's initial advice, the NCSC suspected the threat actor was likely stealing tokens from endpoints, particularly iOS devices. This led the NCSC to gather as many devices as possible from victims over the first two days of its investigation. However, this theory proved fruitless, highlighting the difficulty that organizations faced in determining the intrusion's attack vector. By the second week of the NCSC's investigation, Microsoft had revoked the key and the NCSC's focus shifted from stopping malicious activity to identifying exfiltrated data. Finally, by mid-July, the NCSC turned its attention to examining potentially compromised corporate accounts.[136]

1.3.3 VICTIM COORDINATION AND NOTIFICATION

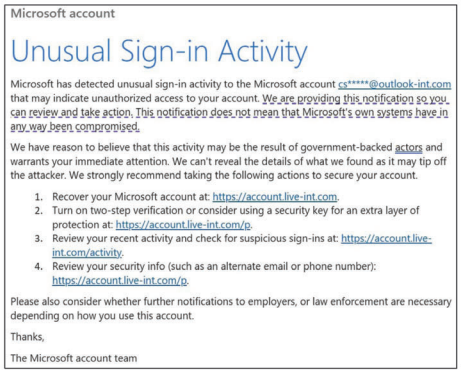
Victim coordination was complicated for this incident as it involved multiple U.S. government agencies, foreign governments, senior government officials, private sector organizations, and private individuals. While both Microsoft and government agencies undertook separate efforts to notify victims, Microsoft had legal and contractual limitations on what victim information it could share with the government, absent victim consent.[137]

FBI worked with Microsoft to obtain the U.S. victim information, and on July 10, 2023, Microsoft lawfully provided FBI with a list of affected email accounts and related subscriber information for those accounts. FBI engaged directly with almost every victim with an affected personal account. For compromised enterprise accounts, FBI worked with system owners, who in turn informed individuals whose accounts were part of the intrusion.[138]

By July 25, 2023, FBI had identified the owners of nearly all affected accounts and had begun issuing leads to notify government officials deemed to have the most sensitive information, in line with FBI Cyber Division policy on victim notification requirements. FBI learned that some victims were unaware that a threat actor had accessed their emails. Microsoft informed FBI that it had notified customers through several methods, including short message service (SMS)

[132] CISA, Board Meeting.
[133] NCSC, Board Meeting.
[134] CISA, Board Meeting.
[135] NCSC, Board Meeting.
[136] NCSC, Board Meeting.
[137] Microsoft, Board Meeting.
[138] FBI, Board Meeting.

text messages, nation-state notifications (NSNs),[139] emails sent to recovery accounts (see Figure 2), and pop-up messages via an authenticator application, but some victims told FBI that they viewed these notifications as possible spam and disregarded them. As a result, FBI changed its stance and notified every identified account owner through coordination with FBI field offices, Department of Justice (DoJ), CISA, State, and Commerce. FBI provided each victim with a joint Cybersecurity Advisory previously published by FBI and CISA on July 12, 2023, as well as a copy of Microsoft's blog outlining analysis of Storm-0558 activity and cyber hygiene best practices.[140]



Microsoft account

Unusual Sign-in Activity

Microsoft has detected unusual sign-in activity to the Microsoft account cs*****@outlook-int.com that may indicate unauthorized access to your account. We are providing this notification so you can review and take action. This notification does not mean that Microsoft's own systems have in any way been compromised.

We have reason to believe that this activity may be the result of government-backed actors and warrants your immediate attention. We can't reveal the details of what we found as it may tip off the attacker. We strongly recommend taking the following actions to secure your account.

1. Recover your Microsoft account at: https://account.live-int.com.
2. Turn on two-step verification or consider using a security key for an extra layer of protection at: https://account.live-int.com/p.
3. Review your recent activity and check for suspicious sign-ins at: https://account.live-int.com/activity.
4. Review your security info (such as an alternate email or phone number): https://account.live-int.com/p.

Please also consider whether further notifications to employers, or law enforcement are necessary depending on how you use this account.

Thanks,

The Microsoft account team

Figure 2: Microsoft Victim Notification Email

Case Study: Congressman Don Bacon

Congressman Don Bacon is a Member of the House of Representatives and currently serves on the House Armed Services Committee, including its Strategic Forces and Tactical Air and Land Forces subcommittees. Congressman Bacon is also a member of the House Taiwan Caucus.[141] As a prominent congressional voice on national security matters, Congressman Bacon is a high-value target for adversarial intelligence-gathering objectives. Microsoft's first noticed outreach to Congressman Bacon about the intrusion was an email prompting him to change his password, sent a month before FBI contacted him. Congressman Bacon thought the password change email looked strange and was potentially fraudulent, so he changed his password directly rather than using the link provided in the notification instructions. He later learned from FBI that his personal email had been compromised. FBI assured him that his devices were secure and that he had done nothing wrong; rather, the intrusion originated from a compromise affecting Microsoft. Microsoft did not advise Congressman Bacon to take any action to protect his account beyond the one email recommending a password change. At some point after the initial password change email, Microsoft sent another that provided details about the intrusion, including that Microsoft believed it had been synchronized with Secretary of State Antony Blinken's visit, June 16 to June 21, 2023, and Commerce Secretary Gina Raimondo's visit, August 27 to August 30, 2023, to China.[142]

---

[139] Whenever an organization or individual account holder is targeted or compromised by observed nation-state activities, Microsoft delivers an NSN directly to that customer to give them the information they need to investigate the activity. *Source: Lambert, John; Microsoft, "Microsoft Digital Defense Report shares new insights on nation-state attacks," October 25, 2021, https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/*

[140] FBI, Board Meeting.

[141] United States Congress, "*Committees and Caucuses*," https://bacon.house.gov/about/committees-and-caucuses.htm

[142] Rep. Don Bacon, Board Meeting.

From July 4 to July 14, 2023, Microsoft issued notifications to 63 high-profile individuals in the U.K.[143] who were identified as having been directly targeted or compromised by observed nation-state activities. However, the NCSC was concerned that some victims may not pay attention to these notifications even though the notifications may point to a widely reported incident. All Enterprise NSNs explicitly identified Storm-0558 as the PRC-affiliated threat actor, and a dedicated team issued an individualized NSN to each affected person. This process is unique to NSNs and is distinct from the notifications sent to other personal victims via email or other automated methods.[144] The NCSC provided the most sensitive impacted individuals with tailored and dedicated briefings summarizing the intrusion and asked victims what data may have been exfiltrated from their emails. The NCSC explored all available avenues and obtained the victim identities through a difficult, time-consuming process.[145]

1.3.4 REMEDIATION AND RECOVERY

Between June 24 and July 3, 2023, to remediate Storm-0558's activity, Microsoft:

1) revoked the key's ability to sign tokens and cleared related caching data stored in downstream systems;[146]
2) accelerated an update to change the way that Exchange Online accepted tokens, blocking any requests using the same method as Storm-0558 had used to exploit the vulnerability;[147, 148]
3) fixed the flaw that allowed unauthorized access to enterprise data with consumer keys by updating various software packages within its applications and rapidly deploying these updates across its systems;[149]
4) rotated other signing keys for enterprise and consumer tokens, issuing the new keys from enterprise infrastructure that it deemed safer;
5) enhanced how it monitors and alerts for suspicious activities within its identity systems, a process Microsoft was continuing to refine at the time of its discussion with the Board;[150] and
6) developed and tailored contextual guides that detailed the intrusion and provided them to organizations and individual customers.[151]

Microsoft's Engagement with the PRC Government

Given the culpability of a PRC-affiliated threat actor in this compromise, the Board was pleased to be told that Microsoft first contacted the PRC government only after it had remediated the incident, having its first communication with the PRC government on August 17, 2023. Typically, Microsoft directly engages with the PRC government at a high level after incidents such as this. In this case, Microsoft published a blog in July 2023, and its legal teams engaged in follow-on discussions with the PRC government.[152]

1.4 PUBLIC REPORTING

On July 11, 2023, Microsoft published its first blog about the Exchange Online intrusion, disclosing that Storm-0558 had used an MSA consumer signing key that enabled it to forge authentication tokens and access Exchange Online and

[143] Anonymized.
[144] Anonymized.
[145] NCSC, Board Meeting.
[146] Microsoft, Board Meeting.
[147] Microsoft identified the design flaw within the GetAccessTokensForResources API. Source: Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[148] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[149] Anonymized.
[150] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[151] Microsoft, Board Meeting.
[152] Microsoft, Board Meeting.

Outlook accounts.[153] Microsoft stated that it had notified all impacted customers and launched an investigation,[154, 155] and publicly named Commerce as an affected entity; however, the Board learned that Microsoft did not provide Commerce forewarning that the blog post would publicly name Commerce as an affected entity.[156]

Microsoft published a second blog on July 14, 2023, filling some gaps in the first blog post, including indicators and technical details. This second post also provided insights into detecting the attacker infrastructure. Microsoft also provided details on the scale of the intrusion, characteristics of Storm-0558's infrastructure, and portions of the malware the threat actor had used to conduct the intrusion.[157] Researchers in the security community scrutinized the timing and content of Microsoft's second blog, and identified gaps and inconsistencies in Microsoft's public accounts of the intrusion, including tactics, techniques, and procedures (TTPs), IoCs, and indicators of attack (IoA).[158]

In response to Microsoft's blogs, Wiz, a cloud security company, launched a limited independent review of the incident. Wiz concluded that the compromised 2016 MSA key could sign access tokens for many types of applications, far beyond Microsoft's initial reporting. For Wiz, this revelation underscored the need for a broader awareness and proactive measures across all affected stakeholders.[159] CISA also conducted an in-depth review of Microsoft's public statements. CISA's findings pointed to the need for greater clarity and transparency from Microsoft about the initial compromise's blast radius, token scope, and impact. Specifically, CISA noted information gaps in what additional capabilities the stolen key granted the threat actor, Microsoft's incident response measures, and the potential for threat actors to access internal servers or additional key material.[160]

On September 6, 2023, Microsoft published a third blog, entitled "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*." This blog stated that, "Our investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ('crash dump')." The blog went on to say that "a race condition allowed the key to be present in the crash dump" and that the crash dump "was subsequently moved from the isolated production network into our debugging environment on the internet connected corporate network." Finally, Microsoft said that the engineer's account that Storm-0558 had compromised in 2021 "had access to the debugging environment containing the crash dump which incorrectly contained the key" and while it had no logs showing the actual exfiltration, "this was the most probable mechanism by which the actor acquired the key."[161]

As Microsoft continued to investigate, it determined that elements of the September 6 blog related to how the actor acquired the impacted customer token signing key were likely inaccurate. Microsoft told the Board that although the blog stated its "technical investigation has concluded," it continued to investigate the threat actor and subsequently determined that while a crash dump could have included key material and that such a dump could have been moved out of the secure token signing environment, Microsoft had not found any dump containing this key material, as it had mistakenly asserted in the September 6 blog.[162]

During the Board's interview with Microsoft in November 2023, Microsoft told the Board that it was considering issuing a new or updated blog on its ongoing investigative findings, but that it had not yet made any decisions in that regard. In this meeting, Microsoft confirmed that although its investigation into how the threat actor obtained the key material had been ongoing, it had no change in the number of customers impacted, depth of impact, or time of impact. At that time, Microsoft intended to publish an update to the blog in the near future.[163] In a written response to follow-up questions on this topic from the Board, Microsoft responded, "We believe that describing how the company is

---

[153] MSRC; Microsoft, "*Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*," July 11, 2023, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
[154] Tamari, Shir; Wiz, "*Compromised Microsoft Key: More Impactful Than We Thought*," July 21, 2023, https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr
[155] Anonymized.
[156] Commerce Department, Board Meeting.
[157] Microsoft Threat Intelligence; Microsoft, "*Analysis of Storm-0558 techniques for unauthorized email access*," July 14, 2023, https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
[158] Anonymized.
[159] Tamari, Shir; Wiz, "*Compromised Microsoft Key: More Impactful Than We Thought*," July 21, 2023, https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr
[160] CISA, Board Meeting.
[161] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023, https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[162] Microsoft, Board Meeting.
[163] Microsoft, Board Meeting.

considering updating its public statements would entail disclosure of attorney-client privileged information. However, we will continue to assess the September 6, 2023 blog, including whether to update it, upon completion of the investigation."[164]

On March 12, 2024, Microsoft published an addendum to its September 6 blog that provided further information as it related to Microsoft's ongoing investigation. In its update, Microsoft clarified that, in the past, its standard debugging process did not prohibit the ability to move crash dump material out of the secure signing environment, indicating that such a scenario was once possible. Microsoft's statement also confirmed that the race condition discussed above could allow the crash dump to move from the secure token signing environment, but would not impact whether the 2016 MSA key could be present in the crash dump.[165]

Ultimately, this March 12 addendum maintained that Microsoft's "leading hypothesis remains that operational errors resulted in key material leaving the secure token signing environment that was subsequently accessed in a debugging environment via a compromised engineering account." Still, Microsoft did not recant its initial crash dump theory as a likely root cause, as it initially implied in its September 6 blog.[166] At the conclusion of the Board's review, even in the context of Microsoft's March 12 update, Microsoft has not identified a crash dump that contains the 2016 MSA key, or any other evidence of the key having been moved inappropriately.

[164] Microsoft, Response to Board Request for Information.
[165] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
[166] MSRC; Microsoft, "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," September 6, 2023 (updated March 12, 2024), https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

2 FINDINGS AND RECOMMENDATIONS

2.1 CLOUD SERVICE PROVIDERS

2.1.1 MICROSOFT CORPORATE SECURITY CULTURE

The Board concludes that Microsoft's security culture was inadequate. The Board reaches this conclusion based on:

1. the cascade of Microsoft's avoidable errors that allowed this intrusion to succeed;
2. Microsoft's failure to detect the compromise of its cryptographic crown jewels on its own, relying instead on a customer to reach out to identify anomalies the customer had observed;
3. the Board's assessment of security practices at other CSPs, which maintained security controls that Microsoft did not;
4. Microsoft's failure to detect a compromise of an employee's laptop from a recently acquired company prior to allowing it to connect to Microsoft's corporate network in 2021;
5. Microsoft's decision not to correct, in a timely manner, its inaccurate public statements about this incident, including a corporate statement that Microsoft believed it had determined the likely root cause of the intrusion when in fact, it still has not; even though Microsoft acknowledged to the Board in November 2023 that its September 6, 2023 blog post about the root cause was inaccurate, it did not update that post until March 12, 2024, as the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction;
6. the Board's observation of a separate incident, disclosed by Microsoft in January 2024, the investigation of which was not in the purview of the Board's review, which revealed a compromise that allowed a different nation-state actor to access highly-sensitive Microsoft corporate email accounts, source code repositories, and internal systems; and
7. how Microsoft's ubiquitous and critical products, which underpin essential services that support national security, the foundations of our economy, and public health and safety, require the company to demonstrate the highest standards of security, accountability, and transparency.

If Microsoft had not paused manual rotation of keys; if it had completed the migration of its MSA environment to rotate keys automatically; if it had put in place a technical or other control to generate alerts for aging keys, the 2016 MSA key would not have been valid in 2023. Further, if Microsoft had not made the error that allowed consumer keys to authenticate to enterprise customer data (or, alternatively, if it had detected and addressed this flaw), the scope of the intrusion would have been far narrower and would not have impacted the State Department, Commerce Department, or any other enterprise customers. If Microsoft had deployed alerting or prevention to detect forged tokens that do not conform to Microsoft's own token generation algorithms, this incident likely could also have been stopped or detected by Microsoft all on its own. Even after all this, if Microsoft had other security controls in place for its digital identity system—as the Board finds other CSPs had in place at the time—this intrusion vector could have been blocked or detected. Finally, once State Department alerted Microsoft to the intrusion, Microsoft did not have the logs or other forensic data to determine how or when Storm-0558 had stolen the key.

The decision to completely stop manual rotation of signing keys in 2021 after a large cloud outage, along with failing to prioritize the development of an automated key rotation solution, are troubling examples of decision-making processes within the company that did not prioritize security risk management at a level commensurate with the threat and with Microsoft technology's vital importance to more than one billion of its customers worldwide. Taken together with the inadequate controls in the authentication system to detect and mitigate key theft after multiple attempts by the threat actor to compromise identity and authentication systems, including in Operation Aurora in 2009 and RSA SecureID in 2011—something that all other major CSPs have worked to address in their systems' architectures—the Board finds that Microsoft had not sufficiently prioritized rearchitecting its legacy infrastructure to address the current threat landscape. In addition, the failure to detect the compromise of an employee's laptop in an acquired company in 2021, prior to allowing it to connect to Microsoft's corporate network, raises questions about the robustness of Microsoft's M&A compromise assessment program.

The Board is also concerned with Microsoft's public communications after the incident. In its September 6, 2023 blog post entitled "*Results of Major Technical Investigations for Storm-0558 Key Acquisition*," Microsoft explained that Storm-0558 likely stole the 2016 MSA key in the "crash dump" scenario described above. However, soon after publishing that blog, Microsoft determined it did not have any evidence showing that the crash dump contained the 2016 MSA key. This led Microsoft to assess that the crash dump theory was no longer any more probable than other theories as the mechanism by which the actor had acquired the key, which Microsoft chose to leave uncorrected for more than six months after publishing its September 6 blog.

The Board is troubled that Microsoft neglected to publicly correct this known error for many months. Customers (private sector and government) relied on these public representations in Microsoft's blogs. The loss of a signing key is a serious problem, but the loss of a signing key through unknown means is far more significant because it means that the victim company does not know how its systems were infiltrated and whether the relevant vulnerabilities have been closed off. Left with the mistaken impression that Microsoft has conclusively identified the root cause of this incident, Microsoft's customers did not have essential facts needed to make their own risk assessments about the security of Microsoft cloud environments in the wake of this intrusion. Microsoft told the Board early in this review that it believed that the errors in the blog were "not material." The Board disagrees. After several written follow up questions from the Board regarding the blog, Microsoft informed the Board on March 5, 2024, that it would be updating the blog in the "near future." One week following this communication, and more than six months after its publication of the September 6 blog, Microsoft corrected its mistaken assertions through an addendum to the blog's existing webpage.

The Board also takes note of a separate incident that Microsoft disclosed in January 2024. This disclosure revealed a compromise that allowed a different nation-state actor, which Microsoft calls Midnight Blizzard and the U.S. government has previously attributed to the Russian Foreign Intelligence Service (SVR),[167] to access highly-sensitive Microsoft corporate email accounts.[168] Nearly two months later, Microsoft published a new blog post stating that Midnight Blizzard had also gained unauthorized access to some of Microsoft's source code repositories and internal systems.[169] While this second intrusion was outside of the scope of the Board's current review, the Board is troubled that this new incident occurred months after the Exchange Online compromise covered in this review. This additional intrusion highlights the Board's concern that Microsoft has not yet implemented the necessary governance or prioritization of security to address the apparent security weaknesses and control failures within its environment and to prevent similar incidents in the future.

Individually, any one of the failings described above might be understandable. Taken together, they point to a failure of Microsoft's organizational controls and governance, and of its corporate culture around security.

Microsoft's products and services are ubiquitous. It is one of the most important technology companies in the world, if not the most important. This position brings with it utmost and global responsibilities. It requires a security-focused corporate culture of accountability, which starts with the CEO, to ensure that financial or other go-to-market factors do not undermine cybersecurity and the protection of Microsoft's customers.

Unfortunately, throughout this review, the Board identified a series of operational and strategic decisions that collectively point to a corporate culture in Microsoft that deprioritized both enterprise security investments and rigorous risk management. These decisions resulted in significant costs and harm for Microsoft customers around the world. The Board is convinced that Microsoft should address its security culture.

In 2002, Microsoft's founder and then-CEO, Bill Gates, wrote an email to the entire Microsoft workforce on the importance of prioritizing security in product development. He wrote:

> So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid e-mail-borne viruses. If we discover a risk that a feature could compromise someone's

[167] CISA, "*SVR Cyber Actors Adapt Tactics for Initial Cloud Access*," February 26, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a
[168] MSRC; Microsoft, "*Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*," January 19, 2024, https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
[169] MSRC; Microsoft, "*Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*," March 8, 2024, https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

> privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services. [170]

The Board concludes that Microsoft has drifted away from this ethos and needs to restore it immediately as a top corporate priority. The Board is aware of Microsoft's recent changes to its security leadership and the "Secure Future Initiative" that it announced in November 2023.[171] The Board believes that these and other security-related efforts should be overseen directly and closely by Microsoft's CEO and its Board of Directors, and that all senior leaders should be held accountable for implementing all necessary changes with utmost urgency. The Board recommends the following:

- **RECOMMENDATION 1:** Microsoft's customers would benefit from its CEO and Board of Directors directly focusing on the company's security culture. The CEO and Board should develop, and share publicly, a plan with specific timelines to make fundamental, security-focused reforms across the company and its full suite of products, and then hold leaders at all levels of the company accountable for its implementation. Given the company's critical importance to its more than one billion customers and the national security of this nation and, indeed, the entire world, progress in this area should be rapid and substantial.
- **RECOMMENDATION 2:** Microsoft leadership should consider directing internal Microsoft teams to deprioritize feature developments across the company's cloud infrastructure and product suite until substantial security improvements have been made. In all instances, security risks should be fully and appropriately assessed and addressed before new features are deployed.
- **RECOMMENDATION 3:** As noted in the National Cybersecurity Strategy, "The most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem. Today, end users bear too great a burden for mitigating cyber risks."[172] Microsoft and all CSPs should heed this call and take accountability for the security outcomes of their customers, ensuring that senior leaders make security a business priority, creating internal incentives and fostering an across-the-board culture to make security a design requirement.
- **RECOMMENDATION 4:** The Board notes that some CSPs, including Microsoft until recently, offer granular logging, which can be invaluable in security incident detection, investigation, and response—as a part of a paid package offering to their core services. This course of business should stop. Security-related logging should be a core element of cloud offerings and CSPs should provide customers the foundational tools that provide them with the information necessary to detect, prevent, or quantify an intrusion, recognizing that many customers will still require additional or third-party analytic capabilities to build a fully mature security program.

2.1.2 CSP CYBERSECURITY PRACTICES

During this review, the Board identified best practices drawn from all CSPs that would materially improve the security of cloud systems. These include automated regular key rotation; storage of keys in segmented and isolated key systems (e.g., hardware security modules [HSMs] or similar); use of stateful token validation; limiting scope of keys (e.g., to individual customers in some cases); use of proprietary data in token generation algorithms that could allow for detection of adversary-forged tokens that may not include such data; and the use of tokens bound to particular operations or sessions rather than broad bearer tokens.

As a result of threat actors targeting authentication and identity systems in the 2009 Operation Aurora intrusions,[173, 174] the Board found that other CSPs recognized the importance of addressing this threat model by implementing different approaches to secure their identity systems. This is unsurprising and appropriate, as each CSP is different and

---

[170] Wired, "*Bill Gates: Trustworthy Computing*," January 17, 2002, https://www.wired.com/2002/01/bill-gates-trustworthy-computing/
[171] Smith, Brad; Microsoft, "*A new world of security: Microsoft's Secure Future Initiative*," November 2, 2023, https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/
[172] The White House, "*National Cybersecurity Strategy*," March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[173] Anonymized.
[174] Google, Board Meeting.

should choose a security architecture best suited to its technological infrastructure and customer use cases, such as those demonstrated in the following examples.

- Google re-worked its identity system to rely as much as possible on stateful tokens, in which every credential is assigned a unique identifier at issuance and recorded in a database as irreversible proof that the credential Google receives is one that it had issued. Google also implemented fully automatic key rotation where possible and tightened the validation period for stateless tokens, reducing the window of time for threat actors to locate and obtain active keys. Google also undertook a comprehensive overhaul of its infrastructure security including implementing Zero Trust networks and hardware-backed, Fast IDentity Online (FIDO)-compliant two-factor authentication (2FA) to protect these identity systems.[175]
- Similarly, the Amazon Web Services (AWS) IAM Signature Version 4 (SigV4) protocol provides each customer with unique authentication keys for each of their users or roles, but these keys are not bearer tokens nor are they used directly for signing. Having no tokens, these credentials are not susceptible to token replay. Instead, highly compartmentalized signing keys are cryptography-derived, and each request is signed in a way that can only authorize the same specific action, which can be safely retried.[176]
- Oracle Cloud Infrastructure also enables and requires each customer tenancy to have its own public-private key pair that signs each request sent on an encrypted Transport Layer Security (TLS) connection, in a token spoofing-resistant manner.[177]

CSPs should implement security architectures with a level of security commensurate with their critical role in the ecosystem by making decisions through sound engineering practices that are based on an informed threat model. This is especially true for core digital identity systems. CSPs should also collect forensics in their production and corporate environments so that they can determine the true cause of any intrusion (which was not the case with the stolen 2016 MSA key).

The Board therefore recommends that CSPs adopt the following security practices, or their equivalents, as needed to achieve the high level of security they require.

- **RECOMMENDATION 5:** Given Microsoft's inability to determine how and when the adversary was able to steal its signing key, all CSPs should review and revise as appropriate their logging and overall forensics capabilities around their identity systems and other systems that enable environment-level compromise, such as root key material. CSPs should maintain sufficient forensics to detect exfiltration of those data, including logging all access to those systems and any private keys stored within them. These logs should be analyzed continuously for any unauthorized insider or external threat actor activity. Retention should include all time the key was in active use and extend at least two years beyond the expiration of that key. Longer retention periods of at least 10 years may be appropriate for some high-value log types.
- **RECOMMENDATION 6:** CSPs should engineer their digital identity and credential systems in such a way that substantially reduces the risk of complete system-level compromise. This should be an overriding, top-priority, design goal in the engineering process and be informed by a rigorous threat model developed by the CSP in response to its understanding of the threat landscape. The Board spoke with all major U.S.-based CSPs to gain an understanding of their existing practices and develop a set of recommended baseline best practices. While the specific practices implemented may vary for different use cases and situations, the Board believes technical mechanisms exist today across the industry that can, if broadly implemented, significantly reduce the likelihood of complete system-level compromise. Each of these practices is implemented by at least one major CSP, demonstrating their technical feasibility. Some of these practices, while compatible with accepted industry standards, would also benefit from additional standards development, which is discussed in another recommendation. These mechanisms include the following.[178]

[175] Google, Board Meeting.
[176] AWS, Board Meeting.
[177] Oracle, Board Meeting.
[178] Each of these mechanisms would have, if in place at the time of the incident, aided in the prevention, impact reduction, or detection of the reviewed incident. For some mechanisms, as outlined in the Facts section and in the Recommendations, partial implementation aided in the response to this incident. Broad implementation across CSPs would enhance the resilience of critical digital identity systems.

- **Stateful tokens**: Microsoft's authentication system accepted a token that it had not issued. By storing records in a database when tokens are issued and validating against that database at access time, CSPs may enforce that only tokens issued by the CSP can access customer data. Note: this approach is not possible for use with third-party services reliant on an IDP maintained by a cloud provider.
- **Automated frequent key rotation**: Microsoft paused manual key rotations for its MSA system in 2021 but did not remove the 2016 MSA key. By rotating encryption keys frequently (e.g., monthly) and in an automated manner with monitoring of rotation systems, CSPs can ensure that the blast radius of a compromised key is limited in duration.
- **Per customer keys (key scope)**: Microsoft had a single key that signed tokens for all consumer, and due to the validation flaw, enterprise customers. Tying encryption keys to customer tenancy would limit the scope of key compromise.
- **Bound tokens**: Microsoft's identity system used bearer tokens that did not require any proof of possession, thus making the tokens more vulnerable to replay attacks. By digitally binding tokens to specific requests or network sessions, token theft and token replay attacks can be eliminated. While this incident demonstrates the risks of key compromise, some victims and responders spent significant time investigating bearer token replay attacks to which not all CSPs are vulnerable.
- **Common authentication libraries**: Microsoft used a variety of different client libraries to verify tokens across different systems. This diversity complicated implementing uniform, and correct, validation behavior, as well as made the remediation efforts much more complex and time sensitive. By ensuring that all CSP services use the same authentication libraries, CSPs can more effectively enforce consistent token validation behavior and authorization policy.
- **Secure key storage**: While Microsoft separated the organization and production environments, this incident illustrated that Microsoft insufficiently protected MSA system key material. By storing key material in isolated systems and leveraging, where feasible, technologies such as dedicated HSMs, the risk of key compromise can be reduced. The Board recognizes that in some situations and levels of scale, traditional HSM technology may not be viable but believes that the core idea of isolated key storage with minimal key release is appropriate.
- **Linkable tokens**: The relationship between the tokens used in this incident was not exposed in logs made available to customers, making them difficult to track. By linking all tokens derived from a single root authentication event together and exposing this linking to their customers in logs, CSPs and customers can better track and discover identity-related attacks and respond, including in an automated way.
- **Proprietary data use in token generation algorithm:** Some CSPs inject proprietary data into their generated authentication tokens, which they can use to differentiate between tokens that their own systems generated and those generated by malicious third parties. While one cannot rely on the fact that the adversary would not detect and reproduce such behavior, it can nevertheless prove potentially helpful as a "canary in the coal mine" alert that the CSP is observing tokens that had not been generated by its own code.

- **RECOMMENDATION 7:** CISA should validate annually with major CSPs that provide services to the U.S. government which of these and other applicable security practices they are implementing. CISA should publish the results of its validation review (including stating that a company refused to provide requested information if that is the case).
- **RECOMMENDATION 8:** The National Institute of Standards and Technology (NIST) and the Risk Management Framework (RMF) Joint Task Force (JTF) should update Special Publication (SP) 800-53's control catalog to better account for risks to cloud-based digital identity systems, including incorporating the technical recommendations of the Board from this incident, as appropriate.
- **RECOMMENDATION 9:** Large enterprises need robust compromise assessment and remediation processes for entities they acquire or with whom they merge. These processes should recognize that smaller, acquiree companies may have less robust security procedures and that adversaries may view them as an entry point

onto a parent company's corporate network. This can include targeting them after announcement of an acquisition but before closing.

2.1.3 AUDIT LOGGING NORMS

Logging is essential to detection, investigation, and remediation of potential intrusions. In this case, the logs State Department used to detect this incident (MailItemsAccessed) are of critical value and have enabled detection of other nation-state compromises involving Exchange Online. Despite this obvious utility, these logs, and similar logs at other CSPs, are not available for all types of critical business data stored by CSPs. The Board recommends the following.

- **RECOMMENDATION 10:** CSPs, as part of a CISA-led task force, should define and adopt a minimum standard for default audit logging in cloud services. This standard should, at a minimum, ensure that all access (including access by the CSP itself) to customer business data in the cloud produces logs that are available to the customer without additional charges, with a minimum default retention of six months by the CSP.

2.1.4 DIGITAL IDENTITY STANDARDS AND GUIDANCE

The Board finds that the current ecosystem of Digital Identity standards does not provide the security necessary to counter modern threat actors, and that some CSPs have not sufficiently prioritized implementing emerging standards that improve the security of digital identity systems. This is both a current problem (the need to implement emerging standards) and a long-term need (upleveling the security bar of digital identity standards). The Board recommends the following.

- **RECOMMENDATION 11:** CSPs should implement emerging standards such as Open Authorization (OAuth) 2 Demonstrating Proof-of-Possession (DPoP) (bound tokens) and OpenID Shared Signals and Events (SSE) (sharing session risk) that better secure cloud services against credential related attacks.
- **RECOMMENDATION 12:** Relevant standards bodies should refine and update these standards to account for a threat model of advanced nation-state attackers targeting core CSP identity systems.
- **RECOMMENDATION 13:** CSPs and relevant standards bodies, such as OpenID Foundation (OIDF), Organization for the Advancement of Structured Information Standards (OASIS), and The Internet Engineering Task Force (IETF), should develop or update profiles for core digital identity standards such as OIDC and Security Assertion Markup Language (SAML) to include requirements and/or security considerations around key rotation, stateful credentials, credential linking, and key scope.

2.1.5 CSP TRANSPARENCY

Customers rely on CSPs for more than their cloud services—they rely on CSPs to be transparent about security incidents and vulnerabilities, as these disclosures will influence decisions the customers make about their own risk tolerance and investment decisions, along with necessary transparency to their own customers, clients, and regulators. Moreover, these customers reasonably expect that CSPs will update them, in a timely manner, about security incidents as investigations evolve, including correcting any information that later proves to be wrong. Finally, the U.S. government relies on CSPs to share information about incidents with a potential national security nexus, including suspected nation-state intrusions. During its review, the Board finds that Microsoft fell short, as, for many months, it chose to not update the September 6 blog that incorrectly implied that the 2016 MSA key had been stolen from a crash dump and that it had identified and corrected the issues that led to the adversary stealing the key.

The Board recommends that all CSPs adopt transparency and disclosure practices commensurate with their customers' needs and expectations, including the following.

- **RECOMMENDATION 14:** U.S.-based CSPs should report all incidents suspected to have been perpetrated by an actor affiliated with a nation-state targeting their infrastructure and corporate systems to the U.S. government, even in the absence of a regulatory obligation to report. Separately, CISA and the Office of Management and Budget (OMB) should consider appropriate contractual provisions with CSPs to require such reporting.[179]

[179] CISA, "*Cyber Incident Reporting for Critical Infrastructure Act of 2022*," March 9, 2022, https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf

- **RECOMMENDATION 15:** CSPs should be transparent to U.S. government agencies, customers, and other stakeholders on what they know as well as what they do not know when initially investigating a cyber incident.
- **RECOMMENDATION 16:** CSPs should promptly correct significant factual inaccuracies as they discover them in their public or customer statements.
- **RECOMMENDATION 17:** CSPs should commit to disclosing through the CVE process all vulnerabilities, including flaws such as the one in Microsoft's token validation logic and those that do not require customer action to patch. CSPs should work with the CVE program to develop necessary updates to Common Weakness Enumeration (CWE) to account for the particulars of cloud environments. CSPs should collaborate with the CVE Program to develop these norms and commit to timely and comprehensive disclosure of these vulnerabilities, enabling organizations to make thoughtful risk decisions about all their vendors' security programs, including cloud services. The Board believes that incorporating all known vulnerabilities across the entire technology stack in CVE's comprehensive repository would be a public benefit for industry and government customers, as well as security researchers.

2.1.6 VICTIM NOTIFICATION PROCESSES

Victim notification in cyber incidents is never simple and can be even more complicated when attackers compromise cloud-based services. In this intrusion, the Board found that some victims ignored or did not see the notifications, and some who saw them believed them to be spam or phishing. In some cases, Storm-0558 compromised the personal accounts of some government employees, but Microsoft was initially unable to share the employee's names with their employer due to legal restrictions and recommended the U.S. government issue a warrant for the information so it could provide those details. This impacted and delayed the agencies' ability to aid their employees in responding to that aspect of the intrusion.

The Board recommends that CSPs and the U.S. government improve processes for notifying individuals of intrusions, including ensuring receipt of such notifications, to include the following.

- **RECOMMENDATION 18:** CSPs and the U.S. government, in conjunction with major mobile device platform vendors, should develop a targeted, quickly recognizable "amber alert" style victim notification mechanism for high-impact situations. The alert should be more readily distinguishable from notification emails, which are frequently mistaken by victims for phishing, building on some existing mechanisms for NSNs within platform providers' ecosystems where the mobile device operating system can send a native system alert about the compromise of an end user's CSP account, such as a push notification.
- **RECOMMENDATION 19:** CSPs should develop a process to identify and categorize high-impact incidents involving compromised accounts that present higher risks to national security, such as those of government officials. CSPs should verify whether the victim is in receipt of the notifications; provide guidance to the victim on how they can further protect their information; and detail next steps based on the severity or type of incident, particularly when the victim is targeted by a nation-state actor.
- **RECOMMENDATION 20:** CSPs and the U.S. government should develop mechanisms to incentivize and enable CSPs to connect victims with the appropriate U.S. government resources, international partners, and different sets of victims. These mechanisms should enable collaborative investigation and sharing of best practices to break down silos and barriers that create independent and duplicative investigative workstreams, even within U.S. government and allied partner agencies.

2.2 U.S. GOVERNMENT

2.2.1 SECURITY STANDARDS AND COMPLIANCE FRAMEWORKS

A large, vibrant, and diverse ecosystem of secure cloud services is important for the economic competitiveness of the U.S. and the execution of the U.S. government's varied missions.

Cloud services are a critical component of the cybersecurity ecosystem, especially when they protect the most sensitive government data. However, the Board finds that existing compliance requirements for government cybersecurity do not consistently require sound practices around key management or token issuance. To address this, the Federal Risk

Authorization Management Program (FedRAMP) can play a key role in ensuring stronger cybersecurity practices, including in cloud-based digital identity, across the cloud service ecosystem.

FedRAMP

FedRAMP was established by OMB in December 2011 to promote the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies.

The General Services Administration (GSA) operates the FedRAMP Program Management Office (PMO) and is governed by the FedRAMP Board. FedRAMP leverages many controls that are published in NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations."

The Board concludes that a more flexible tailoring of security controls for cloud-based digital identity systems provides a path to balance the importance of securing these systems with the other important goal of supporting such an ecosystem. To that end, the Board recommends updating 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. Specifically, the Board recommends the following.

- **RECOMMENDATION 21:** FedRAMP, in coordination with OMB and CISA, should establish a minimum threshold for periodically re-evaluating legacy FedRAMP authorization packages. For example, some FedRAMP authorized packages are for services that have become especially widely used across the government while others may be considered High Value Assets (HVA) that may merit more regular review. FedRAMP should consult with CISA and NIST to identify additional relevant security requirements for critical components (such as digital identity access) of these higher-risk FedRAMP authorized providers, and how to effectively tailor security baselines to focus cloud provider effort on addressing these requirements. This threshold should drive the priority in which FedRAMP PMO re-reviews FedRAMP authorized security packages for continuous data monitoring.
- **RECOMMENDATION 22:** FedRAMP should work with OMB to establish a Technical Advisory Group (TAG). The TAG should be available to FedRAMP for consultation for technical, strategic, and operational direction. The TAG should regularly provide recommendations on security best practices and ways to iteratively improve FedRAMP continuous monitoring requirements and guidance.
- **RECOMMENDATION 23:** FedRAMP should establish a process for conducting discretionary special reviews of FedRAMP authorized Cloud Service Offerings (CSOs) that convene security experts within the federal government to make recommendations for security improvements for the CSO. Recommendations from these reviews should inform the issuance (or continuation) of a FedRAMP authorization. FedRAMP should establish criteria for these reviews that limit their scope to especially high-impact situations.
- **RECOMMENDATION 24:** FedRAMP should strengthen the minimum audit logging standards (e.g., FedRAMP Assignment of AU-2) to align with the goal of logging access to sensitive business data (including by the CSP itself). FedRAMP should further require that these logs be made available to customers (not just the CSP itself) at no additional cost.
- **RECOMMENDATION 25:** NIST is encouraged to continue releasing point updates to add and remove controls from its security and privacy control baselines to maintain focus on contemporary threats, and to consult with the FedRAMP program to incorporate feedback about observed threats and incidents related to cloud provider security.

APPENDIX A: REVIEW PARTICIPANTS – EXTERNAL PARTIES

The Board's review involved organizations and individuals representing a variety of viewpoints, including targeted organizations, law enforcement, CSPs, cloud security, incident response, regulators, cybersecurity and industry experts, and others. The Board requested information in the form of briefings and written materials.

The Board is grateful for the voluntary participation of those parties that provided timely responses. Their efforts helped the Board collect the observable timeline of events, corroborate facts, and understand the complex and nuanced dimensions of the Microsoft Exchange Online intrusion and related cloud identity topics.

RELATED BRIEFINGS

The Board engaged with 20 organizations with expertise in cloud security, cloud identity, and/or the Microsoft Exchange Online intrusion. Those organizations are identified below.

- Amazon Web Services, Inc.
- Broadcom Inc.
- Canadian Centre for Cyber Security
- CrowdStrike Holdings, Inc.
- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- Federal Risk and Authorization Management Program (FedRAMP)
- Google LLC
- International Business Machines Corporation (IBM)
- Lacework, Inc.
- Mandiant, Inc.
- Microsoft Corporation
- National Security Agency (NSA)
- Office of the Director of National Intelligence (ODNI)
- Office of Representative Don Bacon
- Oracle Corporation
- U.K. National Cyber Security Centre (NCSC)
- U.S. Department of Commerce
- U.S. Department of State
- Wiz Inc.

APPENDIX B: MICROSOFT EXCHANGE ONLINE INTRUSION TIMELINE

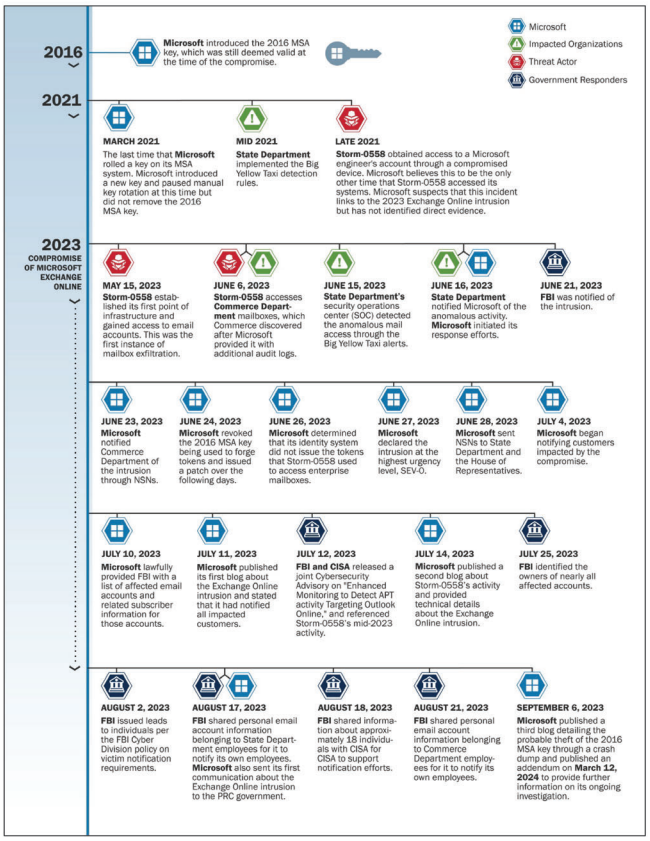


Figure 3: Microsoft Exchange Online Intrusion Timeline

APPENDIX C: REVIEW PARTICIPANTS – CSRB MEMBERS

The Cyber Safety Review Board members listed below participated in the review of the Summer 2023 Microsoft Exchange Online intrusion in the following roles and capacity.

Federal members serve in their official capacity and act on behalf of their agency or department. Private sector members have been appointed as Special Government Employees (SGEs) for the purposes of serving on the Cyber Safety Review Board. SGEs serve in their individual capacity, though current affiliations are included in the list below.

Robert Silvers, (*Chair*), Under Secretary for Policy, representing the Department of Homeland Security

Dmitri Alperovitch, (*Deputy Chair*), Co-Founder and Chairman, Silverado Policy Accelerator

Jake Braun, Acting Principal Deputy National Cyber Director, representing the Office of the National Cyber Director

Jerry Davis, Senior Vice President, Cyber Operations and Technology, Truist Bank

Chris DeRusha, Federal Chief Information Security Officer, representing the Office of Management and Budget

Eric Goldstein, Executive Assistant Director for Cybersecurity, representing the Cybersecurity and Infrastructure Security Agency

Rob Joyce, Director of Cybersecurity, representing the National Security Agency

Cynthia Kaiser, Deputy Assistant Director, representing the Federal Bureau of Investigation

Marshall Miller, Principal Associate Deputy Attorney General, representing the Department of Justice

Chris Novak, Co-Founder and Managing Director, Verizon Threat Research Advisory Center

Tony Sager, Senior Vice President and Chief Evangelist, Center for Internet Security

John Sherman, Chief Information Officer, representing the Department of Defense

APPENDIX D: ACRONYMS

2FA	two-factor authentication
AD	Active Directory
APAC	Asia-Pacific
API	application programming interface
AWS	Amazon Web Services
CEO	Chief Executive Officer
CISA	Cybersecurity and Infrastructure Security Agency
CSO	Cloud Service Offering
CSP	cloud service provider
CSRB	Cyber Safety Review Board, or the Board
CVE	common vulnerability and exposure
CWE	Common Weakness Enumeration
DART	Detection and Response Team
DoJ	Department of Justice
DPoP	Demonstrating Proof-of-Possession
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk Authorization Management Program
FIDO	Fast IDentity Online
FISMA	Federal Information Security Modernization Act
GSA	General Services Administration
HSM	hardware security module
HVA	High Value Asset
IAM	identity and access management
IDP	identity provider
IETF	The Internet Engineering Task Force
IoA	indicator of attack
IoC	indicator of compromise
IP	Internet Protocol
JTF	Joint Task Force

M&A	mergers and acquisitions
MSA	Microsoft Services Account
MSTIC	Microsoft Threat Intelligence Center
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSN	nation-state notification
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OIDC	OpenID Connect
OIDF	OpenID Foundation
OMB	Office of Management and Budget
OWA	Outlook Web Access
PMO	Project Management Office
PRC	People's Republic of China
RMF	Risk Management Framework
SAML	Security Assertion Markup Language
SDK	software development kit
Sigv4	Signature Version 4
SMS	short message service
SOC	security operations center
SSIRP	Software and Services Incident Response Plan
SVR	Russian Foreign Intelligence Service
TAG	Technical Advisory Group
TLS	Transport Layer Security
TTPs	tactics, techniques, and procedures
U.K.	United Kingdom
U.S.	United States
VPS	virtual private server

Chairman GREEN. Specifically, Storm–0558 assessed Microsoft—accessed Microsoft Exchange accounts using authentication tokens signed by an inactive private encryption key that Microsoft created in 2016.

The Beijing-backed actor obtained tens of thousands of individual U.S. Government emails by compromising the Microsoft Exchange email accounts of U.S. officials working on national security matters relating to China.

The CSRB concluded that this intrusion would've been prevented had Microsoft cultivated a strong security culture, which the CSRB said, "requires an overhaul, particularly in light of the company's

centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations".

By any measure, this cyber intrusion was not sophisticated. It did not involve advanced techniques of cutting-edge technologies. Instead, Storm–0558 exploited basic, well-known vulnerabilities that could've been avoided through basic cyber hygiene.

In other words, this was avoidable. This is extremely concerning, and it falls to this committee to do the due diligence and determine just where Microsoft sits and how it's taken this report to heart.

Our goals today are simple. We want to give the company we put so much faith in as a Government the opportunity to discuss the lessons learned, the actions taken, and, of course, to share where they feel the report could've been wrong.

To be clear, the U.S. Government would never expect a private company to work alone in protecting itself against a nation-state actor. We need to do more work to define roles and responsibilities for public- and private-sector actors in the event of nation-state attacks. Our Nation's adversaries possess advanced cyber capabilities and substantial resources often exceeding the defensive cybersecurity measures available to even the most sophisticated companies. However, we do expect Government vendors to implement basic cybersecurity practices.

Since this is not the first time Microsoft has been the victim of an avoidable cyber attack, and in the light of the report, it's now Congress's responsibility to examine the response to this report. We must restore the trust to the American people, who depend on Microsoft products every day. We also must address broader questions regarding the mitigation of economic and national security risks.

This hearing aims to shed light on these issues and ensure Microsoft has implemented the CSRB's recommendations to safeguard against future breaches.

As we dive into these issues, we need to keep three things in mind.

First, closing the cyber work force gap, my top priority for the committee this year. The security challenges we face as a Nation are compounded by the persistent shortage of cybersecurity professionals. As Microsoft continues its work to invest in our cyber work force, we must harken back to the lessons from the report. Our cyber professionals must be trained to think security first. We must equip them with the right skills to protect our networks and to build our systems' security.

Second, we need to define the role of public and private-sector entities in protecting our networks against nation-state actors. I think the Federal Government has been silent too long on this. These attacks have become increasingly common rather than anomalies. We need clearly defined responsibilities so that we can effectively respond to nation-state attacks on our networks in a private-public partnership.

Finally, we must address a fundamental issue, the economic incentives that drive cybersecurity investments. As the CSRB's report recently revealed, underinvestment in essential security measures exposed critical vulnerabilities. Changing the economic incentives for cybersecurity investment is not about imposing onerous

regulations or stifling innovation; it's about creating an environment where the costs of neglecting cybersecurity are outweighed by the potential benefits of comprehensive security measures.

Today, we will explore the steps Microsoft is taking to strengthen its security culture through its Secure Future Initiative. While I commend Microsoft for announcing steps to reform its security practices, I want to hear today what Microsoft's follow-through has been on those commitments on its past responses to other significant cyber incidents, such as SolarWinds.

One of my biggest concerns is Microsoft's presence in China, our Nation's primary strategic adversary, and the regime's responsibility for the hack we are discussing today. Over the years, Microsoft has invested heavily in China, setting up research and development centers, including the Microsoft Research Asia Center in Beijing. Microsoft's presence in China creates a set of complex challenges and risks, and we have to talk about that today as a part of our discussion on the security issue.

Mr. Smith, as a long-time key leader within Microsoft, I anticipate that you will help us understand the gaps that enabled these recent cyber intrusions. The American people as well as the numerous Federal agencies that depend on Microsoft deserve those assurances that their data and their operations will be protected. Mr. Smith, we appreciate your presence here today and look forward to your testimony.

I also would like to let the Members of the committee know—and listen up, team—that, should your question require an answer that would necessitate movement to a secure location, Mr. Smith will be the only one who knows that answer once you ask the question.

Look, China and Russia, Beijing and Moscow, are watching us right now. If you don't think that's true, you're naive. The last thing we want to do is empower our adversary in any way. Members, if Mr. Smith says the answer would require a secure facility, please accept this and ask another question. The committee staff will determine the best way or mechanism to get you the answer in a secure and Classified manner.

With that, I yield now, and I recognize the Ranking Member for his opening statement.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

JUNE 13, 2024

Each and every day, the U.S. Government depends upon Microsoft cloud services, productivity tools, and operating systems to carry out an array of critical missions. Microsoft is deeply integrated into our Nation's digital infrastructure—a presence that carries heightened respect and heightened responsibility.

We are holding this hearing because of the latest Department of Homeland Security (DHS) Cyber Safety Review Board ("CSRB") report. The report attributed last summer's Microsoft Exchange Online hack, by Storm Zero Five Five Eight, which is backed by the Chinese Communist Party, to "a cascade of security failures at Microsoft".

These determinations were based on a number of findings detailed in the report.

Specifically, Storm Zero Five Five Eight accessed the Microsoft Exchange accounts using authentication tokens signed by an inactive private encryption key that Microsoft created in 2016. The Beijing-backed actor obtained tens of thousands of individual U.S. Government emails by compromising the Microsoft Exchange email accounts of U.S. officials working on national security matters relating to China.

The CSRB concluded that this intrusion would have been prevented if Microsoft had cultivated a strong security culture, which the CSRB said, "requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations".

By any measure, this cyber intrusion was not sophisticated. It did not involve advanced techniques or cutting-edge technologies. Instead, Storm Zero Five Five Eight exploited basic, well-known vulnerabilities that could have been avoided through basic cyber hygiene practices. In other words, this was avoidable.

This is extremely concerning, and it falls to this committee to do the due diligence and determine just where Microsoft sits as a company, and how it has taken this report to heart.

Our goals today are simple. We want to give the company we put so much faith in as a Government the opportunity to discuss lessons learned, actions taken, and of course to share where they feel the report could be wrong.

To be clear, the U.S. Government would never expect a private company to work alone in protecting itself against nation-state attacks.

We need to do more work to define roles and responsibilities for public and private-sector actors in the event of nation-state attacks on our networks. Our Nation's adversaries possess advanced cyber capabilities and substantial resources, often exceeding the defensive cybersecurity measures available to even the most sophisticated companies.

However, we do expect Government vendors to implement basic cybersecurity practices.

Since this is not the first time Microsoft has been the victim of an avoidable cyber attack, and in light of the CSRB's report, it is now Congress's responsibility to examine Microsoft's response to this report. We must restore the trust of the American people, who depend upon Microsoft products every day. We must also address broader questions regarding the mitigation of economic and national security risks.

This hearing aims to shed light on these issues and ensure that Microsoft has implemented the CSRB's recommendations to safeguard against future breaches.

As we dive into these issues, we need to keep 3 themes in mind.

First, closing the cyber workforce gap—my top priority for the committee this year. The security challenges we face as a Nation are compounded by the persistent shortage of cybersecurity professionals.

As Microsoft continues its work to invest in our cyber workforce, we must harken back to the lessons from the CSRB report. Our cyber professionals must be trained to think of security first. We must equip them with the right skills to protect our networks and to build our systems securely.

Second, we need to define the role of public and private-sector entities in protecting our networks against nation-state actors.

These attacks have become increasingly common, rather than anomalies.

We need clearly-defined responsibilities so that we can effectively respond to nation-state attacks on our networks.

Finally, we must address a fundamental issue: the economic incentives that drive cybersecurity investments. As the CSRB's report recently revealed, underinvestment in essential security measures exposed critical vulnerabilities.

Changing the economic incentives for cybersecurity investment is not about imposing onerous regulations or stifling innovation.

It is about creating an environment where the costs of neglecting cybersecurity are outweighed by the potential benefits of comprehensive security measures.

Today, we will explore the steps Microsoft is taking to strengthen its security culture through its Secure Future Initiative. While I commend Microsoft for announcing steps to reform its security practices, I want to hear about Microsoft's follow-through on its stated commitments in the long term—based largely on its past responses to other significant cyber incidents, such as SolarWinds.

One of my biggest concerns is Microsoft's presence in China—our Nation's primary strategic adversary and the regime responsible for the hack we are discussing today. Over the years, Microsoft has invested heavily in China, setting up research and development centers, including its Microsoft Research Asia Center in Beijing. Microsoft's presence in China creates a set of complex challenges and risks that we must also talk about today as part of our discussion about a strong security culture.

Mr. Smith, as a long-time, key leader within Microsoft, I anticipate that you will help us understand the gaps that enabled these recent cyber intrusions. The American people, as well as the numerous Federal agencies that depend on Microsoft, deserve assurances that their data and operations are protected.

Mr. Smith, we appreciate your presence here today and look forward to your testimony.

I also would like to let the Members of the committee know that should their question require an answer that would necessitate movement to a secure location, Mr. Smith will be the only one who knows that once the question is asked.

Look, China and Russia are watching this right now. The last thing we want is to empower our adversaries in any way.

Members, if Mr. Smith says the answer would require a secure facility, please accept this and ask another question. The committee staff will determine the best mechanism to get you the answers you ask in a Classified manner.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I'd like to thank you for holding this hearing on the Cyber Safety Review Board investigation of an intrusion into Federal networks involving Microsoft.

At the outset, I want to be clear: This is not a "gotcha" hearing. It's not the committee's goal to shame, embarrass, or discredit the witness, Microsoft, or any other entity mentioned in this CSRB report.

We have three objectives today: Accountability, securing Federal networks, and securing the broader internet ecosystem.

Last year, we were disturbed to learn that a state-sponsored threat actor from China had access to email accounts of high-ranking officials at the Departments of State and Commerce and an email account of a Member of Congress, among others.

As the investigation unfolded, we learned that the threat actor accessed these accounts by forging tokens using a stolen key from 2016 and that the State Department, not Microsoft, had discovered the intrusion.

By August, Secretary Mayorkas announced that the CSRB would review the Microsoft Exchange on-line intrusion and the malicious targeting of cloud environments. The CSRB engaged in a thorough and expeditious review, and its report was released earlier this year. I might add, the Chair just included a copy of that report in the record.

The CSRB did exactly the kind of review it was supposed to do, and it did so in a manner only the Government can. The CSRB examined a serious incident and made pointed findings and recommendations that will ultimately improve how Microsoft, other cloud service providers, and the Government approach security.

It is incumbent on this committee to hold Microsoft, one of the Federal Government's most prominent IT vendors and security partners, accountable for the findings and recommendations in the report. Microsoft deserves credit for cooperating with the board's investigation, but make no mistake: It's Congress's expectation that Microsoft or any similarly-situated company would do just the same.

Microsoft is one of the largest technology suppliers in the world, and its products are used by governments and private-sector entities alike. The company provides an estimated 85 percent of the productivity software used by the Federal Government. Microsoft also sells security tools and is one of the Government's top cloud service providers. Moreover, a reported 25 to 30 percent of its Government revenue comes from noncompetitive contracts, at least in part due to the terms of its licensing agreements.

Any company with such a significant footprint in our Federal network has an obligation to cooperate with a Government review

of how a Chinese threat actor accessed sensitive information by exploiting vulnerabilities in one of their products.

Turning to the report's findings, the CSRB determined that last summer's intrusion was, "preventable and never should have occurred". Additionally, it found that, "Microsoft's security culture was inadequate and requires an overhaul".

As someone responsible for overseeing the security of Federal networks that rely heavily on Microsoft and as a user of Microsoft products myself, I find these observations deeply troubling.

The CSRB report exhaustively described how last summer's incident occurred and includes a thorough history of the threat actor's previous activities. Importantly, the report observed that the security community has been tracking the threat actor for over 20 years.

Over that time, the threat actor has demonstrated tactics and objectives like those we saw in last summer's attack. Dating back to Operation Aurora in 2009 and the RSA compromise in 2011, the threat actor has a well-documented interest compromising cloud identity systems, stealing signing keys, and forging tokens that would enable access to targeted customer accounts.

For over a decade, every technology provider in the world has been on notice and should have stepped up their approach to securing identity and authentication accordingly, but the CSRB found Microsoft did not do so.

While Microsoft did cooperate with the CSRB investigation, the board found the company was slow to fully transparent—to be fully transparent with the public, most notably about how the threat actor obtained the signing key. To this day, we still do not know how the threat actor accessed the signing key.

Microsoft's explanations about why the key was still active in 2023 and why it worked for both consumer and enterprise accounts have not been comforting. I remain troubled that Microsoft was reluctant to be transparent with the public that it was not confident about the root cause of the incident.

My concerns about whether we can rely on Microsoft to be transparent were heightened this morning when I read a *ProPublica* article about how an employee alerted Microsoft's leadership to a vulnerability in its Active Directory Federation Service before security researchers publicly reported it in 2017. That vulnerability, which Microsoft chose not to fix, was ultimately used by Russian hackers to carry out secondary phases of the SolarWinds attack in 2020.

Even more troubling, the article recounts Microsoft's testimony before the Senate in 2021 which denied that any Microsoft vulnerability was exploited in SolarWinds. Transparency is a foundation of trust, and Microsoft needs to be more transparent.

In 2002, Bill Gates said, "When we face a choice between adding features and resolving security issues, we need to choose security". The CSRB found that Microsoft had, "drifted away from this ethos". I agree.

Last November, Microsoft announced the Secure Future Initiative, touting a reinvigorated approach to security. But, in January, Microsoft itself was compromised by Russian threat actors who used unsophisticated tactics to access the emails of high-level employees. Unfortunately, those emails included correspondence with

Government officials and put the security of Federal networks at risk once again. Basic cybersecurity tools that were not enabled would have thwarted this intrusion.

In May, following the CSRB report, Microsoft announced an expansion of the Secure Future Initiative that committed to making security a top priority. But, the same month, Microsoft announced Recall, a new feature that takes and stores periodic snapshots of a user's computer screen, which has raised concerns among both privacy and security experts.

I understand that, last Friday, Microsoft modified the roll-out of Recall in order to incorporate significant changes. I hope it will continue to consider these concerns of security and privacy as it rolls out new products.

On a final note, I've been warned that the committee's oversight of this incident will chill private-sector cooperation with the board in the future. That cannot and should not be the case.

I want to put future subjects of CSRB investigations on notice: This committee will not tolerate refusals to cooperate with legitimate investigations undertaken by the board, particularly when Federal networks are involved. Any effort to obstruct CSRB investigations into cyber incidents would invite significant scrutiny by this committee and would certainly force expedited consideration of proposals to grant CSRB greater investigatory powers.

Microsoft is one the Federal Government's most important technology and security partners, but we cannot afford to allow the importance of that relationship to enable complacency or interfere with our oversight. National security demands that technology providers continue the evolution toward transparency so we can better secure the digital ecosystem.

With that, I look forward, Mr. Chairman, to a productive conversation today about how Microsoft will improve its security culture and thereby the security of its customers, and I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JUNE 13, 2024

I would like to thank the Chairman for holding today's hearing on the Cyber Safety Review Board's (CSRB) investigation of an intrusion into Federal networks involving Microsoft. At the outset, I want to make clear: this is not a "gotcha" hearing. It is not the committee's goal to shame, embarrass, or discredit the witness, Microsoft, or any other entity mentioned in the CSRB report.

We have three objectives today: Accountability, securing Federal networks, and securing the broader internet ecosystem.

Last year, we were disturbed to learn that a state-sponsored threat actor from China had accessed the e-mail accounts of high-ranking officials at the Departments of State and Commerce and an e-mail account of a Member of Congress, among others.

As the investigation unfolded, we learned that the threat actor accessed these accounts by forging tokens using a stolen signing key from 2016 and that the State Department—not Microsoft—had discovered the intrusion. By August, Secretary Mayorkas announced that the CSRB would review the Microsoft Exchange Online intrusion and the malicious targeting of cloud environments.

The CSRB engaged in a thorough and expeditious review, and its report was released earlier this year. The CSRB did exactly the kind of review it was supposed to do, and it did so in a manner only the Government can. The CSRB examined a serious incident and made pointed findings and recommendations that will ultimately improve how Microsoft, other cloud service providers, and the Government approach security.

It is incumbent on this committee to hold Microsoft—one of the Federal Government's most prominent IT vendors and security partners—accountable for the findings and recommendations in the report.

Microsoft deserves credit for cooperating with the board's investigation. But make no mistake: It is Congress's expectation that Microsoft—or any similarly-situated company—would do so. Microsoft's is one of the largest technology suppliers in the world, and its products are used by governments and private-sector entities alike. The company provides an estimated 85 percent of the productivity software used by the Federal Government. Microsoft also sells security tools and is one of the Government's top cloud service providers. Moreover, a reported 25 to 30 percent of its Government revenue comes from non-competitive contracts, at least in part due to the terms of its licensing agreements.

Any company with such a significant footprint in our Federal networks has an obligation to cooperate with a Government review of how a Chinese threat actor accessed sensitive information by exploiting vulnerabilities in one of their products.

Turning to the report's findings: The CSRB determined that last summer's intrusion was "preventable and never should have occurred." Additionally, it found that "Microsoft's security culture was inadequate and requires an overhaul." As someone responsible for overseeing the security of Federal networks that rely heavily on Microsoft, and as a user of Microsoft products myself, I find these observations deeply troubling. The CSRB report exhaustively describes how last summer's incident occurred and includes a thorough history of the threat actor's previous activities.

Importantly, the report observed that the security community has been tracking the threat actor for over 20 years. Over that time, the threat actor has demonstrated tactics and objectives like those we saw in last summer's attack. Dating back to Operation Aurora in 2009 and the R.S.A. compromise in 2011, the threat actor has a well-documented interest compromising cloud identity systems, stealing signing keys, and forging tokens that would enable access to targeted customer accounts. For over a decade, every technology provider in the world has been on notice and should have stepped-up their approach to securing identity and authentication accordingly.

But the CSRB found Microsoft did not do so. And while Microsoft did cooperate with the CSRB investigation, the board found the company was slow to be fully transparent with the public, most notably about how the threat actor obtained the signing key. To this day, we still do not know how the threat actor accessed the signing key. Microsoft's explanations about why the key was still active in 2023 and why it worked for both consumer and enterprise accounts have not been comforting. And I remain troubled that Microsoft was reluctant to be transparent with the public that it was not confident about the root cause of the incident.

My concerns about whether we can rely on Microsoft to be transparent were heightened this morning when I read a *ProPublica* article about how an employee alerted Microsoft leadership to a vulnerability in its Active Directory Federation Services before security researchers publicly reported it in 2017. That vulnerability—which Microsoft chose not to fix—was ultimately used by Russian hackers to carry out secondary phases of the SolarWinds attack in 2020.

Even more troubling, the article recounts Microsoft's testimony before the Senate in 2021, which denied that any Microsoft vulnerability was exploited in SolarWinds. Transparency is the foundation of trust, and Microsoft needs to be more transparent.

In 2002, Bill Gates said "When we face a choice between adding features and resolving security issues, we need to choose security." The CSRB found that Microsoft had "drifted away from this ethos." I agree.

Last November, Microsoft announced the Secure Future Initiative, touting a reinvigored approach to security. But in January, Microsoft itself was compromised by Russian threat actors who used unsophisticated tactics to access the emails of high-level employees. Unfortunately, those emails included correspondence with Government officials and put the security of Federal networks at risk once again. Basic cybersecurity tools—that were not enabled—would have thwarted the intrusion.

In May, following the CSRB report, Microsoft announced an expansion of the Secure Future Initiative that committed to making security the top priority. But the same month, Microsoft announced "Recall"—a new feature that takes and stores periodic snapshots of a user's computer screen, which has raised concerns among both privacy and security experts. I understand that last Friday, Microsoft modified the rollout of Recall in order to incorporate significant changes. I hope it will continue take the concerns of the security and privacy community seriously as it does so.

On a final note, I have been warned that the committee's oversight of this incident will chill private-sector cooperation with the board in the future. That cannot—

and should not—be the case. I want to put future subjects of CSRB investigations on notice: this committee will not tolerate refusal to cooperate with legitimate investigations undertaken by the board—particularly when Federal networks are involved.

Any efforts to obstruct CSRB investigations into cyber incidents would invite significant scrutiny from this committee and would certainly force expedited consideration of proposals to grant the CSRB greater investigatory powers.

Microsoft is one of the Federal Government's most important technology and security partners. But we cannot afford to allow the importance of that relationship to enable complacency or interfere with our oversight. National security demands that technology providers continue the evolution toward transparency so we can better secure the digital ecosystem. With that, I look forward to a productive conversation today about how Microsoft will work to improve its security culture, and thereby the security of its customers.

Chairman GREEN. I thank the Ranking Member for his opening remarks.

Other Members of the committee are reminded that opening statements may be submitted to the record.

I am pleased to have a distinguished witness here before us today.

I ask that our witness please rise and raise his right hand.

[Witness sworn.]

Chairman GREEN. Let the record reflect that the witness has answered in the affirmative.

I would now like to formally introduce our witness.

Mr. Brad Smith currently serves as the vice chair and president of Microsoft Corporation, where he plays a pivotal role in steering the company's strategic direction and legal affairs.

He joined Microsoft in 1993, initially leading the legal and corporate affairs team in Paris, and later held various senior roles in the legal and corporate affairs department.

Under his leadership, Microsoft has tackled significant legal challenges and been at the forefront of critical policy debates, including cybersecurity, privacy, and artificial intelligence, among other issues. He has testified numerous times before the U.S. Congress and other governments on these key policy issues.

Before joining Microsoft, Mr. Smith worked as an associate and then partner at Covington & Burling, a prestigious law firm here in Washington. He holds a bachelor's degree from Princeton University and a law degree from Columbia University.

I thank the witness for being here.

I now recognize Mr. Smith for 5 minutes to summarize his opening statement.

STATEMENT OF BRAD SMITH, VICE CHAIR AND PRESIDENT, MICROSOFT CORPORATION

Mr. SMITH. Well, thank you, Mr. Chairman, and thank you, Ranking Minority Member Thompson. Thank you to all of you for the opportunity to be here today.

I think you, between the two of you, captured so well so much of what is so important for us to talk about this afternoon.

A lot of times in life, the most important words to heed are words that are difficult to hear. So, as you can imagine, as I listened to the two of you just now, it wasn't how I hoped I might spend an afternoon in June when the year began.

But we're here for an important reason. It starts with the role this committee plays: the protection of the homeland security of the United States. The reality is, you cannot protect the homeland security of this country without protecting the cybersecurity of it as well. That is a shared responsibility between the public and private sectors. Hence, what you do to oversee us and others in the private sector is critical.

I think the most important thing for me to say, the most important thing for me to write in my written testimony, is that we accept responsibility for each and every finding in the CSRB report.

As you can imagine, you get a report, you look at it, it's difficult to read; you sort-of think, how are you going to react? When I sat down with Satya Nadella, Microsoft's chairman and CEO, we both resolved immediately that we would react without any defensiveness, without equivocation, without hesitation, and we would instead use this report to make Microsoft and the cybersecurity protection of this country better. That's our goal.

Part of that, frankly, involves accepting responsibility, apologizing to those that were impacted, as I have done in person. It involves reminding our employees of something that I often say to them: No one ever died of humility. Use the mistakes you make so you can learn from them and get better.

Of course, that only works if you actually use what you learn and you do get better. I appreciate that's where both of you are pushing, quite rightly. That involves two things: It involves strategy, and it involves culture.

So, from a strategic perspective, we did start last November to apply the lessons we were learning already from Storm–0558. That's why we launched the Secure Future Initiative.

But I think, here, what's most important is the CSRB's recommendations. There are 25 of them. Sixteen are really applicable to us—4 only to us, 12 to all cloud services and other technology providers. So we have mapped all 16 of those recommendations onto our plan for our Secure Future Initiative so that we will do each and every one of them, and we're making progress.

But we're not stopping there. There's 18 other concrete recommendations that we have incorporated as part of this plan. We have measurable milestones. In fact, we now have the equivalent, full-time, of 34,000 engineers working on this project. This is the largest engineering project focused on cybersecurity in the history of digital technology.

But I think you asked a second question as well: Is that enough? I think, if we did that alone, it would not be. That's what you're saying, and those are words I heed as well. That is why we're focused on changing, strengthening, and building a world-class security culture. I look forward to talking about that.

It starts with the tone at the top. It needs to reach all of our employees. Just yesterday, our board of directors approved two new steps. One will change the compensation of our most senior people so that annual bonuses are tied in part to cybersecurity with an exclusive focus on it. But, second, I think, even more that that, that this will become part of the biannual review for every employee at Microsoft, what they're doing on cybersecurity.

Then I would conclude by saying that I think the two of you captured so well everything else we need to think about here. Because if we improve Microsoft alone, that won't be enough. We're dealing with four formidable foes in China, Russia, North Korea, Iran. They're getting better; they're getting more aggressive. We should all expect them to work together. They're waging attacks at an extraordinary rate.

So I welcome the opportunity to ask ourselves to learn together, what can we do in that space as well? You frame some excellent ideas in your two openings. I look forward to talking about them.

Thank you.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF BRAD SMITH

JUNE 11, 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 data centers 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 United States and numerous allied governments.

This role brings with it tremendous responsibility. Expanding and intensifying geopolitical conflicts have created a more dangerous cyber world. It's no accident that the first shots fired in the war against Ukraine were malicious cyber attacks 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 cyber attacks by 4 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 cyber attacks 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 2 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 multi-year 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 6 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 cyber space.

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 2 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

[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.

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 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 1980's 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 3 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 1 of the 6 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 long-standing 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.

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 300 nation-state actors. We report what we see through frequent cybersecurity technical blogs, podcasts, and other

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

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

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, cyber attacks 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 cyber space. The 2 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 cyber space. 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 6 months, we have seen them pour 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 cyber crime, 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 cyber crime, 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 health care sector, including in the United States. The FBI estimated in its 2023 Internet Crime Report that health care has become the sector most frequently targeted by ransomware. The number of such attacks last year against U.S. health care providers increased by 128 percent, claiming 389 health care organizations as victims.[7]

The impacts of these attacks are real and frightening. For example, last Thanksgiving, a cyber attack on Ardent Health Services, a Tennessee-based company owning more than 2 dozen hospitals across at least 5 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

---

[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.

[7] Ransomware__Attacks__Surge__in__2023.pdf (dni.gov).

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 cyber attacks 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, United Health Group was targeted by the Russian-speaking BlackCat (ALPHV) ransomware group. The attack shut down the largest health care 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 United Health 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 cyber space. 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 cyber space as well.

This is grave at multiple levels. It's one thing to engage in cyber combat with 4 separate nation-state adversaries, but quite another scenario if 2 or all 4 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.

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 9 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 cyber war waged by 4 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, benefiting from at least 2 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 2 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 cyber space. 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 2 years and the 2 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 2 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.

ADDENDUM TO WRITTEN TESTIMONY

To: Members, Homeland Security Committee
Re: Full Committee Hearing at 1:15pm on Thursday, June 13, 2024

MICROSOFT BOARD OF DIRECTORS COMPENSATION ANNOUNCEMENT/DETAILS

As I stated in the written testimony I submitted yesterday, Microsoft's board of directors was scheduled to meet today. I'm submitting this addendum to provide you with an update on the changes the board discussed and approved today relating to security accountability and compensation for the company's next fiscal year, which begins on July 1. These changes were made to ensure that all Microsoft employees, and particularly our senior leaders, are held even more accountable for the company's security commitments as part of our review and compensation processes.

At today's meeting, the board approved a recommendation from the compensation committee to change the criteria that will be used for the award of annual individual bonuses for the top Microsoft executives on our Senior Leadership Team (SLT). Beginning with the start of the company's new fiscal year on July 1, one-third of the individual performance element for each SLT member's bonus will be based exclusively on the committee's assessment of the executive's individual performance relating to cybersecurity.

This assessment will be based on quantitative metrics and qualitative assessments relating to the implementation of the CSRB's recommendations, additional objectives in the company's Secure Future Initiative, and other aspects of the executive's cybersecurity work and performance. Microsoft CEO Satya Nadella and the board committee will receive input directly from a third party that will provide an additional and independent assessment of the company's progress in these areas.

The board also decided that for the current fiscal year, which ends on June 30, the compensation committee will consider explicitly each SLT member's cybersecurity performance when it makes its annual assessment of the executive's performance. Beyond the design changes to our executive pay program to include a greater accountability for cybersecurity, the board also has the ability to exercise downward discretion on compensation outcomes as it deems appropriate.

In addition, the company will make security a mandatory part of the bi-annual reviews for all Microsoft employees. These involve what the company internally refers to as "Connect" meetings and reviews that all employees have with their manager. Beginning with the new fiscal year, these assessments will include a new "core

priority" relating to cybersecurity, so that all employees will identify and discuss the work they do relating to cybersecurity with their manager. With this change, cybersecurity will be considered in every employee's annual bonus and compensation.

These changes are being made in addition to the company's updating of the ongoing mandatory security training that is in place for all Microsoft employees to reflect recent lessons learned and the steps being taken as part of the Secure Future Initiative.

I will be happy to answer any questions about any of this when the hearing takes place tomorrow.

BRAD SMITH

Chairman GREEN. Thank you, Mr. Smith.

Members will be recognized in order of seniority for their 5 minutes of questioning. I want to remind everyone to please keep their questioning to 5 minutes. An additional round of questioning may be called after all Members have been recognized.

I now recognize myself for 5 minutes of questioning.

I was intrigued from your statement and your written statement about the—you know, let me start by saying this. We, as human beings, respond to initiatives—or incentives—I'm sorry—incentives. Economics is about the study of incentives.

You mentioned the recent payroll changes for your senior executives. I wonder if you're at liberty to discuss how deep that goes, you know, what level of leadership. I think that's a novel approach, and I'd love to hear more about that.

Mr. SMITH. Sure. Let me say two things.

First, the board of directors took the first step yesterday, and it acted a bit ahead of schedule. We ordinarily make these decisions in July, August. But for the 16 most senior people in the company, including our CEO, including me and others, with the new fiscal year, which starts July 1, one-third of the individual performance element of our bonus will be about one thing and one thing only: cybersecurity. So that's the first thing.

Second, the board did note that, when it awards bonuses for the fiscal year that ends at the end of this month, it will take cybersecurity performance of the individual executive into account.

But the thing we probably spent the most time as a senior leadership team talking about the last month or so is how to create incentives for everybody. Of course, it's based on the culture of the company and our processes.

So, twice a year, every employee has a forum and a conversation with their manager; we call it a "connect forum." They first reflect and show what they've done, and then the manager comments, and they talk about it. So what we have created is a new piece of this that everyone will have to address on cybersecurity.

The thing I like about it most, to be honest, is it gives every employee at Microsoft the opportunity to think, what have I done, what could I do, how am I doing, and then be rewarded at the end of the year based on that.

Chairman GREEN. That sounds—that's encouraging. Having run a company myself, I think how you tie the incentives drives performance and what people make the priority. So I appreciate that.

Let me ask a little bit about your involvement in China. I'd love to get a little bit more detail of granularity on where you are right now, you know, what's your current posture and, you know, what are you sharing with the Chinese people—or to the Chinese Gov-

ernment, I mean—are you having to give up code, and what the involvement there is.

If you don't mind elaborating on that a little bit.

Mr. SMITH. Sure. It's a broad topic.

We have a few different activities in China. It's not a major source of revenue for Microsoft globally. It accounts for about 1.4 or 1.5 percent of our revenue.

We do have an engineering team that we have been reducing. We announced most recently that we were offering about 800 people, 700 or 800 people, the opportunity to move out of China, and they were going to need to move out of China in order to keep the job they have. So we've been reducing our engineering presence.

There are two things that we do that we believe are very important.

First, we do run some data centers, cloud services, principally, I would say, for the benefit of multinational companies who do business in China. We're not alone. Others in our industry do the same thing.

But the reason I think this is so important is, if you're an American automobile company, an aircraft company, a pharmaceutical company, a coffee company, you need to use the cloud when you're in China. We want their American trade secrets to be stored in an American data center in China——

Chairman GREEN. Let me, if I could, jump in. What access does the Chinese government have to that?

Mr. SMITH. None.

Chairman GREEN. OK.

Mr. SMITH. Believe me, every time there is anything remotely close to a request, I always ensure we say no.

Chairman GREEN. OK.

Very specifically on this hack—because it did come from China—can you talk how you are, with your presence in China, ensuring that that source isn't going to use your location in China as a vector? I mean, what other—if you can, what are you doing there to prevent that?

Mr. SMITH. I think it involves having a very direct understanding yourself of what your guardrails are, what your limits are, what you can do, and what you won't do. You have to know your own mind. We do.

Second, you've got to be prepared to look people in the eye and say "no" to them.

That's something I do myself. I was in Beijing in December. I got pushed because there was unhappiness about reports that we've made publicly about attacks from China, about U.S. critical infrastructure, and about, you know, influence operations. I said, there are lines that we don't believe government should cross. We're going to be principled, and we're going to be public.

Chairman GREEN. Huh.

Mr. SMITH. There are many things we're not going to do in China, and there will be things we're not allowed to do in China, but I think, at the end of the day, we have to know our principles.

Chairman GREEN. Thank you.

My time has expired, and I now recognize the Ranking Member for his 5 minutes of questioning.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

I'd like to enter into the record a *ProPublica* article entitled, "Microsoft Chose Profit Over Security and Left U.S. Government Vulnerable to Russian Hack, Whistleblower Says."

Chairman GREEN. So ordered.

[The information referred to follows:]

ARTICLE SUBMITTED BY RANKING MEMBER BENNIE G. THOMPSON

Technology

Microsoft Chose Profit Over Security and Left U.S. Government Vulnerable to Russian Hack, Whistleblower Says

by Renee Dudley, with research by Doris Burke
June 13, 5 a.m. EDT

Former employee says software giant dismissed his warnings about a critical flaw because it feared losing government business. Russian hackers later used the weakness to breach the National Nuclear Security Administration, among others.

A model of the Microsoft campus at the company's headquarters in Redmond, Washington Greg Kahn, special to ProPublica

Microsoft hired Andrew Harris for his extraordinary skill in keeping hackers out of the nation's most sensitive computer networks. In 2016, Harris was hard at work on a mystifying incident in which intruders had somehow penetrated a major U.S. tech company.

The breach troubled Harris for two reasons. First, it involved the company's cloud — a virtual storehouse typically containing an organization's most sensitive data. Second, the attackers had pulled it off in a way that left little trace.

He retreated to his home office to "war game" possible scenarios, stress-testing the various software products that could have been compromised.

Early on, he focused on a Microsoft application that ensured users had permission to log on to cloud-based programs, the cyber equivalent of an officer checking passports at a border. It was there, after months of research, that he found something seriously wrong.

The product, which was used by millions of people to log on to their work computers, contained a flaw that could allow attackers to masquerade as legitimate employees and rummage through victims' "crown jewels" — national security secrets, corporate intellectual property, embarrassing personal emails — all without tripping alarms.

To Harris, who had previously spent nearly seven years working for the Defense Department, it was a security nightmare. Anyone using the software was exposed, regardless of whether they used Microsoft or another cloud provider such as Amazon. But Harris was most concerned about the federal government and the implications of his discovery for national security. He flagged the issue to his colleagues.

They saw it differently, Harris said. The federal government was preparing to make a massive investment in cloud computing, and Microsoft wanted the business. Acknowledging this security flaw could jeopardize the company's chances, Harris recalled one product leader telling him. The financial consequences were enormous. Not only could Microsoft lose a multibillion-dollar deal, but it could also lose the race to dominate the market for cloud computing.

Harris said he pleaded with the company for several years to address the flaw in the product, a ProPublica investigation has found. But at every turn, Microsoft dismissed his warnings, telling him they would work on a long-term alternative — leaving cloud services around the globe vulnerable to attack in the meantime.

Harris was certain someone would figure out how to exploit the weakness. He'd come up with a temporary solution, but it required customers to turn off one of Microsoft's most convenient and popular features: the ability to access nearly every program used at work with a single logon.

He scrambled to alert some of the company's most sensitive customers about the threat and personally oversaw the fix for the New York Police Department. Frustrated by Microsoft's inaction, he left the company in August 2020.

Andrew Harris shared his Microsoft employee badge on his LinkedIn page when he announced his departure from the company in 2020. Screenshot by ProPublica

Within months, his fears became reality. U.S. officials confirmed reports that a state-sponsored team of Russian hackers had carried out SolarWinds, one of the largest cyberattacks in U.S. history. They used the flaw Harris had identified to vacuum up sensitive data from a number of federal agencies, including, ProPublica has learned, the National Nuclear Security Administration, which maintains the United States' nuclear weapons stockpile, and the National Institutes of Health, which at the time was engaged in COVID-19 research and vaccine distribution. The Russians also used the weakness to compromise dozens of email accounts in the Treasury Department, including those of its highest-ranking officials. One federal official described the breach as "an espionage campaign designed for long-term intelligence collection."

Harris' account, told here for the first time and supported by interviews with former colleagues and associates as well as social media posts, upends the prevailing public understanding of the SolarWinds hack.

From the moment the hack surfaced, Microsoft insisted it was blameless. Microsoft President Brad Smith assured Congress in 2021 that "there was no vulnerability in any Microsoft product or service that was exploited" in SolarWinds.

He also said customers could have done more to protect themselves.

Harris said they were never given the chance.

"The decisions are not based on what's best for Microsoft's customers but on what's best for Microsoft," said Harris, who now works for CrowdStrike, a cybersecurity company that competes with Microsoft.

Microsoft declined to make Smith and other top officials available for interviews for this story, but it did not dispute ProPublica's findings. Instead, the company issued a statement in response to written questions. "Protecting customers is always our highest priority," a spokesperson said. "Our security response team takes all security issues seriously and gives every case due diligence with a thorough manual assessment, as well as cross-confirming with engineering and security partners. Our assessment of this issue received multiple reviews and was aligned with the industry consensus."

Get in Touch

We're still reporting on the cybersecurity industry and cyberspace regulation. If you have specific information to share about these topics, you can contact Renee Dudley by email at renee.dudley@propublica.org or on Signal at 929-317-0748.

ProPublica's investigation comes as the Pentagon seeks to expand its use of Microsoft products — a move that has drawn scrutiny from federal lawmakers amid a series of cyberattacks on the government.

Smith is set to testify on Thursday before the House Homeland Security Committee, which is examining Microsoft's role in a breach perpetrated last year by hackers connected to the Chinese government. Attackers exploited Microsoft security flaws to gain access to top U.S. officials' emails. In investigating the attack, the federal Cyber Safety Review Board found that Microsoft's "security culture was inadequate and requires an overhaul."

Microsoft President Brad Smith testifies during a Senate Select Committee on Intelligence hearing about SolarWinds on Feb. 23, 2021. Drew Angerer/Getty Images

For its part, Microsoft has said that work has already begun, declaring that the company's top priority is security "above all else." Part of the effort involves adopting the board's recommendations. "If you're faced with the tradeoff between security and another priority, your answer is clear: Do security," the company's CEO, Satya Nadella, told employees in the wake of the board's report, which identified a "corporate culture that deprioritized both enterprise security investments and rigorous risk management."

ProPublica's investigation adds new details and pivotal context about that culture, offering an unsettling look into how the world's largest software provider handles the security of its own ubiquitous products. It also offers crucial insight into just how much the quest for profits can drive those security decisions, especially as tech behemoths push to dominate the newest — and most lucrative — frontiers, including the cloud market.

"This is part of the problem overall with the industry," said Nick DiCola, who was one of Harris' bosses at Microsoft and now works at Zero Networks, a network security firm. Publicly-traded tech giants "are beholden to the share price, not to doing what's right for the customer all the time. That's just a reality of capitalism. You're never going to change that in a public company because at the end of the day, they want the shareholder value to go up."

A "Cloud-First World"

Early this year, Microsoft surpassed Apple to become the world's most valuable company, worth more than $3 trillion. That triumph was almost unimaginable a decade ago. (The two remain in close competition for the top spot.)

In 2014, the same year that Harris joined Microsoft and Nadella became the CEO, Wall Street and consumers alike viewed the company as stuck in the past, clinging to the "shrink-wrapped" software products like Windows that put it on the map in the 1990s. Microsoft's long-stagnant share price reflected its status as an also-ran in almost every major technological breakthrough since the turn of the century, from its Bing search engine to its Nokia mobile phone division.

As the new CEO, Nadella was determined to reverse the trend and shake off the company's fuddy-duddy reputation, so he staked Microsoft's future on the Azure cloud computing division, which then lagged far behind Amazon. In his earliest all-staff memo, Nadella told employees they would need "to reimagine a lot of what we have done in the past for a ... cloud-first world."

Microsoft CEO Satya Nadella promotes the company's cloud offerings at an event in San Francisco in 2014. David Paul Morris/Bloomberg via Getty Images

Microsoft salespeople pitched business and government customers on a "hybrid cloud" strategy, where they kept some traditional, on-premises servers (typically stored on racks in customers' own offices) while shifting most of their computing needs to the cloud (hosted on servers in Microsoft data centers).

Security was a key selling point for the cloud. On-site servers were notoriously vulnerable, in part because organizations' overburdened IT staff often failed to promptly install the required patches and updates. With the cloud, that crucial work was handled by dedicated employees whose job was security.

The dawn of the cloud era at Microsoft was an exciting time to work in the field of cybersecurity for someone like Harris, whose high school yearbook features a photo of him in front of a desktop computer and monitor with a mess of floppy disks beside him. One hand is on the keyboard, the other on a wired mouse. Caption: "Harris the hacker."

Harris' high school yearbook Classmates.com

As a sophomore at Pace University in New York, he wrote a white paper titled "How to Hack the Wired Equivalent Protocol," a network security standard, and was awarded a prestigious Defense Department scholarship, which the government uses to recruit cybersecurity specialists. The National Security Agency paid for three years of his tuition, which included a master's degree in software engineering, in exchange for a commitment to work for the government for at least that long, he said.

Early in his career, he helped lead the Defense Department's efforts to protect individual devices. He became an expert in the niche field known as identity and access management, securing how people log in.

As the years wore on, he grew frustrated by the lumbering bureaucracy and craved the innovation of the tech industry. He decided he could make a bigger impact in the private sector, which designed much of the software the government used.

At Microsoft he was assigned to a secretive unit known as the "Ghostbusters" (as in: "Who you gonna call?"), which responded to hacks of the company's most sensitive customers, especially the federal government. As a member of this team, Harris first investigated the puzzling attack on the tech company and remained obsessed with it, even after switching roles inside Microsoft.

Eventually, he confirmed the weakness within Active Directory Federation Services, or AD FS, a product that allowed users to sign on a single time to access nearly everything they needed. The problem, he discovered, rested in how the application used a computer language known as SAML to authenticate users as they logged in.

This is what makes a SAML attack unique. Typically, hackers leave what cybersecurity specialists call a "noisy" digital trail. Network administrators monitoring the so-called "audit logs" might see unknown or foreign IP addresses attempting to gain access to their cloud services. But SAML attacks are much harder to detect. The forged token is the equivalent of a robber using a copied master key. There was little trail to track, just the activities of what appear to be legitimate users.

Harris and a colleague who consulted for the Department of Defense spent hours in front of both real and virtual whiteboards as they mapped out how such an attack would work, the colleague told ProPublica. The "token theft" risk, as Harris referred to it, became a regular topic of discussion for them.

A Clash With "Won't Fix" Culture

Before long, Harris alerted his supervisors about his SAML finding. Nick DiCola, his boss at the time, told ProPublica he referred Harris to the Microsoft Security Response Center, which fields reports of security vulnerabilities and determines which need to be addressed. Given its central role in improving Microsoft product security, the team once considered itself the "conscience of the company," urging colleagues to improve security without regard to profit. In a meeting room, someone hung a framed photo of Winston

"the Wolf," the charismatic fixer in Quentin Tarantino's movie "Pulp Fiction" who is summoned to clean up the aftermath of bloody hits.

Members of the team were not always popular within the company. Plugging security holes is a cost center, and making new products is a profit center, former employees told ProPublica. In 2002, the company's founder, Bill Gates, tried to settle the issue, sending a memo that turned out to be eerily prescient. "Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company," Gates wrote, adding: "So now, when we face a choice between adding features and resolving security issues, we need to choose security."

At first, Gates' memo was transformational and the company's product divisions were more responsive to the center's concerns. But over time, the center's influence waned.

Its members were stuck between cultural forces. Security researchers — often characterized as having outsized egos — believed their findings should be immediately addressed, underestimating the business challenges of developing fixes quickly, former MSRC employees told ProPublica.

Product managers had little motivation to act fast, if at all, since compensation was tied to the release of new, revenue-generating products and features. That attitude was particularly pronounced in Azure product groups, former MSRC members said, because they were under pressure from Nadella to catch up to Amazon.

"Azure was the Wild West, just this constant race for features and functionality," said Nate Warfield, who worked in the MSRC for four years beginning in 2016. "You will get a promotion because you released the next new shiny thing in Azure. You are not going to get a promotion because you fixed a bunch of security bugs."

Former employees told ProPublica that the center fielded hundreds or even thousands of reports a month, pushing the perennially understaffed group to its limits. The magazine Popular Science noted that volume as one of the reasons why working in the MSRC was one of the 10 "worst jobs in science," between whale feces researchers and elephant vasectomists.

"They're trained, because they're so resource constrained, to think of these cases in terms of: 'How can I get to 'won't fix,'" said Dustin Childs, who worked in the MSRC in the years leading up to Harris' saga. Staff would often punt on fixes by telling researchers they would be handled in "v-next," the next product version, he said. Those launches, however, could be years away, leaving customers vulnerable in the interim, he said.

The center also routinely rejected researchers' reports of weaknesses by saying they didn't cross what its staff called a "security boundary." But when Harris discovered the SAML flaw, it was a term with no formal definition, former employees said.

Jaap Arriens / Sipa USA via AP Images

By 2017, the lack of clarity had become the "butt of jokes," Warfield said. Several prominent security researchers who regularly interacted with the MSRC made T-shirts and stickers that said "___ [fill in the blank] is not a security boundary."

"Any time Microsoft didn't want to fix something, they'd just say, 'That's not a security boundary, we're not going to fix it,'" Warfield recalled.

Unaware of the inauspicious climate, Harris met virtually with MSRC representatives and sketched out how a hacker could jump from an on-premises server to the cloud without being detected. The MSRC declined to address the problem. Its staff argued that hackers attempting to exploit the SAML flaw would first have to gain access to an on-premises server. As they saw it, Harris said, that was the security boundary — not the subsequent hop to the cloud.

Business Over Security

"WTF," Harris recalled thinking when he got the news. "This makes no sense."

Microsoft had told customers the cloud was the safest place to put their most precious data. His discovery proved that, for the millions of users whose systems included AD FS, their cloud was only as secure as their on-premises servers. In other words, all the buildings owned by the landlord are only as secure as the most careless tenant who forgot to lock their window.

Harris pushed back, but he said the MSRC held firm.

Harris had a reputation for going outside the chain of command to air his concerns, and he took his case to the team managing the products that verified user identities.

He had some clout, his former colleagues said. He had already established himself as a known expert in the field, had pioneered a cybersecurity threat detection method and later was listed as the named inventor on a Microsoft patent. Harris said he "went kind of crazy" and fired off an email to product manager Mark Morowczynski and director Alex Simons requesting a meeting.

He understood that developing a long-term fix would take time, but he had an interim solution that could eliminate the threat. One of the main practical functions of AD FS was to allow users to access both on-premises servers and a variety of cloud-based services after entering credentials only once, a Microsoft feature known as "seamless" single sign-on. Harris proposed that Microsoft tell its customers to turn off that function so the SAML weakness would no longer matter.

According to Harris, Morowczynski quickly jumped on a videoconference and said he had discussed the concerns with Simons.

"Everyone violently agreed with me that this is a huge issue," Harris said. "Everyone violently disagreed with me that we should move quickly to fix it."

Morowczynski, Harris said, had two primary objections.

First, a public acknowledgement of the SAML flaw would alert adversaries who could then exploit it. Harris waved off the concern, believing it was a risk worth taking so that customers wouldn't be ignorant to the threat. Plus, he believed Microsoft could warn customers without betraying any specifics that could be co-opted by hackers.

According to Harris, Morowczynski's second objection revolved around the business fallout for Microsoft. Harris said Morowczynski told him that his proposed fix could alienate one of Microsoft's largest and most important customers: the federal government, which used AD FS. Disabling seamless SSO would have widespread and unique consequences for government employees, who relied on physical "smart cards" to log onto their devices. Required by federal rules, the cards generated random passwords each time employees signed on. Due to the configuration of the underlying technology, though, removing seamless

SSO would mean users could not access the cloud through their smart cards. To access services or data on the cloud, they would have to sign in a second time and would not be able to use the mandated smart cards.

Harris said Morowczynski rejected his idea, saying it wasn't a viable option.

Morowczynski told Harris that his approach could also undermine the company's chances of getting one of the largest government computing contracts in U.S. history, which would be formally announced the next year. Internally, Nadella had made clear that Microsoft needed a piece of this multibillion-dollar deal with the Pentagon if it wanted to have a future in selling cloud services, Harris and other former employees said.

Killing the Competition

By Harris' account, the team was also concerned about the potential business impact on the products sold by Microsoft to sign into the cloud. At the time, Microsoft was in a fierce rivalry with a company called Okta.

Microsoft customers had been sold on seamless SSO, which was one of the competitive advantages — or, in Microsoft parlance, "kill points" — that the company then had over Okta, whose users had to sign on twice, Harris said.

Harris' proposed fix would undermine the company's strategy to marginalize Okta and would "add friction" to the user experience, whereas the "No. 1 priority was to remove friction," Harris recalled Morowczynski telling him. Moreover, it would have cascading consequences for the cloud business because the sale of identity products often led to demand for other cloud services.

"That little speed bump of you authenticating twice was unacceptable by Microsoft's standards," Harris said. He recalled Morowczynski telling him that the product group's call "was a business decision, not a technical one."

"What they were telling me was counterintuitive to everything I'd heard at Microsoft about 'customer first,'" Harris said. "Now they're telling me it's not 'customer first,' it's actually 'business first.'"

DiCola, Harris' then-supervisor, told ProPublica the race to dominate the market for new and high-growth areas like the cloud drove the decisions of Microsoft's product teams. "That is always like, 'Do whatever it frickin' takes to win because you have to win.' Because if you don't win, it's much harder to win it back in the future. Customers tend to buy that product forever."

According to Harris, Morowczynski said his team had "on the road map" a product that could replace AD FS altogether. But it was unclear when it would be available to customers.

In the months that followed, Harris vented to his colleagues about the product group's decision. ProPublica talked to three people who worked with Harris at the time and recalled these conversations. All of them spoke on the condition of anonymity because they feared professional repercussions. The three said Harris was enraged and frustrated over what he described to them as the product group's unwillingness to address the weakness.

Neither Morowczynski nor Simons returned calls seeking comment, and Microsoft declined to make them available for interviews. The company did not dispute the details of Harris' account. In its statement, Microsoft said it weighs a number of factors when it evaluates potential threats. "We prioritize our security response work by considering potential customer disruption, exploitability, and available mitigations," the spokesperson said. "We continue to listen to the security research community and evolve our approach to ensure we are meeting customer expectations and protecting them from emerging threats."

Another Major Warning

Following the conversation with Morowczynski, Harris wrote a reminder to himself on the whiteboard in his home office: "SAML follow-up." He wanted to keep the pressure on the product team.

Soon after, the Massachusetts- and Tel Aviv-based cybersecurity firm CyberArk published a blog post describing the flaw, which it dubbed "Golden SAML," along with a proof of concept, essentially a road map that showed how hackers could exploit the weakness.

Years later, in his written testimony for the Senate Intelligence Committee, Microsoft's Brad Smith said this was the moment the company learned of the issue. "The Golden SAML theory became known to cybersecurity professionals at Microsoft and across the U.S. government and the tech sector at precisely the same time, when it was published in a public paper in 2017," Smith wrote.

Lavi Lazarovitz of CyberArk said the firm mentioned the weakness — before the post was published — in a private WhatsApp chat of about 10 security researchers from various companies, a forum members used to compare notes on emerging threats. When they raised the discovery to the group, which included at least one researcher from Microsoft, the other members were dismissive, Lazarovitz said.

"Many in the security research community — I don't want to say mocked — but asked, 'Well, what's the big deal?'" Lazarovitz said.

The CyberArk headquarters in Newton, Massachusetts Sipa via AP Images

Nevertheless, CyberArk believed it was worth taking seriously, given that AD FS represented the gateway to users' most sensitive information, including email. "Threat actors operate in between the cracks," Lazarovitz said. "So obviously, we understood the feedback that we got, but we still believed that this technique will be eventually leveled by threat actors."

The Israel-based team also reached out to contacts at Microsoft's Israeli headquarters and were met with a response similar to the one they got in the WhatsApp group, Lazarovitz said.

The published report was CyberArk's way of warning the public about the threat. Disclosing the weakness also had a business benefit for the company. In the blog post, it pitched its own security product, which it said "will be extremely beneficial in blocking attackers from getting their hands on important assets like the token-signing certificate in the first place."

The report initially received little attention. Harris, however, seized on it. He said he alerted Morowczynski and Simons from the product group as well as the MSRC. The situation was more urgent than before, Harris argued to them, because CyberArk included the proof of concept that could be used by hackers to carry out a real attack. For Harris, it harkened back to Morowczynski's worry that flagging the weakness could give hackers an advantage.

"I was more energetic than ever to have us actually finally figure out what we're going to do about this," Harris said.

But the MSRC reiterated its "security boundary" stance, while Morowczynski reaffirmed the product group's earlier decision, Harris said.

Harris said he then returned to his supervisors, including Hayden Hainsworth and Bharat Shah, who, as corporate vice president of the Azure cloud security division, also oversaw the MSRC. "I said, 'Can you guys please listen to me,'" Harris recalled. ""This is probably the most important thing I've ever done in my career.'"

Harris said they were unmoved and told him to take the problem back to the MSRC.

Microsoft did not publicly comment on the CyberArk blog post at the time. Years later, in written responses to Congress, Smith said the company's security researchers reviewed the information but decided to focus on other priorities. Neither Hainsworth nor Shah returned calls seeking comment.

Defusing a Ticking Bomb

Harris said he was deeply frustrated. On a personal level, his ego was bruised. Identifying major weaknesses is considered an achievement for cybersecurity professionals, and, despite his internal discovery, CyberArk had claimed Golden SAML.

More broadly, he said he was more worried than ever, believing the weakness was a ticking bomb. "It's out in the open now," he said.

Publicly, Microsoft continued to promote the safety of its products, even boasting of its relationship with the federal government in sales pitches. "To protect your organization, Azure embeds security, privacy, and compliance into its development methodology," the company said in late 2017, "and has been recognized as the most trusted cloud for U.S. government institutions."

Attendees walk through the exhibition floor during the Microsoft Developers Build Conference in Seattle in 2017. David Ryder/Bloomberg via Getty Images

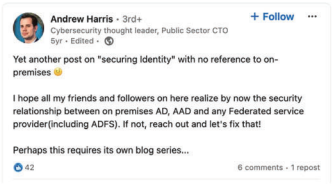
Internally, Harris complained to colleagues that customers were being left vulnerable.

"He was definitely having issues" with the product team, said Harris' former Microsoft colleague who consulted for the Defense Department. "He vented that it was a problem that they just wanted to ignore."

Harris typically pivoted from venting to discussing how to protect customers, the former colleague said. "I asked him to show me what I'm going to have to do to make sure the customers were aware and could take corrective action to mitigate the risk," he said.

Harris also took his message to LinkedIn, where he posted a discreet warning and an offer.

"I hope all my friends and followers on here realize by now the security relationship" involved in authenticating users in AD FS, he wrote in 2019. "If not, reach out and let's fix that!"



In 2019, Harris posted a discreet warning and an offer on LinkedIn.
Screenshot by ProPublica

Separately, he realized he could help customers with whom he had existing relationships, including the NYPD, the nation's largest police force.

"Knowing this exploit is actually possible, why would I not architect around it, especially for my critical customers?" Harris said.

On a visit to the NYPD, Harris told a top IT official, Matthew Fraser, about the AD FS weakness and recommended disabling seamless SSO. Fraser was in disbelief at the severity of the issue, Harris recalled, and he agreed to disable seamless SSO.

In an interview, Fraser confirmed the meeting.

"This was identified as one of those areas that was prime, ripe," Fraser said of the SAML weakness. "From there, we figured out what's the best path to insulate and secure."

More Troubling Revelations

It was over beers at a conference in Orlando in 2018 that Harris learned the weakness was even worse than he'd initially realized. A colleague sketched out on a napkin how hackers could also bypass a common security feature called multifactor authentication, which requires users to perform one or more additional steps to verify their identity, such as entering a code sent via text message.

They realized that, no matter how many additional security steps a company puts in place, a hacker with a forged token can bypass them all. When they brought the new information to the MSRC, "it was a nonstarter," Harris said. While the center had published a formal definition of "security boundary" by that point, Harris' issues still didn't meet it.

Nadella delivers the keynote address at a 2018 conference in Seattle for software developers. Elaine Thompson/AP

By March 2019, concerns over Golden SAML were spilling out into the wider tech world. That month, at a conference in Germany, two researchers from the cybersecurity company Mandiant delivered a presentation demonstrating how hackers could infiltrate AD FS to gain access to organizations' cloud accounts and applications. They also released the tools they used to do so.

Mandiant said it notified Microsoft before the presentation, making it the second time in roughly 16 months that an outside firm had flagged the SAML issue to the company.

In August 2020, Harris left Microsoft to work for CrowdStrike. In his exit interview with Shah, Harris said he raised the SAML weakness one last time. Shah listened but offered no feedback, he said.

"There is no inspector general-type thing" within Microsoft, Harris said. "If something egregious is happening, where the hell do you go? There's no place to go."

SolarWinds Breaks

Four months later, news of the SolarWinds attack broke. Federal officials soon announced that beginning in 2019 Russian hackers had breached and exploited the network management software offered by a Texas-based company called SolarWinds, which had the misfortune of lending its name to the attack. The hackers covertly inserted malware into the firm's software updates, gaining "backdoor" access to the networks of companies and government agencies that installed them. The ongoing access allowed hackers to take advantage of "post-exploit" vulnerabilities, including Golden SAML, to steal sensitive data and emails from the cloud.

Despite the name, nearly a third of victims of the attack never used SolarWinds software at all, Brandon Wales, then acting director of the federal Cybersecurity and Infrastructure Security Agency, said in the aftermath. In March 2021, Wales told a Senate panel that hackers were able to "gain broad access to data stores that they wanted, largely in Microsoft Office 365 Cloud ... and it was all because they compromised those systems that manage trust and identity on networks."

Microsoft itself was also breached.

In the immediate aftermath of the attack, Microsoft advised customers of Microsoft 365 to disable seamless SSO in AD FS and similar products — the solution that Harris proposed three years earlier.

As the world dealt with the consequences, Harris took his long simmering frustration public in a series of posts on social media and on his personal blog. Challenging Brad Smith by name, and criticizing the MSRC's decisions — which he referred to as "utter BS" — Harris lambasted Microsoft for failing to publicly warn customers about Golden SAML.

Microsoft "was not transparent about these risks, forced customers to use ADFS knowing these risks, and put many customers and especially US Gov't in a bad place," Harris wrote on LinkedIn in December 2020. A long-term fix was "never a priority" for the company, he wrote. "Customers are boned and sadly it's been that way for years (which again, sickens me)," Harris said in the post.

In the months and years following the SolarWinds attack, Microsoft took a number of actions to mitigate the SAML risk. One of them was a way to efficiently detect fallout from such a hack. The advancement, however, was available only as part of a paid add-on product known as Sentinel.

The lack of such a detection, the company said in a blog post, had been a "blind spot."

"Microsoft Is Back on Top"

In early 2021, the Senate Select Committee on Intelligence called Brad Smith to testify about SolarWinds.

Although Microsoft's product had played a central role in the attack, Smith seemed unflappable, his easy and conversational tone a reflection of the relationships he had spent decades building on Capitol Hill. Without referencing notes or reading from a script, as some of his counterparts did, he confidently deflected questions about Microsoft's role. Laying the responsibility with the government, he said that in the lead-up to the attack, the authentication flaw "was not prioritized by the intelligence community as a risk, nor was it flagged by civilian agencies or other entities in the security community as a risk that should be elevated" over other cybersecurity priorities.

Smith also downplayed the significance of the Golden SAML weakness, saying it was used in just 15% of the 60 cases that Microsoft had identified by that point. At the same time, he acknowledged that, "without question, these are not the only victims who had data observed or taken."

When Sen. Marco Rubio of Florida pointedly asked him what Microsoft had done to address Golden SAML in the years before the attack, Smith responded by listing a handful of steps that customers could have taken to protect themselves. His suggestions included purchasing an antivirus product like Microsoft Defender and securing devices with another Microsoft product called Intune.

"The reality is any organization that did all five of those things, if it was breached, it in all likelihood suffered almost no damage," Smith said.

Neither Rubio nor any other senator pressed further.

Ultimately, Microsoft won a piece of the Defense Department's multibillion-dollar cloud business, sharing it with Amazon, Google and Oracle.

Since December 2020, when the SolarWinds attack was made public, Microsoft's stock has soared 106%, largely on the runaway success of Azure and artificial intelligence products like ChatGPT, where the company is the largest investor. "Microsoft Is Back on Top," proclaimed Fortune, which featured Nadella on the cover of its most recent issue.

In September 2021, just 10 months after the discovery of SolarWinds, the paperback edition of Smith's book, "Tools and Weapons," was published. In it, Smith praised Microsoft's response to the attack. The MSRC, Smith wrote, "quickly activated its incident response plan" and the company at large "mobilized more than 500 employees to work full time on every aspect of the attack."

In the new edition, Smith also reflected on his congressional testimony on SolarWinds. The hearings, he wrote, "examined not only what had happened but also what steps needed to be taken to prevent such attacks in the future." He didn't mention it in the book, but that certainly would include the long-term alternative that Morowczynski first promised to Harris in 2017. The company began offering it in 2022.

Development by Lucas Waldron.

Renee Dudley
Renee Dudley is a tech reporter at ProPublica.
renee.dudley@propublica.org @renee_dudley 929-317-0748

Doris Burke
Doris Burke is a senior research reporter at ProPublica.

Mr. THOMPSON. I'm sure you are somewhat familiar with that article and the fact that we were left vulnerable with that situation.

Can you say to us or commit to us that you have established a process for an ombudsman to ensure that employee concerns about security at Microsoft or their products are prioritized and addressed?

Mr. SMITH. Well, one of the changes we've just made as part of the Secure Future Initiative is a new governance structure. It takes our chief information security officer, or CISO, as it's called in the industry, creates an office, and then puts deputy CISOs in every part of the company. The job of these individuals is to constantly monitor and assess and pick up feedback and apply a prin-

cipled approach to address these things. So I would hope that that would address part of what you're referring to.

I would say one other thing, though. The fundamental cultural change that we are seeking to make is to integrate security into every process. We've really thought a lot over the last couple months, what's the key to getting better when your adversary is investing and constantly changing?

The thing that we have really concluded is, there's a lot that we can learn from what's called "total quality management." This really came out of American business thinking, and then Toyota really innovated it in the 1980's. The basic process was to empower every employee to focus on continuous employment—sorry—continuous improvement and speak up.

That's what we're trying to do: empower every employee to be able to speak up—and there's going to be debates; I mean, I don't think one can say that debates will end—but to ensure that those voices are heard and heeded.

Mr. THOMPSON. Well—and I trust, based on what you've said, that that will be—that, going forward, that anybody who comes forward with something, they will be at least heard and responded to.

With respect to that, we are here because of Storm–0558, as it's commonly referred to. The real concern is, Microsoft didn't find the problem; it was the State Department.

Help us out.

Mr. SMITH. That's a great question. The one thing I'd ask all of us to think about is: That's the way it should work. No one entity in the ecosystem can see everything. So we all need to work together. The way networks are constructed, people will see specific endpoints.

In this case, as you know, it was the individuals at the State Department who saw the intrusion into the State Department email system. First of all, you ought to give those folks a medal, in all seriousness. That is fantastic. That is real innovation and great professionalism at work. So they let us know.

By the way, we're the ones, interestingly enough, at the same time, who identified the Chinese intrusions into electricity companies, water companies, air traffic control systems.

We're all going to see different things. So, when somebody else sees it, we should applaud and say, "Thank you," not say, "Oh, I wish I had found it instead."

Mr. THOMPSON. Well, I wish it were that simple. But we have a real challenge. Because you are such a big customer of Government, we rely heavily on your product. It's not our job to find the culprits. That's what we're paying you for. So I want you to—don't switch the roles——

Mr. SMITH. I'm not switching it at all. I——

Mr. THOMPSON. OK.

Mr. SMITH [continuing]. Appreciate what you're saying for sure.

Mr. THOMPSON. Great.

So I—maybe we'll have another round, Mr. Chairman, but——

Chairman GREEN. You can ask your question.

Mr. THOMPSON. OK. Well, thank you.

So the Federal Government is one of your largest customers, as I said. How can you earn back the trust that this situation has caused?

Mr. SMITH. I think it's just critical that we acknowledge shortcomings, accept responsibility, devise a strategy to address them, change the culture, be transparent about what we're doing, and always listen to feedback.

Mr. THOMPSON. Thank you.

I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the gentleman from Louisiana, Mr. Higgins, for his 5 minutes of questioning.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Smith, congratulations on your company's success. In fact, it's the very success of Microsoft that makes you such a big target, isn't it?

Mr. SMITH. That's certainly a part of it.

Mr. HIGGINS. Would you generally agree that Microsoft has grown so massive because of your own technological advancements that you have driven from within your company and because of the trust that has been extended to Microsoft products through the decades?

Mr. SMITH. Yes, I think that's fair. I think success comes from many things, but, of all of the factors that we place the most importance on, I would say earning and retaining the trust of our customers——

Mr. HIGGINS. OK. So we're in agreement, you and I.

Mr. SMITH. Yes.

Mr. HIGGINS. Microsoft's a great company. Everybody in here has some kind of interaction with Microsoft. We really don't have much choice. So it's critical that this committee gets this right.

Quite frankly, the American people, myself included, we have some issues with what has happened and how it happened and what has transpired since. Yet there's no plan B, really. We have to address with you, is what that means. Sometimes life comes down to—my dad used to say, there's always one guy. It's always one guy. Today, congratulations——

Mr. SMITH. I'm the guy.

Mr. HIGGINS [continuing]. You're the one guy.

Mr. SMITH. I get it.

Mr. HIGGINS. So I have a couple of difficult questions, and I apologize for any discomfort, because I am a gentleman——

Mr. SMITH. Yes.

Mr. HIGGINS [continuing]. But, again, you're the guy.

Why did Microsoft not update its blog post after the hack—they call it—it's very fancy here, America calling it an "intrusion." But after the hack, the 2023 Microsoft Online Exchange intrusion, why did it take 6 months for Microsoft to update the means by which most Americans would sort-of be made aware of such a hack?

Mr. SMITH. Well, first of all, I appreciate the question. It's one that I asked our team when I read the CSRB report. It's the part of the report that surprised me the most.

Yes, we had 5 versions of that blog, the original and then 4 updates. We do a lot of updates of these reports. When I asked the

team—you know—they said the specific thing that had changed—namely, a theory, a hypothesis, about the cause of the intrusion—you know, changed over time, but it didn't change in a way that would give anyone useful or actionable information that they could apply——

Mr. HIGGINS. OK. So you see, Mr. Smith, respectfully, that answer does not encourage trust. Regular Americans listening are going to have to—are going to have to move the tape back on a Microsoft instrument and listen to what you said again.

Mr. SMITH. But——

Mr. HIGGINS. But you didn't do it. I mean, you're Microsoft, you had a major thing happen, and the means by which you communicate with your customers was not updated for 6 months. So I'm just going to say, I don't really accept that answer——

Mr. SMITH. Could I just add——

Mr. HIGGINS [continuing]. As thoroughly honest, but I need to move on——

Mr. SMITH. No, could I—then could I just say——

Mr. HIGGINS [continuing]. To another question.

Mr. SMITH [continuing]. I said the same thing, and we had the same conversation inside the company.

Mr. HIGGINS. OK. I accept that, that you did.

So, bigger question: China. I mean, you go to China. You meet with—you, like, went to China. I guess you've made many trips there. You're doing business there. That's fine. But you meet with Chinese Communist Party officials, and you reiterated Microsoft's support for helping the CCP achieve technological advancements. I believe this is your quote—I'm asking you—to "actively participate in the digital transformation of China's economy." I believe that was your statement.

My question is, does it strike you as contradictory that you would make that statement just months after China sponsored the attack that we're discussing?

I yield for your answer, sir.

Mr. SMITH. The reality is, that was not my statement. I chose my words more carefully. That was the statement made by an official of the Chinese Government, attributing it to me.

Mr. HIGGINS. So that was not your quote?

Mr. SMITH. I was—let me just say, I was more careful and precise in what I said, and that was not my quote.

Mr. HIGGINS. So you find it as contradictory or——

Mr. SMITH. Sorry?

Mr. HIGGINS. You say that's not your quote, but——

Mr. SMITH. No, I mean, it——

Mr. HIGGINS [continuing]. Was that the position of Microsoft?

Mr. SMITH. It—what I——

Mr. HIGGINS. My time has expired. I'm just trying to complete this answer.

Mr. SMITH. I'll just—I'll just—yes, I thank you for giving me the opportunity.

I explained in a meeting that there were areas where we thought it was appropriate and even important for us to be present and participate. But I did not choose or use the words——

Mr. HIGGINS. OK.

Mr. SMITH. When I saw that quote appear, I was like, "Hmm, interesting."

Mr. HIGGINS. Thank you, sir.

My time has far expired. I yield, Mr. Chairman.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Swalwell for his 5 minutes of questioning.

Mr. SWALWELL. Thank you, Chairman.

I wanted to echo the Ranking Member's sentiment, that I don't view this hearing as a shaming of any particular company but, rather, an opportunity to learn from mistakes in the past so that we can better secure the digital ecosystem, especially with, you know, a company that has such a large footprint in that ecosystem.

So, first, Mr. Smith, I was hoping we could go back to the *ProPublica* story where an employee alleges that a vulnerability was discussed and it was at the same time you were seeking Government business.

Knowing that you do have so many Government clients today, as we sit here today, are there any vulnerabilities within your operating system that have been expressed to you, similar to what was alleged in the past, that would affect any Government system that you're aware of?

Mr. SMITH. What I would say is that everything that we're doing is focused on identifying every vulnerability that we can find, every vulnerability our employees can find, so we can go address them.

Given the diversity of digital technology, given the complexity, I'm not sitting here today aware of anything that fits your description, but I am constantly hoping that every day we'll have people who find something and raise it so we can fix it. That's the culture we need, I think.

Mr. SWALWELL. "So we can fix it," which I think is the theme——

Mr. SMITH. Exactly.

Mr. SWALWELL [continuing]. Here today.

In that spirit of what can we fix, what did you learn from the internal decision-making process on updating the blog post on the root cause of how the Chinese threat actor got the key? Like, what would you do differently in an existing attack?

Mr. SMITH. You know, we get—a lot of times, people say, "Why do you update things so often?" You know, "You lose people's attention." I think the answer is: Because we need to. We updated that particular blog 4 times. It was at least one time too few. We should've updated it again.

So I just think that the lesson learned is: You know, maybe it's something you see a lot in life; it's hard to overcommunicate. Let's work even harder to overcommunicate.

Mr. SWALWELL. You discuss in your written testimony the growing connection between nation-state activity and ransomware.

A city in my Congressional district, Hayward——

Mr. SMITH. Yep.

Mr. SWALWELL [continuing]. Was hit very hard and experienced a ransomware attack last year, where the city's on-line operations were crippled and a state of emergency was declared.

Where do you see these ransomware attacks happening? What types of targets in the United States do you see as most at risk?

Mr. SMITH. Well, this is a critical issue. I hope this committee and we all can find new ways to work on it. Because it was last July in Hayward where, as you know, systems went off-line for 2 weeks. In Hinds County, you know, in the Second District of Mississippi, they had a similar problem. They had to write a check for $600,000—I suspect it had to be converted to cryptocurrency—and it was probably mailed to Moscow, even if it was over the internet.

This is a scourge and the No. 1 vulnerability right now. It's just, I think, so disconcerting that ransomware operators are focused on hospitals, rural hospitals. There were 389 health care institutions last year that were victimized.

So some of the suggestions that the Chairman and Ranking Member Thompson alluded to at the beginning, I think, require that we all come together to help these institutions. We launched an initiative just, you know, 3 days ago. We weren't alone; the White House did it, Google did it. We all need to do this together.

But I also think we need to send a message. I think that message has to be sent to Moscow. We need to remind them that when we fought with them 80 years ago it was to protect people, and it was reflected 4 years later in the Geneva Convention that said, even in times of war, governments have to protect civilians.

This is supposed to be a time of peace, at least between our two countries. What are they doing? They are enabling their employees to use the tools they get at work and go home and run these ransomware operations and target hospitals or cities and counties, schools—the Jackson School District, the Vicksburg Warren School District. This is unconscionable.

I think we have to find our voice, not only for ourselves but with our allies, and not only as governments but with the tech sector, with the business community, and we have to find a way, as a country, to create a deterrent reaction. Because, right now, this is just open season. It's open season on the most vulnerable people in our country, and we have to find a way to change that.

Mr. SWALWELL. Thank you, Mr. Smith.

I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Gimenez for 5 minutes of questioning.

Mr. GIMENEZ. Thank you, Mr. Chairman.

I know a lot of other committee Members are going to home in on the security breach. I'm more interested in Microsoft's presence in China, which I consider to be the greatest existential threat to our security here in the United States.

Your presence in China, is that a joint venture or is that fully owned by Microsoft? What's the nature of that relationship?

Mr. SMITH. I don't recall all of the precise corporate structures. We do operate as a subsidiary. We also do have a joint—we have at least one joint venture for certain activities.

Mr. GIMENEZ. Are you aware of 2017 National Intelligence Law in China?

Mr. SMITH. Yes, I am.

Mr. GIMENEZ. Do you know what that law states?

Mr. SMITH. If I remember correctly, one of the things it states is that, when an organization finds a vulnerability, it has to report——

Mr. GIMENEZ. No, sir, that's not the one I'm talking—that's not where I'm going, OK?

Mr. SMITH. OK.

Mr. GIMENEZ. So, here, I just happen to have AI myself.

Mr. SMITH. Hopefully it's ours.

Mr. GIMENEZ. Oh, yes. I don't know. If it is, it's pretty bad for you, because it says this——

Mr. SMITH. OK.

Mr. GIMENEZ [continuing]. OK?

"Yep, in China, there is a law called the National Intelligence Law that was implemented in 2017. This law requires all organizations and citizens to cooperate with China's intelligence agencies, including the People's Liberation Army, in matters of national security. While the law does not specifically mention companies working in China, it does apply to all organizations operating within the country, including foreign companies."

Do you operate in China?

Mr. SMITH. Yes, we do.

Mr. GIMENEZ. Do you comply with this law?

Mr. SMITH. No, we do not.

Mr. GIMENEZ. How is it you got away with not complying with the law? Do you have a waiver from the Chinese government saying that you don't have to comply with this law?

Mr. SMITH. No, we do not, but there are——

Mr. GIMENEZ. You do not?

Mr. SMITH [continuing]. But there are many laws—there are two types of countries in the world: those that apply every law they enact and those who enact certain laws but don't always apply them. In this context, China, for that law, is in the second category.

Mr. GIMENEZ. Do you really believe that? Because, look, I sit on the Select Committee on China, and that's not the information that we get, is that all companies in China have to cooperate with the intelligence agencies of China and the People's Liberation Army.

You operate in China, and you're sitting there telling me that you don't have to comply with the laws of China?

Mr. SMITH. I will tell you that there are days when questions are put to Microsoft and they come across my desk and I say, no, we will not do certain things.

Mr. GIMENEZ. But you're complied by Chinese law to do it. The people in China that work for Microsoft are violating Chinese law when they don't do it.

Mr. SMITH. I always make sure that it's clear to the Chinese government that if the Chinese government wants to sue somebody they need to sue me. I have——

Mr. GIMENEZ. It's not about suing. In China, they don't sue you, man. They arrest you, OK? Do you understand that?

Mr. SMITH. Clearly. We make clear that there's no point in arresting people who have no authority to do these things.

Mr. GIMENEZ. They have the authority to do those things because it's their law.

Mr. SMITH. No——

Mr. GIMENEZ. You're in China.

Mr. SMITH. No. I'm talking about our employees.

Mr. GIMENEZ. OK, yes. Your employees in China are subject to Chinese law.

Mr. SMITH. But they——

Mr. GIMENEZ. Are they not?

Mr. SMITH. But they don't have the ability to make these decisions. We've taken that out of their hands.

Mr. GIMENEZ. I'm sorry, I just—for some reason, I just don't trust what you're saying to me, OK?

You're operating in China. You have a cozy relationship in China. You're there. They allow you to be there. I can't believe that they're going to say, "Yes, OK, no problem. You don't have to comply with our law that everybody else does. Every other foreign company has to, but not Microsoft."

I—I'll take you at your word——

Mr. SMITH. I can——

Mr. GIMENEZ [continuing]. But—but——

Mr. SMITH. Yes.

Mr. GIMENEZ [continuing]. I'm just demonstrating to you the problems that we have with American companies working in China and that, for 1 percent of your resources, or of your income, is it really worth it to be in Communist China, especially when you have such a law that says you have to comply with their intelligence agencies and the PLA?

Mr. SMITH. The thing I would ask all of us to think about—and I—look, I appreciate your questions and the seriousness of them. We think constantly about these things.

I do think that there's two valuable reasons for us to be in China, and I think they both serve the interests of the United States. The first is to protect American information, American trade secrets of American companies who are doing business in China. The second is to ensure that we're always learning from what's going on in the rest of the world——

Mr. GIMENEZ. That—could I—I only have 13 seconds. Could I say this? Those American companies and all these American secrets that are working in China, they have to comply with the same law. Do you think they all do?

Thank you, and I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Correa for 5 minutes of questioning.

Mr. CORREA. Thank you, Mr. Chairman.

I'd just welcome you, Mr. Smith. Also, as the Ranking Member said, this is not a shaming situation. But yet, you know, reading on this issue—I've been on Homeland for 8 years—this is very disturbing. That statement is an understatement as to how I'm feeling right now.

What do I tell my constituents back home that actually pay you for your services, that an unsophisticated password spray, password key, well-known vulnerabilities, enabled this to happen?

Mr. SMITH. I think—I would hope you would tell them——

Mr. CORREA. I'm asking you.

Mr. SMITH. Oh. What should I tell them?

Mr. CORREA. What should I tell them?

Mr. SMITH. I would hope that you would share with them that we acknowledge these issues——

Mr. CORREA. They are paying you for your service. It's not a freebie. They're paying you. I pay you. I run your service up here and at home; I also pay you for service.

Mr. SMITH. I would—I want people to know, on the one hand——

Mr. CORREA. Not one hand or the other. Just tell me straight-up——

Mr. SMITH. OK.

Mr. CORREA [continuing]. What's the message?

Mr. SMITH. The message has two parts. First, we see our customers attacked more than 300 million times every day, and we have people who work 24/7——

Mr. CORREA. Are we doing our job as the Federal Government in helping you, or is there something else we can do to help you do your job better?

Mr. SMITH. I think that there are things that we could do more together, and I would love to see the Federal Government focus on a few key things.

I think that the investment in cybersecurity training that the Chairman mentioned at the outset is an imperative. I think we have done a lot. We have trained, as a company, 203,000 people in this Nation in the last 4 years on cybersecurity. But we need the Federal Government to do more.

I think we need Federal assistance to help our critical infrastructure providers upgrade their technology. I think we need the kind of——

Mr. CORREA. Do you, Microsoft, need to invest more in this area?

Mr. SMITH. We are investing more. We've increased our investment. But, more that that, I think it's——

Mr. CORREA. Do you believe that Microsoft responded in a timely basis to these known breaches?

Mr. SMITH. We both responded immediately with people who work 24/7, pretty much around-the-clock——

Mr. CORREA. As soon as you found out this stuff was happening, you responded?

Mr. SMITH. I'm sorry?

Mr. CORREA. As soon as you found out or you would find out these breaches are occurring, you respond?

Mr. SMITH. Oh, absolutely.

One thing I would love for you all just to know is that, despite these tens of millions of attacks every year——

Mr. CORREA. Do you respond to known vulnerabilities immediately?

Mr. SMITH. Yes. We respond to every intrusion. We address vulnerabilities.

Mr. CORREA. We know the challenges that our competitors around the world pose to us, friendly and unfriendly. I would love to talk to you sometime in the SCIF to tell us exactly what it is that we need to do to make sure this doesn't happen again, as I am beyond shocked to read about this situation.

You have our trust, our business, both at the public and the private sector. To hear about what's going on here is very disturbing at best. I hear you saying, "You know what? We're here to cooperate fully." The damage, though. I've got constituents back home

that have been—lost money because of malware, so on and so forth. It's painful.

The private sector, they run on your platforms. They trust on you being on top of your game. Any thoughts?

Mr. SMITH. We are determined. We start by acknowledging where we fell short. We are focused. I had a—the last comment made with our board of directors yesterday was by the senior engineer leading what we call the Secure Future Initiative, and her last words to our board were, "We want you to know, our engineers are energized by this." And——

Mr. CORREA. In my last 9 seconds, I would ask you: You know, we often say here that the chain is only as strong as its weakest link. Are you going to strengthen up? Are you going to do a better job over there?

Mr. SMITH. Absolutely.

Let me just say this in closing: I would hope that you would share with your constituents, we never take their trust for granted.

Mr. CORREA. Chair, I'm out of time.

Chairman GREEN. The gentleman yields.

A point of clarification for the record, it was 300 million attacks a day? Did I hear that correctly?

Mr. SMITH. Yes, that is correct, against our customers that we observe. We detect more than 300 million such attacks every day.

Chairman GREEN. Just clarifying for the record.

I now recognize Mr. Pfluger for 5 minutes of questioning.

Mr. PFLUGER. Thank you, Mr. Chairman.

Mr. Smith, thanks for being here. I want to talk about the collaboration. In many committees on Capitol Hill, we're talking about this balance and tension between safety and security and liberty and, you know, private enterprises.

So what I really want to hear from you is talk to us about the relationship with CISA. I know you've mentioned this in testimony written and also today, but just talk to us about how that relationship is, what can be better from your side, what can be better, what you expect from the Government.

Is it a mandate for reporting from the Government? Is it, you know, voluntary roundtables in a Classified setting? I'd like to hear a little bit about that, and I have some follow-up questions.

Mr. SMITH. Yes. I think CISA is a critical agency. It's been moving in a positive direction overall. I think the CSRB plays an important part of this.

I think that ultimately we would benefit from finding more ways to keep working together across the tech sector and then with the CISA and other agencies in the U.S. Government and, frankly, with our allies, because it's an entire ecosystem that we're seeking to defend, and nobody can do it by themselves.

I think fundamentally, just as—the CSRB's words were well taken by us. We needed to focus on our culture. I think we have a collective culture, and it's a collective culture that we need to work on by inspiring more collaboration not just with the Government but, frankly, across our industry.

So that, you know, people compete. Somebody said, there's no plan B. I think about two-thirds of the folks who are sitting behind

me in this room are trying to sell plan B to you in one way or another, and that's OK.

But there's a higher calling here as well. I like to say, you know, the truth is when shots are being fired, people end up being hit, and they take their turn being the patient in the back of the ambulance. Everybody else, you're either going to be an ambulance driver or you're going to be an ambulance chaser. Let's be ambulance drivers together.

Mr. PFLUGER. Let's drill down to that and the relationship that you have with the U.S. intelligence community, with DOD. The thing that's unique about Microsoft is you pretty much cover every sector, every industry, every—you know, households, businesses.

But when you look at the relationship with the national security entities, tell us what the biggest gaps are right now to making sure that they can stay secure in their operations.

Mr. SMITH. The thing to think about is that defenders too often work in silos. Every company thinks about their products. Every agency thinks about what they have. Attackers look for the seams between the silos. The more silos you have, the more seams you have.

Just as there are seams in different technology products, because most customers deploy them together, there are seams across the Government. So a lot of times one of the challenges for us is that the parts of the Government, when this information is coming in about, say, an active cyber attack from a place like China, that information doesn't necessarily flow from one part of the Federal Government to another. There's a lot of work being done to address this, but I think that needs to be advanced more quickly as a matter of priority.

Mr. PFLUGER. Three hundred million attacks a day, that's incredible.

Finally, let me just talk about—I think—this is the Committee on Homeland Security. We're very worried about what nation-state actors and non-nation-state actors are doing and how that affects our homeland. Obviously, the PRC and the CCP's attempts to undermine this country, our Government, industries, intellectual property, all of it is a massive concern.

So I know you've mentioned this before here today, but just talk to us a little bit about the relationship with the PRC. How does that affect intellectual property, things that you have that could be either exploited for their benefit to undermine the United States of America?

Mr. SMITH. I would say two things: I mean, first, any company that has valuable intellectual property has to be very careful to protect it from theft, unless it's IP that they're publishing, and a lot of code is published in open-source form.

But you have to think about how to protect it so it doesn't go where it should not. There are certain intrusions, especially from, say, a place like the PRC, you know, that are focused on discovering trade secrets.

Mr. PFLUGER. Knowing that, is Microsoft taking steps to improve what you're protecting?

Mr. SMITH. Absolutely. Absolutely. I mean, it's—the other thing just to know is that the adversaries are constantly changing their

tactics. If this were a case of just saying, gee, this is what was done in like 2022, let's all go fix what was done in 2022, then you'd feel good.

But I guarantee that what is done in 2025 is going to be different from what is being done in 2024. You constantly have to learn, adapt, and change, which is what we're doing.

Mr. PFLUGER. Thank you. My time is expired. I have more questions. We'll submit them for the record.

Mr. Chairman, I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Carter for 5 minutes of questioning.

Mr. CARTER. Mr. Chairman, thank you very much.

Mr. Smith, thank you for being here. Mr. Smith, it's no secret that our critical infrastructure is being targeted. I'm particularly worried about rural hospitals and how they continue to be targeted and attacked by nation-state threat actors.

Just this week, Microsoft announced a new rural hospital cybersecurity program. One of the hospitals in my district, Saint James Parish Hospital, is a participant.

Would you describe this program and how it will help the Nation's rural hospitals defend against attacks?

Mr. SMITH. Yes. Thank you. We talked a little bit about this before, obviously. I just think it's a critical priority for the whole country, because people's lives literally are at stake. What we have launched this week is, first, a program to provide technology assistance to hospitals, especially rural hospitals, giving them security tools—you know—at the lowest possible price. In some cases, it's a 75 percent discount. In some cases, it's free of charge for a year.

The second thing we're doing is then going in and helping with all that know-how, advisers, technology assessments, so we can work with people.

The third thing we're focused on is then trying to help them use technology so that they can be more effective. As I'm sure you're seeing, right now there are a lot of rural hospitals in this country that are barely afloat.

When a rural hospital closes, not only do people lose access to local health care, but some of the good jobs in the community are destroyed at the same time. There's a shortage of people to work in these hospitals.

So one of the things we're trying to focus on is how can we use digital technology, especially AI, you know, to improve the quality of rural health care, reduce the cost, not just for the patients but for the operators of these especially small hospitals with, say, 25 or fewer beds.

So we're trying to put together a holistic approach that we think could make a difference.

Mr. CARTER. What about HBCUs and other small organizations that could likewise use technical assistance and the help that might be in a similar situation financially as a rural hospital?

Mr. SMITH. Well, we have educational pricing in general, but I would say there's two categories in the educational community that deserve special priority, and we're trying to give them special priority.

One is HBCUs and, therefore, we've created a special program to invest in them, to provide scholarships, to work on cybersecurity training and the like.

The second is the Nation's community colleges. I feel that this is the great resource, the 1,000-plus community colleges in this country. We need to equip them and send them into this battle.

That requires 3 things: One is equipping them with the curriculum, which we can do, and other tech companies have done a good job as well. I want to spread credit where it's due.

Mr. CARTER. I don't want to interrupt you, but I have got a few more questions and a little bit of time.

Mr. SMITH. OK. I'll let you go. I'd be happy to talk to you any time.

Mr. CARTER. Was that a yes?

Mr. SMITH. Yes.

Mr. CARTER. That is a yes——

Mr. SMITH. That is absolutely a yes.

Mr. CARTER [continuing]. That you are prepared to and have programs to work with other disadvantaged organizations, particularly HBCUs.

Mr. SMITH. Yes.

Mr. CARTER. OK, great. The increasing frequency and sophistication of nation-state cyber attacks in the United States, do you agree that the country is currently lacking in having successful deterrent strategy? If so, what steps are needed to enhance deterrents, and what can we do in addition to partnering with you to do that?

Mr. SMITH. This is a critical and hard problem we need to solve as a Nation, and it requires we do 3 things: First, we've got to draw the red lines so it's clear to the world what they cannot do without accountability.

Second, we need transparency. We need collective action with the private and public sector and with allied governments so that when those red lines are crossed, there is a public response and people know what has happened.

Third, we need to start defining some consequences, because right now these threat actors are living in a world where they are not facing consequences.

Mr. CARTER. Real quickly, I've got 30 seconds and I've got a real important question. I'm going to read this, because I want to make sure I get it right.

Earlier this year, I was briefed by members of the Cyber Safety Review Board about its review of last summer's incident, and I wanted to raise an issue we discussed there on value logging.

Members of this committee have for years raised concerns that Microsoft was charging extra money for customers to gain access to basic logging data, and customers need to identify and investigate cyber incidents.

When you or one of your representatives testified before the committee in the aftermath of the SolarWinds breach, they explained that everything that we do is designed to generate a return, other than philanthropic work.

The State Department paid for extra logging, generating a profit for Microsoft and ultimately using these logs to detect this attack,

but not every customer had that logging capability enabled. Last summer, Microsoft finally announced that it would provide free logging to customers, and in February made those logs available for all Federal customers.

Why did it take so long to make this decision, and what was the—went into your changing your mind?

Mr. SMITH. Well, in fact, we've even gone a little bit farther than——

Mr. CARTER. That's fine, but can you just answer the question I asked?

Mr. SMITH. I wish we had moved faster and had gone farther. I think there was a focus on the real cost associated with keeping and retaining logs, but we should have recognized sooner, especially as the threat landscape changed, that we would be best served, I think as we are now, by not just retaining but providing these logs for free.

Mr. CARTER. So what's the status on providing free logs to all customers and not just Federal agencies?

Mr. SMITH. Basically, what we've decided is for all of our so-called enterprise offerings, there's 3 layers and for all of them we retain the logs for 6 months, which is what the CSRB recommended.

We will provide those logs, say, these are individual customer logs. We will provide them to those customers. They get access to them when they need them at no additional cost.

Mr. CARTER. Would you agree that it's as important for Microsoft, the company, to have this level of security for its customers as it is for customers to, in fact, have the security?

Mr. SMITH. Yes.

Mr. CARTER. Thank you. My time is expired.

Chairman GREEN. The gentleman's time is expired.

I now recognize Ms. Greene for 5 minutes.

Ms. GREENE. Thank you, Mr. Chairman.

Mr. Smith, this has been a very engaging, intriguing conversation. I'm a business owner, so I've been listening to this and, you know, taking it in and thinking about it through that lens.

You started with something that I find impressive. You said you accept responsibility, and I just want to commend you for that. I appreciate it. We don't hear that very often here, but I think it's valuable and I think it's right. So I just wanted to say thank you.

I understand that Microsoft has a unique role to play in our cybersecurity landscape, as it's responsible for nearly 85 percent of the productivity software, such as Word, Excel, and PowerPoint used by the U.S. Government.

Given the company's presence, Microsoft is, of course, at significant risk of cyber attacks. Over 300 million a day. Is that true, 300 million a day?

Mr. SMITH. We detect 300 million a day against our customers. So that's what we get to see, given all of the telemetry we have. Last year, if you look at, you know, phishing attacks, we had 47 million against ourselves over the year.

Ms. GREENE. Wow. That's far more than I——

Mr. SMITH. It's a lot.

Ms. GREENE [continuing]. Could have even comprehended. Of course, these are serious. We're all—everyone here on the committee is recognizing that.

As you stated in your testimony, cyber attacks have become more prolific, just as you stated. As a result of the attack that your company went under, in May 2021 the Biden administration released an Executive Order on improving the Nation's cybersecurity which required the establishment of the Cyber Safety Review Board under DHS.

I want to talk to you a little bit about the board. I think, of course, oversight is important, but I think there should be more action taken by our Government to prevent cyber attacks.

So could we talk a little bit about the board? My understanding is the Cyber Safety Review Board is a mix of Government and industry representatives.

Is it true that Microsoft is not represented on the board?

Mr. SMITH. That is correct.

Ms. GREENE. Is any of your competitors on the board?

Mr. SMITH. Yes, they are.

Ms. GREENE. So, essentially, the—so how did this work? When this attack happened, the board—can you talk a little bit about that process?

Mr. SMITH. Yes. You're getting at such a critical question, because I will say, first, I think we benefit from having this kind of organized effort. I think it's probably a mistake to put on the board people who work for competitors of, say, a company that is the subject of a review.

The spirit of this when it was created was to create a community of people who could learn together, but I just don't—I'm less concerned about the way the process worked. I just worry that where people want to take it in the future and just make hay out of others' mistakes, and I'm just not sure that's going to do us that much good.

Ms. GREENE. Right. So did CSRB, did it share with Microsoft what your competitors said about their own security practices?

Mr. SMITH. I don't believe so. I don't know—I don't believe so. I could be wrong, but I don't believe so.

Ms. GREENE. OK. With your competitors on the board helping produce the report, was this used in any other way in the marketplace?

Mr. SMITH. Yes. I just—I want to say two things because, first, I think the most important thing for me to do and for Microsoft to do is what you said at the outset. I just want to be here and accept responsibility. I don't want to deflect any of that responsibility, because we have the highest responsibility.

But, second, the words that I would offer—and I'll offer it to the folks in the back who work for our competitors, because there's a bunch of them here—it's fine. Go tell people that you have something better, but we have to have a higher cause here. We are not the adversaries with each other even though we may compete with each other. The adversaries are our foreign foes.

So let's try to exercise a little self-restraint about how we work in these processes, because I don't think that the next company

that gets an invitation from the CSRB is likely to be necessarily as willing as we were to share everything, which we did.

Ms. GREENE. Well, I agree, I think competition is healthy——

Mr. SMITH. I do too.

Ms. GREENE [continuing]. In the business world. I think it's great, actually. I enjoyed it for years and years. But I think oversight is also extremely important. Of course, I think everyone in this room agrees that we do not want any foreign country gathering any of our information, whether it's from an American citizen to our Government, of course.

CISA also has been—has a bad reputation, especially among Republicans. They colluded with big tech and social media companies, stripped many Americans of their First Amendment rights. So that was another reason why I wanted to ask you a little bit about the board and how that worked.

But furthermore, I have more questions, but I'm out of time. I think it would be extremely important for there to be assistance from the Federal Government in protecting not only companies like yours but mom-and-pop companies, I mean, across the board to regular citizens from cyber attacks. It's a serious problem and it will continue. I'm out of time. Thank you.

Chairman GREEN. The gentlelady yields.

I now recognize Mr. Thanedar for his—or Dr. Thanedar for his 5 minutes of questioning.

Mr. THANEDAR. Thank you, Mr. Chairman.

Thank you, Mr. Smith, for being here.

I owned a small technology company before I came into public service, a much smaller technology company. I was involved with some—8 different acquisitions.

Now, the CSRB raised questions about Microsoft's mergers and acquisitions compromise assessment program after it failed to detect that a laptop belonging to an employee of an acquired company had been compromised.

The board went on to recommend that large enterprises develop a robust M&A compromise assessment program, recognizing adversaries might view the acquiree as an entry point to the parent company.

How is Microsoft improving its M&A compromise assessment programs? Is there additional support or guidance the Federal Government should be providing the private sector regarding M&A compromise assessments?

Mr. SMITH. I'm not sure of the answer to your last part, but I do know that it's critical that we do more. We've been focused on this for a long time, and it's sort-of an, I'll even say, obvious thing that when you acquire a company you have to take a close look at its cybersecurity controls, which we long have and do.

Yet, as the CSRB report found, we had an inadequacy. So, in part, to address this, part of the governance change we're implementing is to have a new deputy chief information security officer focused solely on the integration of companies that are acquired, because we clearly need to step it up and will.

Mr. THANEDAR. Thank you. Mr. Smith, as you state in your testimony, nation-states adversaries are becoming more aggressive. Countries like China, Russia, Iran, and North Korea present grave

threats to our national security, and defending against them would require public-private cooperation that prioritizes strengthening cybersecurity across government networks and critical infrastructure.

Considering our reliance on large IT vendors like Microsoft, our defenses will only be as strong as our technology providers are. That is why it was so disappointing to see the CSRB report that Microsoft had failed to properly secure its products.

Microsoft must do better, and I expect that Microsoft will continue to update the committee on its progress. Congress must also do more to ensure the Federal Government has the resources to meet the goals of President Biden's ambitious national cybersecurity strategy.

Mr. Smith, how is Microsoft improving its security to protect itself and its customers to address these increased foreign threats?

Mr. SMITH. It's a multifaceted effort. As I said in my written testimony, it really starts with what is today the largest engineering project focused on cybersecurity in the history of digital technology, you know, with detailed milestones, 34 different categories. I think that's critical.

But it really is I think a new approach to cybersecurity culture. It's a new approach for Microsoft. The more time I spend with it with my colleagues, the more encouraged I am, because fundamentally, it's about taking security and making it part of the engineering process and every process. Treat it like quality.

The cultural change—and several of you have commented about this—I just think it's so important. We want a culture that encourages every employee to look for problems, find problems, report problems, help fix problems, and then learn from the problems.

That's what we need to do. We need to do this in a way that doesn't put security in its own silo, although there are special security teams, but make security part of everyone's job. I think that is one of the indispensable steps we are taking and really need to take.

Mr. THANEDAR. Thank you. With my last 30 seconds, what investments should Congress prioritize to improve our national defenses against nation-state cyber threats?

Mr. SMITH. Invest in the American people. Invest in the training of the American people. Provide more scholarship assistance so that Americans can go to a community college, go to an Historically Black College or University, get a course, get a certificate, get a degree in cybersecurity. There are 400,000 open jobs in the United States today in cybersecurity. Help us fill those jobs.

Mr. THANEDAR. Thank you.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Gonzales for 5 minutes of questioning.

Mr. GONZALES. Thank you, Mr. Chairman.

Mr. Smith, is Microsoft Teams a secure platform?

Mr. SMITH. I believe it is. I use it every day for lots of sensitive conversations.

Mr. GONZALES. I would say I'm concerned. I'm concerned with the trust level that Americans have with Microsoft for a variety of different reasons. I believe Microsoft has been a trusted agent for a long time, and let me give an example.

If you work for the Department of Defense and let's say you want to communicate with others in an unclassified environment, but let's say it's in an official capacity, right? Oftentimes the conversation is, don't use Zoom or others like that, because that's an unsecure platform. Let's use Microsoft Teams.

What I'm seeing, what I'm starting to hear is more and more Government officials, Government agencies, DOD-affiliated folks not trust that. So if Microsoft—if they don't trust that, what options do you have?

Once again, I understand if it's a Classified setting, but I'm talking about how do you reach people without a CAC card, without having to go down the CAC card route? Is there anything that is in the works in order to regain some of that—whether it's warranted or not, there is an eroding amount of trust within Microsoft.

Is there anything in the pipeline that will regain that trust among DOD-affiliated organizations?

Mr. SMITH. Well, first of all, I appreciate the fundamental gravity of the question. I would say that we are continually and constantly focused as part of this work that we're doing in increasing the security for every aspect of what we do, including Teams and every aspect of it.

I feel comfortable talking with the DOD or others on Teams. I want them to feel comfortable, and I want them to know that we are not stopping where we are, because our adversaries are not stopping where they are. We are going to continue and are continuing to invest in hardening the security of Teams even more than it has today.

Mr. GONZALES. Thank you for that. A large part of what we do on this committee is try to get everyone out of silos, right? All these agencies are in silos. Every time there's a national security threat, you look back at these reports and it's always somebody knew something but, you know, when did they know it?

Part of that is the ability to communicate in a, you know, FOUO setting that where you feel as if maybe it's not quite the Classified level but you feel, you know, not everyone is listening on it. I just would reiterate how important that is from a national security standpoint to ensure that the Government has at least some platforms like Microsoft Teams.

My final question is this: How is Microsoft planning to combine your SFI while ensuring tools and software remain user-friendly and accessible?

Mr. SMITH. Great—first of all, I want to just thank you for your first set of questions, and I will quote you back in the company's headquarters.

Second, the point that you make is also so critical, because we have to make security first a top priority, but we have to make it easy for people to use. So we do need to synthesize these things.

I think one of the virtues of what we're doing is not just calling on deeply technical engineers, but also people say in the field of software design and elsewhere.

I think part of our quest—I think it's a great quest for all of us, not just at Microsoft but across the industry—is to continue to have what we call security by default. So that when people get a new computer, a new software program, all of the security settings are

on by default. They have what we call Security by Design, so that it is designed so that it's not only effective but easy for people to use and easy for people to know what is happening.

So we're focused on all of those things. I'll just say there's I think a lot more coming.

Mr. GONZALES. Thank you for that response. Trust is the name of the game, and we have to make sure that Americans continue to trust these different platforms that are out there. So thank you once again for testifying before the committee.

Chairman, I yield back.

Chairman GREEN. The gentleman yields. I now recognize Mr. Magaziner for 5 minutes of questioning.

Mr. MAGAZINER. Thank you, Chairman.

One of the joys of speaking in the order after our colleague from Georgia is that I'm often handed notes to correct incorrect statements that she made. So I just want to enter into the record that Microsoft's competitors were recused from the findings, the final report, and the recommendations of the CSRB-Microsoft investigation, just so that's in the record.

Now, Mr. Smith, the article that Mr. Thompson, Ranking Member Thompson referenced earlier had to do with the so-called SolarWinds breach, in which Russian hackers infiltrated Microsoft's cloud service and was able to gain access to some of our country's most sensitive secrets, including information from the National Nuclear Security Administration, which oversee our nuclear stockpiles, and the National Institutes of Health.

You provided testimony to the Senate Intelligence Committee in which you stated that the flaw that allowed that breach to occur only became known to cybersecurity professionals at Microsoft when it was published in a public paper in 2017.

It has now been widely reported that former employee Andrew Harris discovered the flaw a year earlier, alerted his superiors and other company executives, proposed a series of solutions that were rejected.

So can you now agree that the testimony that you offered to the Senate Intelligence Committee about what Microsoft knew about that flaw and when Microsoft knew it was incorrect?

Mr. SMITH. Well, look, the first thing I would say is I know that came out in an article this morning. I haven't had a chance to read the article yet. I was at the White House this morning.

Mr. MAGAZINER. OK. So if you can't say, all right. I'll just note that the article cited numerous sources inside the company, not just that one individual. But if you're not prepared to say that then we can move on.

Mr. SMITH. OK.

Mr. MAGAZINER. I agree with what Chairman Green said earlier about the importance of incentives. So I welcome the news that came out I believe yesterday that one-third of the individual performance element of bonuses for senior executives will be tied to cybersecurity performance.

How much of the total compensation package for senior executives is the individual performance element?

Mr. SMITH. It depends on the individual. It depends on the year.

Mr. MAGAZINER. Roughly.

Mr. SMITH. I'll say more than enough to get people's attention for sure.

Mr. MAGAZINER. But roughly, like ballpark?

Mr. SMITH. Of the cash portion? It's probably—I don't know. I will say about 15, 20 percent of. If you add stock, it's much lower.

Mr. MAGAZINER. All right. Well, if you could follow up on that, that would be helpful. Because, just to be clear, you know, a third of the individual performance element sounds good, but it depends on how big the individual performance is as a part of the whole. If it's 10 percent of the total compensation package, then the cybersecurity incentive would only be 3 percent of the total package and would potentially count less toward the total than revenue targets or profitability targets or other things.

On the other hand, if it was 60 percent of the whole, then that would be a much more meaningful incentive. So having some understanding of how large a percentage of the whole that individual performance element is would be instructive.

Mr. SMITH. Yes. You're making a good point. The one thing I would just add is, if there's one thing that's true at Microsoft and across the tech sector, people like to get good grades. This is one——

Mr. MAGAZINER. I'm sorry, I have limited time.

Mr. SMITH. Let me just say this is one part of their total grade.

Mr. MAGAZINER. I asked the question. If you don't have the information now, that's fine. I have a few more questions.

On that individual performance incentive, that portion of the compensation, is it restricted stock? Is it something that can be clawed back and, if so, do you know how far back the clawback can be exercised?

Mr. SMITH. Some of these details are still to be refined, but this is the bonus, the cash bonus that people get each year.

Mr. MAGAZINER. I would just suggest, you know, since it's still being refined, if it's a cash bonus then that suggests it would be difficult to claw back. A cybersecurity lapse may not become known until years after the fact. So I would suggest that perhaps some sort of a clawback mechanism could make the incentive more powerful.

Finally, piggybacking on the Chairman's question, the article that was published today stated, "Product managers at Microsoft"—product managers, not senior executives—"had little motivation to act fast, if at all, to address these security flaws since compensation was tied to the release of a new revenue-generating product and features," with one former employee stating, "You will get a promotion because you released the new shiny thing. You are not going to get a promotion because you fixed a bunch of security bugs."

So, given the importance of people at the product manager level, is there any plan for their compensation to be tied, at least in part, to meeting cybersecurity goals?

Mr. SMITH. One of the—the answer is yes. One of the decisions that was announced yesterday that I provided in my addendum is every single Microsoft employee as we get to the new fiscal year will have as part of their biannual review a mandatory part to talk about cybersecurity to do precisely what you just described.

Mr. MAGAZINER. If you'll indulge me for a second. So part of their review, but is there sort-of a portion of their compensation that's directly tied to the cyber portion, to the cyber factor, as will be the case with senior executives to some extent?

Mr. SMITH. It won't be as formulaic, but everybody knows that the bonuses, the compensation—we call them rewards—that you get at the end of the year are based on those reviews and how people do over the year.

Mr. MAGAZINER. I know I'm over, but I'll just say I want to state I do believe it is a positive and I think a good example that we are integrating cyber into compensation packages. I just want to make sure that we're doing it in a way that is really going to be impactful.

So I'll yield back.

Mr. SMITH. Thank you.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Garbarino for his 5 minutes of questioning.

Mr. GARBARINO. Thank you, Mr. Chairman.

Good to see you, Mr. Smith.

In its report, CSRB's overarching conclusion is that Microsoft security culture requires an overhaul, given its centrality in the technology ecosystem. I believe a lot of the recommendations that they've—they recommended you're already putting into place.

But the series of the findings of the CSRB report and the recommendations provided and now—and how the report was written, and now that we're all here having a hearing on it, how do you anticipate future voluntary cooperation with the board's request for information?

Because the CSRB, it's not in statute. They really have—they have—they have to go—they can only get the information that is provided to them by people who complied like your company.

What do you anticipate happening now in the future with other requests?

Mr. SMITH. Well, I guess the short answer is I don't know, but I hope 3 things will ensue: No. 1 is that people will remember that we collaborated and provided everything that the CSRB asked for; No. 2, that I came here today and we acted as a company with a real spirit I hope you'll see of humility, of accepting responsibility, of avoiding being defensive or defiant; and No. 3, and I hope that people will look back 6 and 12 months from now and say—and that you all hope others will do the same.

Because I think if you all can help us encourage that kind of spirit of responsibility, that's how we'll get better, because our—we know our adversaries are going to get better, so we have to find ways to get better too.

Mr. GARBARINO. I appreciate that and I do appreciate your being here and all the meetings that we've had and discussions. I know you've been working with CISA as well and the CSRB board.

You brought up Secure by Design in one of your last questions, and I've had a lot of conversations about that. I think my committee is actually going to have a hearing on Secure by Design.

Can you talk about what Microsoft is doing? Can you go into a little further about the Secure by Design?

Mr. SMITH. Yes. There's—Secure by Design actually connects with, you know, I would say several of the pillars of what we call our Secure Future Initiative. You know, we're focused on our engineering systems and our production systems.

Those really come together, in my view, to encourage our software developers to integrate security into the design of new products so that, as we say, it's baked in.

I think one of the key things that we've really sought to internalize is, as I've said here, to make security part of everybody's job and not just part of the work of the security team.

In hindsight, I think that's one of the mistakes, that we I think relied almost too much on the security experts and didn't do enough to ask everybody to make security part of their job.

So, you know, some of you have asked about this Recall feature. I think it's a great lesson. I mean, we're trying to apply it as a lesson learned. So if somebody is creating the Recall feature, they need to think about the security aspects of the Recall feature. It hasn't even been launched yet, so we've had the time to do this right, but it's—we're trying to focus on culture change.

Culture change requires constant role modelling and practice. So each time we go through this, we're talking very publicly so that everybody can see inside and outside Microsoft quite tangibly how people can weave this into the design decisions they're making.

Mr. GARBARINO. Well, I think Secure by Design is very important. You know, as we all know with cybersecurity, a lot of the intrusions come from end-user error, and you're only as strong as your weakest link.

So I think having more Secure by Design in these products is—having Secure by Design implemented would be great for everybody, every user of a Microsoft product or any product.

Just finally, you mentioned to—you know, you had the question, what should we invest in? You said, America, the people, you know, scholarships. You know, I think that's true. I know the Chairman is working on a piece of legislation that would do just that.

What is Microsoft doing on that end? I know we can do stuff. What is Microsoft doing to help with work force?

Mr. SMITH. Well, we've provided free curriculum, but more than that. We've provided free training to 203,000 Americans on cybersecurity over the last 4 years. We've provided 21,000 scholarships.

The thing I would leave with you all is, as you all may know if you work with community colleges, the students in these colleges are not well-to-do. They're usually trying to earn a living and go to college at the same time. If something goes wrong in their life, it can just throw them out of the ability to go to community college.

These don't have to be hugely expensive scholarships, but they are so impactful. I would really hope and ask and encourage you all. I know Mr. Magaziner is a sponsor on one of these bills. The Chairman, you're crafting these things. If you can make it a priority, it will help everybody.

Mr. GARBARINO. Thank you very much.

I know I'm a little over. I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Ivey for 5 minutes of questioning.

Mr. IVEY. Thank you, Mr. Chairman. I appreciate that.

Mr. Smith, thank you for being here today. We appreciate your presence.

I wanted to ask, this might be a little off the beaten path here, but about AI. The Representative from New York, Ms. Clarke, allowed me to join onto a bill of hers that goes into AI deepfakes and the like.

You know, we've got legislative efforts to fix these issues. Part of it might entail litigation and the like. But my sense of this is that, as a remedy, it just takes too long to implement it in a way to address one of these—on the radio the other day they were talking about middle school bullying is now using sexual deepfakes. Guys are putting up pictures of preteen girls in some instances with, you know—that are deeply psychologically damaging to them.

So since litigation and legislation, we have to make those adjustments to address the problem, but I mean, I think a bigger part of it is going to have to be technological. To address the AI aspect of it, it seems to me that we need an AI counter to that. I don't know what's coming along those lines, but I'd like to know if Microsoft or any—if you're aware of anything that's being developed that could help with that to address that issue in the very near future.

Mr. SMITH. Yes. I mean, first of all, I appreciate your focus on this. I was watching the hearing you all had a couple weeks ago on AI and you were raising it there, and I think that's a good thing.

First, I think we need to understand the problem. I think you've captured it well. We are seeing the creation of AI-based deepfakes in a way that can threaten candidates, all of you, to be honest, this year.

Mr. IVEY. We'll come to elections in a minute.

Mr. SMITH. OK. But as well as teenage girls, women, many others. So the solution is threefold: One, put in place more guardrails around our legitimate products so it's harder for people to use it for abusive purposes.

The second is use AI to——

Mr. IVEY. Give me an example of the guardrails.

Mr. SMITH. Basically, when we have products, we have some ourselves, Microsoft Designer. You build in an architecture. It has classifiers so that if someone is going to do something, you detect what they're doing and in certain cases you stop them from doing it.

So if they feed up—they try to take a photo of someone and remove their clothes, you say, no, that's not allowed. I mean, things about as straightforward as that. But, you know, there's a complex and I think very sophisticated architecture involved.

Second, AI is very good at detecting the use of AI to create images. It's always going to be a cat-and-mouse game, and you get debates among the technology experts. But I have a level of optimism myself about what I see our people in our AI for Good Lab doing to detect these problems.

Third, you've got to be able to respond. You've got to be able to use AI then to stop it or to take it off a platform. We do need good old-fashioned education so that people are aware, so that parents are aware of what their kids might be doing or the problems, the abuses their kids may be facing. Those—it's really multifaceted.

Mr. IVEY. Well, let's back up to No. 2, and that's detection, which I take it would be not so much you have to rely on the parents or even the individuals, the target, because it might be a while before they even become aware of the issue.

What sorts of detection mechanisms are on the near horizon that could be implemented?

Mr. SMITH. Well, we have detection mechanisms that we have in place today, and we're focused on specific problems in particular. If I could, one of them is elections.

Mr. IVEY. How widely available are they?

Mr. SMITH. Well, we are offering free training for every candidate for office in the United States. We've done this in 20 other countries. We have a website.

Mr. IVEY. Let me back up. I want to go back.

Mr. SMITH. OK.

Mr. IVEY. Because we're going to look out for ourselves at some point, because we have the ability to do that. I'm more worried about the deepfakes for especially, you know, teenage girls and the like. What's available for them?

Mr. SMITH. Probably not as much as we need is what I would say.

Mr. IVEY. OK. What steps can we take? How can we move that forward?

Mr. SMITH. I think we put in place guardrails. You're asking a good question. Let me take it back and let me ask our folks what could we create for more people that would empower them to do what every candidate can now do, namely report a deepfake about themselves.

Mr. IVEY. I appreciate that very, very much.

Last question: With respect to elections and misinformation, disinformation, especially the stuff that's coming out maybe even on election day or during that time period when elections have begun, is there a sufficient process in place that coordinates the private sector, the public sector, and potentially voters to address this concern?

I apologize to the Chair for running over.

Mr. SMITH. I'll just say I think a lot of progress has been made. As we get into the summer months in the two conventions, it's a really important question for all of us to have together in a way that is genuinely bipartisan.

You know, we're working with—there's a national association of State election directors. You know, we're working with them. We're working with them so that they can protect their infrastructure, that there are means to educate people about deepfakes and the like.

Frankly, what we're hoping can happen at both of the political conventions is some conversations about how we can enter the election season, say, that starts on Labor Day, you know, with all the protections that we're going to need.

We're basing that on a lot of work. We were in Taiwan for that election. We've been in Europe for the spring. We'll be in the United Kingdom, in France. We're trying to take everything we learn each step of the way and apply it.

Mr. IVEY. Thank you for your answer. I look forward to hearing back from you.

Mr. Chairman, I appreciate your indulgence.

Chairman GREEN. Absolutely. The gentleman yields, and I now recognize the gentleman from Mississippi, Mr. Ezell.

Mr. EZELL. Thank you, Mr. Chairman. Thank you, Mr. Smith, for being here. Thank you for holding this hearing today.

The Federal Government and many Americans trust Microsoft to protect our critical cybersecurity infrastructure. Unfortunately, we're here today because Microsoft has fallen short in some of these areas. I'm especially worried about our national security.

A recent report to Congress from the U.S.-China Economic and Security Review Commission linked multiple cyber attacks to the CCP. Your report directly calls out breaches of Microsoft's email servers at the U.S. Department of State and the Department of Commerce.

Of course, the CSRB report in greater detail describes Microsoft's cultural issues related to security, which we have highlighted.

Mr. Smith, with the CCP and the Russian Federation backing state-sponsored cyber attackers, all organizations face this threat, regardless of their resources or reputation.

Breaches are inevitable, and I acknowledge the Federal Government has a role that we've got to play here. However, despite being known as a leader in defending against attacks, it appears that Microsoft has had some failures which could have been avoidable, and I know you've addressed this. But I want to discuss the company's other investments, specifically its AI offerings and how it can relate to your plan to improve its cyber capabilities.

I'll start by asking you, do you believe that as AI becomes integrated into more products and services, the potential for attacks increases?

Mr. SMITH. I think we'll see two things almost inevitably, and perhaps we soon or already are. One is our adversaries will use AI to try to pursue more sophisticated attacks; but, second, we are already using AI to strengthen security defenses.

I have to say I'm very optimistic about what AI can and already is being used to do to strengthen cybersecurity protection in two ways: No. 1, AI is especially good at detecting anomalies in data, looking for patterns. We have threat-hunting teams at Microsoft. We probably have more threat-hunting teams than anybody else. But seeing what people can do when they have AI to help them detect these patterns, that is key, and that's going to be important across the industry.

The second is to help the chief information security officers, the CISOs, the cybersecurity professionals across the country. So, you know, we've got a product, a cybersecurity Copilot. Others will have similar things. It basically takes a lot of work that these folks have to do, and it helps them do it faster. It helps them do it better. I think that that's going to be a good step as well.

Go back to this gap, the 400,000 open jobs. Hopefully, what AI will do is, in effect, lower the barrier to entry, because an individual who wants to join this profession—and I hope more people will—they'll say, hey, I don't have to learn everything I might have had to learn 5 years ago, because now I have an AI tool that will

help me as well. I think we're going—we're seeing that now. We're going to see it accelerate in the next couple years.

Mr. EZELL. Thank you. What specific cybersecurity measures is Microsoft implementing to protect the additional surface for attacks? What are you doing additionally to protect?

Mr. SMITH. Your question goes to detection.

Mr. EZELL. Yes.

Mr. SMITH. That's a critical piece, and it's 1 of the 6 pillars that we have in the Secure Future Initiative that I mentioned.

I will tell you, we have—I'm very proud of the teams we have, great people who are just so committed to the mission. But it sort-of goes back to then using more technology and more AI so we can make them more effective. We get so much data that we've got to be—basically integrate all of the data that we have so it's more usable by our threat hunters, and then we need to use AI to make it easier for our threat hunters to find things faster.

So I think this cutting of silos, you know, connecting what we call data graphs using AI, I think it's going to make our people—I think every company that does this, you know, will find that it can get better with these approaches.

Mr. EZELL. Quickly, one of the things I'd like to follow up with what Mr. Ivey was saying. He was talking about some of these generated photographs. As a local county sheriff, many times we had parents that would come in, and their teenage daughter had been victimized. We basically had nowhere to go to investigate, to follow up, to catch some of these bad actors that are doing this thing.

I would ask you, as part of your training, to infiltrate these local sheriffs and police officers, especially in the rural areas that have limited opportunities to have the use of some of the things that we've described, we talked about today, because it breaks my heart to see a child go through that when it's been a totally false accusation and then for them to go back to school.

So I would really encourage you to put that on the front burner so that we could help our local law enforcement to try to stop some of this.

Mr. SMITH. I would just say—and I know our time is out—but yes, we will. You're right in two fundamental ways. First, I appreciate it. I mean, some of the most moving things that I've seen over the years have been information from police officers, local law enforcement who are working to protect kids who are being victimized in the way you just described.

Second, the other group I should have mentioned when Mr. Ivey asked is the National Center for Missing and Exploited Children, NCMEC. These are, in my view, real heroes for all of us. We all work together and support them and rely on them.

I think this is this—this great alliance we have in this country between law enforcement, NCMEC, and then tech companies, and it's—and our competitors are part of this. This is one area where I think the industry is pretty united, and the world is better for it.

Chairman GREEN. The gentleman yields.

I now recognize Mrs. Ramirez for 5 minutes of questioning.

Mrs. RAMIREZ. Thank you, Chairman.

Good afternoon, Mr. Smith. I'm freezing here, but I think you might be a little warmer. You've been a little more active.

So—and I've been hearing our conversation today in the hearing. For us, it's pretty clear we have two Homeland Security threats that this hearing is really trying to take up. One of those is cybersecurity attacks, and the other is concerning tech monopolies and monocultures driven by profit, sometimes supremacy and secrecy, and I feel like both are existential threats to the health and well-being of our democracy.

When incidents like the 2023 Microsoft Exchange breach happened and the bombshell damning reports like what was published by *ProPublica* today, they bring us to this reckoning moment, and it's not just for Microsoft.

But that we've been entrusting with our Nation's most sensitive information, and also for this committee this desperate need for the pursuit of accountability when our Nation's homeland security has been compromised.

The Ranking Member mentioned that the *ProPublica* article published earlier today described how Microsoft had dismissed an employee's concerns about a vulnerability in Active Directory that was eventually leveraged by the Russians during SolarWinds. Then Microsoft denied that any vulnerabilities in its systems had contributed to the attack.

So when my colleague Congressman Correa asked you earlier how quickly you address vulnerabilities, you said immediately. But *ProPublica* reported today that an employee alerted Microsoft to the Golden SAML, the SAML vulnerability years before the SolarWinds.

So I guess my question to you, Mr. Smith, is, what is your definition of immediately?

Mr. SMITH. It's right away. Let me just say—and look, this is the classic let's have an article published the morning of a hearing so we can spend the hearing talking about it, and then by a week from now I'll actually have a chance to go back and learn about everything in it.

I am generally familiar with that situation. Let's remember a couple of things. One, that SolarWinds intrusion was by the Russian government into a SolarWinds Orion product, not a Microsoft product.

That Orion product was distributed to more than 30,000 customers. Microsoft was one. Because of what the Russians had done to change the software code of the Orion product, the Russians immediately had an entry point into all of these networks.

Let's also remember that when FireEye brought us in, that was the beginning. This was I think in November 2020. We worked with FireEye, and we came up with a technology tool that in effect blasted that entry point, if you will——

Mrs. RAMIREZ. Mr. Smith, I have a short time. So actually, you might have a little opportunity to talk more about that here. Because yes, Microsoft expanded the Secure Future Initiative and has said that security teams will have an elevated role in the product development.

Maybe, tell me how the employees' concerns that were expressed about a vulnerability in Active Directory would have been handled differently today.

Mr. SMITH. Well, I would say 2 things. First, I would hope that if there is an issue that needs to be addressed, it will be woven into our engineering processes. It will be escalated. It will be decided. People will be evaluated based on how they did.

Second, though, I would like to go back for 1 second on this so-called Active Directory. What we're really talking about here is what was called SAML. It was an industry standard, and it was a security vulnerability in the entire industry standard. What ensued was a conversation across the industry about the best way to address it.

I think this is where, like I said, a week from now I'll bet we can pull together information and have a much more informed conversation about this, and I would welcome that opportunity.

But I think what's most important for today is simply to note how we are changing our engineering processes, how we are integrating Security by Design, how we are changing the way employees review themselves, how we elevate these issues and reward people for finding, reporting, and helping to fix problems.

Mrs. RAMIREZ. Good, good. So I have a few seconds, and so a few sentences. I'm going to shift gears for a second.

How do you ensure that your bundling practices do not limit the ability of customers to prioritize security in their purchasing decisions?

Mr. SMITH. I'm sorry, I couldn't hear that.

Mrs. RAMIREZ. Let me do that again if I can get a few seconds more, Chairman.

How do you ensure that your bundling practices, when—in your bundling practice that you don't limit the ability of your customers to be able to prioritize security in their purchasing decisions? So when they're purchasing that you're not—that they're able to prioritize their security when you're providing these bundling practices.

Mr. SMITH. Let me just say I don't—I'm not aware of any so-called bundling practices that limit what our customers can do in terms of cybersecurity protection.

If you look at the market for cybersecurity protection, frankly, a very robust part of it is about providing tools and services to enable customers to manage the security of their networks when they have solutions that come from so many different vendors.

Microsoft accounts for about 3 percent of the Federal IT budget. What that tells you is that there's 97 percent that's being spent elsewhere. That's pretty typical when you look at it.

So a lot of what we're doing across the industry, I think, especially with industry standards and the like, is to enable I think the kinds of customer choices that I think you quite rightly are encouraging.

Mrs. RAMIREZ. Well, thank you, Mr. Smith. I ran out of time. If we get another round, I'll ask you a follow-up. Thank you.

Chairman GREEN. That would be best. One quick note: If you're like 2 seconds from your time limit, guys, that's not the time to start a new question, right? So you know I give a lot of grace. I

give a lot of grace. But if you're, you know, in a process and all that, we're going to let that question continue on and we'll give you a little extra time for that.

So—and you are—Mrs. Ramirez, Mr. Ezell was just as bad. He literally had 2 seconds left when he started that new—so I now recognize Mr. D'Esposito for 5 minutes of questioning.

Mr. D'ESPOSITO. Well, thank you, Mr. Chairman.

Mr. Smith, the CSRB report stated that Storm–0558 had access to some of these cloud-based mailboxes for at least 6 weeks. Can you tell us who discovered that the system had been compromised and how they did so?

Mr. SMITH. Well, I think Ranking Member Thompson identified this early on in the hearing that, in fact, I think we got a notification from the State Department that they had seen an anomaly in their email system. So they informed us of this last June. Our initial reaction was that this was something that was a token that was being generated through a stolen key at the State Department or in the Government. I remember 7:30 in the morning I was notified about this on a Saturday morning. I was on the phone with Satya Nadella, our CEO, probably within 30 to 60 minutes, but we thought it was confined to that. It took somewhere between a few days to a week or more for us to come to the conclusion that it was broader than that.

Mr. D'ESPOSITO. OK. I obviously—do you believe that Microsoft should have been able to realize that you were compromised before the State Department?

Mr. SMITH. You always want to be the first in life in everything.

Mr. D'ESPOSITO. Well, that depends.

Mr. SMITH. Well, yes, that's true. That's a very good qualification. You always want to be the first to do everything good in life. So I have to, on the one hand, say yes. But on the other hand, I have to say especially given the nature of networks and how they are distributed and different people see different things. Mostly I just want to celebrate the fact that people are finding different things and we're sharing them with each other.

Mr. D'ESPOSITO. OK. So putting the celebration aside, are you confident that moving forward Microsoft has the ability to quickly detect and react to an intrusion like this?

Mr. SMITH. Well, I will tell you, I feel very confident that we have the strongest threat detection system that you're going to find in quite possibly any organization, private or public, on the planet. Will that always mean that we will be the first to find everything? Well, no, that doesn't work that way. But I feel very good about what we have and I feel very confident about what we're building.

Mr. D'ESPOSITO. Now obviously Microsoft is seeing a lot of what these cyber criminals and nation-state actors are doing to the ecosphere. How do you go about sharing information that you collect or identify with law enforcement?

Mr. SMITH. We have a variety of different steps we take, some of which are probably not best talked about in a public hearing that, as the Chairman said, is probably being watched in Beijing and Moscow. But we collaborate with the FBI, we collaborate with local law enforcement all the time. We collaborate, both with the

different agencies of the U.S. Government and other governments that are allies of the United States.

Mr. D'ESPOSITO. OK. I know that many of our staffs use Microsoft for their email amongst many other applications. Can you give us an idea as to the size of the share of Government contracts for networking, cybersecurity, and other matters in this space that Microsoft has?

Mr. SMITH. I don't know the precise number for that precise definition. I know, as I was mentioning, that we account for about 3 percent of the Federal IT budget. I know that the U.S. Government has many choices when it comes to cybersecurity services and I think it takes advantages of them and we're one of them. I don't frankly know how we compare to some of the others.

Mr. D'ESPOSITO. Obviously like you said, the Government has many choices. So with that said, why should they continue to use Microsoft?

Mr. SMITH. Because we are going to work harder than anybody else to earn the trust of our Government and other allied governments every day. We're making the changes that we need to make. We are learning the lessons that need to be learned. We are holding ourselves accountable. We will be transparent. I hope the people will then look at what we've done and say, This is something that they want to do with us. But I know we have to earn their trust every day.

Mr. D'ESPOSITO. Mr. Chairman, I'm following the rules, with that, I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Menendez for 5 minutes of questioning.

Mr. MENENDEZ. Thank you, Mr. Chair. Thank you, Mr. Smith, for appearing here today.

In 2002, Bill Gates issued a memo to Microsoft employees which stated, and I quote, flaws in a single Microsoft product service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company. So now, when we face a choice between adding features or resolving security issues, we need to choose security.

Two-thousand-two, last month Microsoft's chairman and CEO in a blog post to Microsoft employees stated that if you're faced with a trade-off between security and another priority, your answer is clear, do security.

Two-thousand-twenty-four, does last month's directive indicate that Microsoft had drifted from the security first culture set forth in Mr. Gates 2002 memo?

Mr. SMITH. You know, I was there in 2002 when Bill Gates was the CEO of the company and have been there every year since. You know, this is, you know, something I think one just has to be introspective about, because I've been in so many meetings every year where we've done so much to talk about where we are when it comes to security. I think that the biggest mistake we made was not the one that is being described that way. I think the biggest mistake we made——

Mr. MENENDEZ. What do you mean, described that way?

Mr. SMITH. Of drifting away from a security-first culture.

I think the biggest mistake——

Mr. MENENDEZ. I'm not asking if there is a biggest mistake, I am just asking if you do believe if there was a style drift at Microsoft between 2002 to 2024?

Mr. SMITH. No, but let me say what I think, perhaps, happened. As we hired so many cybersecurity experts, it became possible for people who were not in the cybersecurity teams to think that they could rely on those people alone to do a job that we all needed to do together. See, in 2002, we didn't have all these large security teams. Cybersecurity didn't exist at that time the way it does today. So I think there's a profound lesson.

Mr. MENENDEZ. I understand, I understand that the makeup of Microsoft and the different departments may have changed, but this was a statement in 2002 about choosing security first. Then, more or less, the same statement made in 2024. That to me would at least indicate that perhaps there was a sign that security first had maybe taken a backseat potentially.

It would be helpful if you could just describe to me and the committee the Microsoft Security Response Center and how it sits within Microsoft's corporate structure.

Mr. SMITH. The Microsoft Security Response Center, or MSRC as we call it, reports up to, as I recall, our executive vice president for security, a fellow named Charlie Bell who is on our senior leadership team and it is part of a very large, and, I think, robust security organization.

Mr. MENENDEZ. Who makes determinations when something is raised to the Security Response Center as to whether they elevate it up to folks?

Mr. SMITH. I would have to go get the precise answer to that precise question. I will say this: We do try to, and frankly, we need to create an environment where bad news travels fast. That's what we aspire to do. I can definitely tell you, I can tell you in the case of Storm–558 or this Midnight Blizzard we're talking minutes to hours gets to me. I'm usually the last stop before it gets to our CEO, Satya Nadella, and the time from me to him is in minutes, and it's not a large number of minutes.

Mr. MENENDEZ. Great, appreciate that.

The CSRB described various approaches, cloud service providers used to manage and secure identity and authentication systems. There were particular changes they made following Operation Aurora in 2010, I'm glad that Microsoft agreed to transform how it manages and secures its identity systems.

I would like to unpack that a little. Does Microsoft plan to make significant changes to the architecture of its core digital identity systems?

Mr. SMITH. I think the answer is yes.

Mr. MENENDEZ. I'll be quick with this, Chairman. As part of a review, the CSRB issued numerous recommendations for cloud service providers generally in certain Federal agencies. The CSRB also issued 4 recommendations specific to Microsoft. Microsoft updated its secure future initiatives subsequent to the CSRB's report. I would like to discuss how Microsoft plans to implement a couple of those Microsoft specific recommendations.

The CSRB recommended that Microsoft share publicly a plan with specific deadlines for security-based reforms. Does Microsoft

plan to implement the CSRB's recommendation and publicly release deadlines for implementation?

Mr. SMITH. The answer is yes. In fact, of the one things that I mentioned in my written testimony is we have invited CISA to send a team out to our headquarters outside of Seattle in Redmond. Go through all the details of everything that we're doing. We want to show them all of the details. Then, I think, one of the things we'll need to, you know, frankly assess together with CISA is how much or what altitude we should be publishing things, because if we publish them the good news is every American can read them, the bad news is everyone in Moscow can as well. Then I'll just say we recognize the oversight role that you and this committee plays, so, you know, we're interested, happy to share more with you than, of course, we would share with the general public. We just need to do it in a secure way.

Mr. MENENDEZ. I appreciate it. Thank you so much for appearing here today. I look forward to working with you.

Chairman GREEN. We'll have staff look at your microphone. We don't want that to happen to you again.

You get another 5 minutes? Good try.

The Chair now recognizes the gentlelady from Florida, Ms. Lee, for 5 minutes of questions.

Ms. LEE. Good afternoon, Mr. Smith.

Mr. SMITH. Good afternoon.

Ms. LEE. I'd like to follow up on one of the lines of questions from Mr. Menendez. You've testified today that in the wake of the CSRB report that Microsoft is committed to prioritizing security first over product and feature development. That is something that is easy to say and no doubt very difficult to do with far-reaching implications for your company. So, I'd like to hear a little bit more about the specifics, whether you are standing down on product development while you refactor code base, or what other specific ways in which you are throttling or pausing feature release or product release to ensure a focus on the security first as you described.

Mr. SMITH. It's a really good question. I would answer it in 2 parts. First, in the short term, yes, we have reallocated resources. We've moved people, we've told them to reprioritize. By definition, that means that other things may have slowed down or stopped so this can speed up, and that's the right thing to do. I think the real challenge is how you achieve effective, lasting culture change. You know, this is true in any organization, and especially when you have a company like ours. We have 225,924 employees. This has to be real and reach every one of them.

We're calling on a lot of what we learned as a company over the last decade. We have gone through a lot of culture change. I think people feel it has benefited us well. I think you define a North Star which is this notion of "do security first." You then have to change your accountability mechanisms, and that's why compensation is so important. But fundamentally, what we're really gravitating toward is to treat security as the highest priority and quality.

Ms. LEE. So would it be correct to say then that you have reallocated people and resources in furtherance of that objective?

Mr. SMITH. Yes.

Ms. LEE. Has it also affected your revenue projections, I would think?

Mr. SMITH. I would say so far, I'm not aware of it changing any of our revenue projections. Let me just put it this way: I was in Stockholm last Monday, you know, this is a country that as you know has just joined NATO. I met with about 25 customers, Government customers, corporate customers. What I found was really interesting. They asked a lot of tough questions, as you all are, bad news for the folks who want to sell plan B; they don't want to switch, they want us to get it right. We have to get it right to deserve their business. But I think they see that we really are committed to doing that.

Ms. LEE. I know it's come up a couple of times today, but I would like to return to a discussion of the recently-released Recall feature. You mentioned security by default, but that endeavor is something that, if I understand correctly, presented a security exposure of users who might not have understood the nature of how it operated.

So I'd like to hear more about how the status of that product rollout, and how it is consistent with the security-first approach, and what's being done to make sure users are aware of the potential exposures or risks from using it.

Mr. SMITH. Yes, I think I would start with, this product hasn't yet been launched. The feature hasn't yet been finished. We have had a process to share information and take lots of feedback. We've defined—we have designed it so it's off by default, so that people have to choose to turn it on and we can share information with them before they make that decision. We've designed the feature so that the information always stays on one's own PC. It doesn't go to Microsoft, it doesn't go anywhere else.

We've combined it with a hardening of the security in Windows for every part of the computer, and not just this feature alone. Then, we have added additional features that encrypt data, and decrypt it just in time. So we are trying to take a very comprehensive approach to addressing all of the security and privacy issues as well. We're trying to do it in a dialog, because when you do create technology. I think one of the mistakes you can make is to think that you have all the answers. You only get to the best answers when you have these kinds of collective and public conversations.

Ms. LEE. So in an attempt to comply with the Chairman's guidance, I will touch on my last question, which is a bit of a shift in gears, and that is, I would like to hear more about one of the things that I was identified in the report is an area in need of improvement was victim notifications. So, I would like for you to elaborate a little bit more on your thoughts and going-forward plan on how to improve victim notification.

Mr. SMITH. Let me try briefly to address this, because this is a really important topic, and it's a hard one for us and everybody. When we find that someone has been a victim of an attack, it doesn't mean that the fault was ours, it is just that our threat detection system may have found it. We need to let them know. Well, how do you let somebody know? If it is an enterprise, we probably have a connection. There's probably somebody there we can call.

But if it's a consumer, like a consumer-based email system, we don't necessarily know who the human is, we just have an email address. So we send an email. There was a Member of Congress we sent an email to last year, a Member of Congress did what you sort-of expect, he said, Well, that's not really Microsoft is it? It's spam. Then we called somebody. Believe me, we have called people and they say, Oh, give me a break, you're not Microsoft, you're just one more fraud enterprise.

That is the world in which we live. So the CSRB report has a great recommendation on this, it's to create the equivalent of the Amber Alert, but it will require support from Congress that to see that CISA lead this, that the tech sector, and probably the telecommunications companies and the phone makers and the phone operating system makers all come together. This will be a huge step forward.

Chairman GREEN. The gentlelady yields.

I now recognize Mr. Suozzi for his 5 minutes of testimony.

Mr. SUOZZI. Thank you, Mr. Chairman. I want to thank you and the Ranking Member for holding this hearing. Holding Microsoft accountable is a good idea. I think that Mr. Smith has demonstrated he's taken his father's advice. I think you said it was your father who said no one ever died by using humility.

Mr. SMITH. I don't know if he said it, but he definitely—he's still alive today. He is probably watching this, for gosh's sakes. It was definitely something he taught me.

Mr. SUOZZI. He would've definitely taken accountability here today and we appreciate that. Let me just ask what percentage of Microsoft's business comes from governments?

Mr. SMITH. If I had to guess, it's less than 10 percent globally.

Mr. SUOZZI. So what percent of it is just from the Federal Government itself?

Mr. SMITH. Not that much. We love the Federal Government. It is a big customer, it is one of our biggest and it is the one that we are the most devoted to, but it is not the biggest source of our revenue——

Mr. SUOZZI. So you mentioned earlier that there are 300 million cyber attacks a day. Are the sources from state-sponsored adversaries of ours like China, Russia, Iran, and Korea, is it from organized crime or is it from individuals who are doing this?

Mr. SMITH. I would say most of it comes either from those 4 nation-states, or ransomware operators. We track over 300 organizations, and, you know, those 300 account for by far the highest percentage.

Mr. SUOZZI. Can you give a percentage for how much is from state actors versus the ransomware people? Are the state actors sometimes ransomware activists also?

Mr. SMITH. I can't, I'm forgetting off the top of my head, but we can easily get that to you. I will say, in addition to being a substantial percentage they are, by far, the most sophisticated and serious.

Mr. SUOZZI. So my big concern for our country is how divided we are. Our country is divided because of our Members of Congress, there are 435 us, 380 of us are in safe seats so they don't have to worry about the people per se, they only have to worry about the people in primaries, so they pander to their base, and that divides

us. Then social media, the people who get the most attention on social media are the people who say the most extreme things. Then cable news, you know, Tucker Carlson was the most-followed person on FOX before he left; Rachel Maddow. They've got 4 million viewers, 3 million viewers. They are kind-of playing to the extremes. But our foreign adversaries, Chinese Communist Party, Russia, Iran, and North Korea, are taking disinformation and trying to divide us every day by taking messages that we're fighting about already, and blowing them up bigger than ever.

We need the great corporate citizen, Microsoft, and other great corporate citizens, to team up with the people of the United States of America and their governments to figure out how we're going to stop this attack, because they are trying to destroy us from within by dividing us using technology and disinformation and cybersecurity attacks on a regular basis to destroy us.

So what can we do to team up more effectively? What other partners, other than the U.S. Government and Microsoft, should we try and bring into this partnership to try and save our country from this division that is being exacerbated by our foreign adversaries?

Mr. SMITH. Well, there's lots of great companies in our industry that are doing great things in all areas of the industry. The good news is especially there is this extraordinary CISO, chief information security officer community where people work together across industry boundaries.

Mr. SUOZZI. Well, we need to advise the public about what's happening.

Mr. SMITH. Exactly. I think we need processes to do that. I would say at the end of the day, look, I think the point you just made is maybe the most important point that could be made at this hearing, because the greatest threat to this country in this space comes if our adversaries coordinate and unite and we should assume that they not only can, but they will.

Mr. SUOZZI. They are.

Mr. SMITH. The greatest weakness of this country is that we're divided. Not just politically, but in the industry as well. We just always have to remember that if we can find a way to summon the ability to work together you all, if you can work together across the aisle, and we in our industry can work across the industry and then we unite together with new processes that are probably Government-sponsored, and some of them exist, including through CISA, so we can do what you just described and among other things help people learn. Also, take the steps to hold these adversaries accountable so we can start to change what they are doing.

Mr. SUOZZI. Thank you, Mr. Smith.

Mr. Chairman, I would like to participate in an effort by this committee, bipartisan in some way, working with industry to come together as a team to figure out what we can do as a country to identify these threats, notify the public as to what's happening to them on a regular basis, and how we as a country, corporate public partnership, can unite to fight against our foreign adversaries that are trying to destroy our country.

Thank you, Mr. Smith.

Ms. LEE [presiding]. The gentleman yields back. Thank you, Mr. Suozzi.

The gentleman from Texas is recognized for 5 minutes.

Mr. LUTTRELL. Thank you, Madam Chairman.

Good afternoon, Mr. Smith. Let's just chat a bit 5, 10 years downstream. Microsoft secures the network from nefarious to bad actors globally. What is the—and I won't say end game, because I don't ever think there is going to be a finish line when it comes to artificial intelligence and machine learning or the cyber space. What is Microsoft doing, you know, in kill chain results from this little guy right here, but—maybe there's nothing we can do to stop the amount of actors that attack us every single day. But we may not be able to talk about it in open setting, but is there an end game? Is there a way to secure the network where bad actors cannot have these breaches?

Mr. SMITH. I would say two things: First, if you look at the current course and speed, this is probably, for the time being, and until the geopolitical environment in the world changes, a bit of a forever war in cyber space with constant combat. I would hope that that would change, but we can't assume that it will. So what can we collectively change? Well, first at Microsoft, I would not just hope, but fundamentally believe, that, say, 5 years from now, we're going to have production systems, engineering systems, networking, identity systems that make it extraordinarily difficult and just beyond the economic reach of our most sophisticated and well-resourced adversaries to attack and breach.

Mr. LUTTRELL. Is that moving the infrastructure completely to a cloud-based system?

Mr. SMITH. I do believe it is. I do think that the cloud is part of the answer, just not only for us, but for the other companies who are in the cloud services business. I think that, you know, in addition to what we do as a company, I would hope, just as we learned from our competitors and that's a good thing, that we'll share what we're learning, and our competitors will adapt as well.

I think the thing we're going to go have to do the most to internalize is just recognize that we'll do a lot of good things. Let's say we do every single thing that the CSRB has recommended because that's what we are going to do, it won't be enough, because 2 years from now, our adversaries will have done more. So what we need to create is a process where we collectively always learn from what is happening. We do a better job of anticipating and predicting. I do think that AI will be one of the great game-changers and we need to ensure that AI benefits the United States and our allies and the defense of people at a faster rate than it could be used by our foes to attack them.

Mr. LUTTRELL. Inevitably, that is going to be the human variable that is removed from the cybersecurity space, and that will be completely AI-based. Is that a fair statement?

Mr. SMITH. I'm very——

Mr. LUTTRELL. There is a word out there I'm looking for, but I don't have it. Computation-based, I'm sorry, no, the computer systems are going to be the ones that are going to be running forward with this, which they already do.

Mr. SMITH. Let me just say that I am optimistic about what AI can do to strengthen cybersecurity defenses. But I think sometimes

people in the world of technology actually run the risk of underestimating the power of people. What we should really bet on——

Mr. LUTTRELL. Let me say as a Congressional Member, I would never do that. I want everybody to know that.

Mr. SMITH. What we should bet on and what we should pursue as a country, and as an industry, is the opportunity to enable people to stand on the shoulders of better technology. If we can do that with AI, if that's the stronger foundation, we will enable our people, especially in this profession, to achieve so much more. We know that in Moscow and other places, they'll be trying to do the same thing. We've just got to do it better, and we've got to do it faster and we can never take a day off, because that's the reality.

Mr. LUTTRELL. OK, thank you.

Mr. Chairman, I yield back.

Chairman GREEN [presiding]. The gentleman yields. I now recognize Mr. Garcia for 5 minutes of questioning.

Mr. GARCIA. Thank you, Mr. Chairman.

I want to thank everybody, sir, I had a chance to be here for the first half of this hearing, and I rushed to the floor and rushed back. So thank you for answering all of our questions.

I want to just take one step back and kind-of absorb some of what I heard in first half as well. I mean, I clearly—think you understand I appreciate you taking responsibility for the security failures and concerns I think all of us have. I think that's important. I also want to broadly think Microsoft and so many other companies have done incredible work to change the lives of Americans.

Obviously, as someone that really believed in the power of technology, an incredible economic driver that you are to my State in California and other places, I don't want to sweep that part under the rug as well. So I thank you for continuing to work. This is an important serious topic that we're discussing today.

Every company, every government faces serious threats from hackers, from foreign intelligence services. We all know that, that's been established. Russia and China and other countries are trying to steal secrets, steal technology, steal patents, and it's not just within your company, but some companies, of course, across all of our Nation. It is important that we are here on a bipartisan basis. I also want to note that this—the report that we are reviewing today is a report from CISA.

I want to encourage us to support CISA as an organization. There have been some of my colleagues have wanted to abolish CISA, they wanted to reduce support for strengthening cybersecurity in our country. I think that would be a huge mistake. So, I would encourage us to continue to work with CISA and other agencies to make our systems more secure.

I also want to just note, that I believe—is that we need more Federal intervention and partnerships, not less or with Microsoft and other technology companies. It's important that we continue to work. Before I got here, I was the mayor of Long Beach, California and I—for 8 years and I consistently remember the numerous attacks that we got, the cyber attacks we would receive from a city perspective. The challenges for municipalities and governments and smaller governments that are not the Federal Government to deal with those effectively.

So, I encourage you to continue to work not just at the Federal level, but there are so many small cities and towns that don't have the capacity to actually deal with some of these cyber threats that we have.

I also just want to have an initial question, you answered it probably earlier. We know there are an extraordinary number of cyber attacks from nation-state actors, we talked about those today. You want to boil that down? What do you attribute these direct attacks? Why are they attacking Microsoft systems?

Mr. SMITH. Let me just first thank you for your comments. I do want to underscore so it's clear if there's any doubt, we support CISA as well, I support CISA. There's always debates about exactly one piece or another, but it is really doing important and good work for the country.

I think it's really important to look at the motivations of nation-state actors as well as criminal enterprises and just understand what they are doing. I would say over the last year we've seen on the nation-state side, broadly speaking, three kinds of motivations: One is access to information, surveillance, including of other governments, but not governments alone. So, of course, they go to where the information is located which does include our cloud services.

The second, and I think this is extraordinarily disconcerting, is we've seen, from China in particular, this prepositioning of so-called web shells, think of it as tunnels into our water system, our electrical grid, into the air traffic control system. The kind of thing that you look at and you say this is only useful for one thing, and they have it in place of a war or hostilities.

The third thing that you see from nation-states is something that is very unique to North Korea, they have a very different approach to budgeting, they let ministries employ hackers and the ministries work to steal money and then the ministries get to keep the money that they get. It is an oddity, that's the nation-state side. Think about——

Mr. GARCIA. Briefly sir, because I want to ask one more question with my remaining time, but continue.

Mr. SMITH. On ransomware, it is all about making money unfortunately.

Mr. GARCIA. No, I appreciate that. I just want to take a moment to also commend the State Department security operations, they have been involved with you and a lot of other organizations. Their infrastructure, which needs to be strengthened, does a lot of this work, and so, I want to uplift them as well.

Last, I wanted to mention in the CSRB report there was a recommendation to create some type of Amber Alert system, some kind of notification system. We're all concerned about the cybersecurity threats. Does Microsoft support this recommendation? Can you expand a little bit on that?

Mr. SMITH. Yes, and I was talking about this a little bit when you had to leave. I think it could be extraordinarily helpful for our entire industry, for everybody who uses technology, for consumers in particular. I hope that we will find a way to work together to make it a reality.

Mr. GARCIA. Well, thank you. I yield back.

Chairman GREEN. The gentleman yields. I now recognize Mr. Strong for 5 minutes of questioning.

Mr. STRONG. Mr. Smith, I appreciate you being here today. Most of all, I appreciate your humbleness. We've had people sit right before this committee, Cabinet members tell us that the Southern Border, they've got it under control and 3 years later, 3½ years later they sit right there and tell us more than 10 million people have illegally crossed that Southern Border, so you've served Microsoft well today and I appreciate how you've presented yourself.

As you may know, I also serve on the House Armed Services Committee, and specifically the Cyber, Information Technologies, and Innovation Subcommittee. I'm aware of the DOD's cyber challenges and needs.

The recent cyber attacks impacting Microsoft demonstrate how vulnerabilities within a single vendor can be exploited to gain access to sensitive information and systems, potentially compromising national security. Can you please explain, from your perspective, the risk posed by the DOD's reliance on a single-source vendor?

Mr. SMITH. Well, I guess the first thing I would say is I don't see the DOD moving to rely on anybody as a single source in the technology space. There's a lot of competition that's alive and well at the DOD. I think that's a good thing. Then the other thing I would say is just as there is risk on—in relying on one vendor, there's risks in relying on multiple vendors. I would still rely on multiple. So I don't want anybody to be thinking I'm saying something I'm not. But when you have—what we call a heterogeneous environment, meaning technology from lots of different suppliers, you create a lot of different seams. So then you need to have technology and people who can knit it all together. Then the thing we should remember is that a lot of what, say, the SVR, the Russian foreign intelligence agency does, or the GRU, they are military, they look for the seams, because those are the places that are easiest for them to get in. So fundamentally, whether you have one vendor or several, the challenge is similar. We all need to work together and just keep making progress.

Mr. STRONG. Thank you. Would you agree that the vendor responsible for developing and running hardware and software programs for the DOD should not be the same vendor responsible for testing security, conducting security audits, or reporting on security?

Mr. SMITH. I'd want to think a little bit about the precise formulation of your question, it's a very good one. Mostly what I would say is, I think it's well-thought out to focus on testing of solutions and how you have—it's almost a first principle in governance I would say as somebody who is responsible for a lot of governance at Microsoft. You want checks and balances. If one group is performing, you want a separate group to be auditing and assessing. I think that's true in a company, it is maybe even more necessary in a government.

Mr. STRONG. I agree. My friend from New York briefly touched on this, specifically what are the security implications of China and other potential threat actors having access into your network for so

long? What is the threat of that? You know, thank goodness it was discovered, but what is the threat do you see for them being in your system for so long without being noticed?

Mr. SMITH. Yes, I would just like to qualify a little bit of premise, because I noticed in some of the questions that were floating around this week, that people suggested that because the Chinese had acquired this key in 2021 and we didn't find it until 2023, that they must have had access for 2 years. I think that, in fact, they kept it in storage until they were ready to use it, knowing that once they did, it would likely be discovered quickly.

Mr. STRONG. Thank you. That leads to my next question. Are the Chinese still able to access Microsoft's corporate network today?

Mr. SMITH. No, not with anything they did before, and we will do everything we can to ensure that they don't get in any other way.

Mr. STRONG. Thank you. Again, I thank you for the way that you have represented yourself and your company today.

Mr. Chairman, I yield back.

Chairman GREEN. The gentleman's yields.

I now recognize Mr. Crane for 5 minutes of questioning.

Mr. CRANE. Thank you, Mr. Chairman.

Mr. Smith, thank you for preparing and coming before the Homeland Security Committee today.

Mr. Smith, you're the president of Microsoft. Is that correct?

Mr. SMITH. That's correct.

Mr. CRANE. You're here today to discuss some leaks and vulnerabilities that Microsoft has had in the past and what you guys are going to do to fix them in the future? Is that correct?

Mr. SMITH. Yes, that's right.

Mr. CRANE. Mr. Smith, you said earlier in the hearing that some of your competitors are in this very hearing room. Is that correct?

Mr. SMITH. So I've been told. They could raise their hands if you ask them. It's probably not the best use of time.

Mr. CRANE. OK. So would it be fair to say, Mr. Smith, that you understand the importance of being strong and formidable today with some of your opponents, or competitors in the room?

Mr. SMITH. I'm sorry, I didn't hear.

Mr. CRANE. Do you understand the importance of appearing strong and formidable today because some of your, you know, opponents and competitors are in the room?

Mr. SMITH. I think the reason that—I don't know if I would use the word "strong" or "formidable." I think the reason we need to be responsible and resolute is because of our adversaries abroad, not so much the competition in the industry——

Mr. CRANE. OK. How about this, Mr. Smith, have you ever heard the saying that weakness is provocative?

Mr. SMITH. I've heard similar things. I don't know if I've heard that one in particular, but I understand it.

Mr. CRANE. Well, you're running one of the most powerful corporations in the world, so I'm sure that that's something that's not completely alien to you, right?

Mr. SMITH. Yes, I—it's—those—you know, let me put it this way: Size brings power, but mostly what it brings is responsibility. I

would much rather focus on the need to be responsible than anything else.

Mr. CRANE. OK, fair enough. Mr. Smith, would you say that attacks against the United States in the cyber field have increased in the last couple of years?

Mr. SMITH. Absolutely.

Mr. CRANE. Didn't you say in your testimony earlier, sir, that it felt like it was open season?

Mr. SMITH. Yes, or yes, I did say that. I think that's right. It is an open season on U.S. targets by certain foreign adversaries.

Mr. CRANE. How many attacks are you guys seeing a day, Mr. Smith?

Mr. SMITH. I had the precise number in my written testimony, what I've been saying here which is reflective there is more than 300 million per day.

Mr. CRANE. Three hundred million per day?

Mr. SMITH. Yes.

Mr. CRANE. Wow. Mr. Smith, you're aware you're in the Homeland Security Committee. Is that——

Mr. SMITH. Yes, absolutely.

Mr. CRANE. So you understand that the scope of the Homeland Security Committee is much larger than just cyber attacks. Is that correct?

Mr. SMITH. Absolutely.

Mr. CRANE. Good. Are you aware, Mr. Smith, that there was a reporting just this last week that 8 individuals with ties to ISIS were arrested this week in multiple U.S. cities? Did you hear that story?

Mr. SMITH. Actually, I was not until you just told me.

Mr. CRANE. OK. Well, that happened this week. How about this one, Mr. Smith: Are you aware of the reporting that Russian ships were 30 miles off the coast of Florida just this week as well?

Mr. SMITH. I did hear that or read about it.

Mr. CRANE. Yes. One of my colleagues asked you, sir, he said, what can we do to help you? Nobody really wants to say it in this room, but I'm just going to say it, one of the things that we can do to help you is actually get stronger leadership that's respected around the world. That's actually one of the big problems here. I think everybody in this room actually knows that.

So, that is one of the things that I think that we're doing to be doing. But the other thing I wanted to point out, Mr. Smith, is this isn't an isolated incident, right, all these increased cyber attacks that we're seeing, right? We're seeing attacks across the board and everybody in this room knows it. We're seeing it at the border, we are seeing Russian ships off the coast of Florida. Just this week, 8 individuals with affiliation to ISIS were captured in multiple U.S. cities. That's why I started my questioning, sir, with weakness is provocative, and if you knew what this meant and what it meant to you.

Mr. SMITH. Yes, I—I understand. Let me just be clear, I have expertise in one field, not in every field. But I understand what it means in my field.

Mr. CRANE. I know you do, sir. We've said this for a long time in this country, peace through strength. There is something to that.

When the United States senses that we're weak or feckless and we have weak and feckless leadership, these are the types of things that we see. So, I'm hoping that not only this body, but the American people can work together to get better leadership for this country because I know it's going to impact your business. I want to say one more time, I appreciate you actually coming here today, taking ownership and responsibility, because as some of my colleagues have said, it's not something that we see every day, so thank you, sir. Appreciate it.

Mr. SMITH. Well, thank you. Then let me just conclude because I think this gets us through the entire committee, I would just underscore what I've tried to say throughout, we do understand the importance of what you all do on this committee, what the CSRB and what CISA do, the importance of this report, and we are committed to addressing every part of it.

Chairman GREEN. I now recognize the Ranking Member for his 5-minute closing statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Mr. Smith, you've done a creditable job in representing your company. You do understand that there are some challenges with running a company like that. It's only one thing can create a real problem, and I think you have addressed it thus far. So let me thank you for that testimony and committing to participating in the committee's on-going oversight.

Microsoft has an enormous footprint in both Government and critical infrastructure networks. It is our shared interest that the security issues raised by the CSRB are addressed quickly. You've said that the main things you've already done, we appreciate it.

This hearing was important to understand last summer's cyber incident and Microsoft's approach to security. In my view, it is just the beginning of an on-going oversight to ensure that the technology products used by the Federal Government are secure, and that Federal vendors take the security obligation seriously. We've had that discussion in my office, and I'm sure you've talked with other Members about that. So in that spirit, I've got a couple of final questions, I told you there's no "gotcha" kind of thing. If you can say yes or no, that's good. But if you need a little time, I'll understand that too.

Will Microsoft commit to being transparent with its customers, particularly the Government, about vulnerabilities in its products, including cloud products.

Mr. SMITH. The answer is yes. The only qualification I would offer is we need to do it in a way where we share information with the right people and the right governments and do it in a way that doesn't make that same sensitive information available to our adversaries.

Mr. THOMPSON. Sure.

Mr. SMITH. I'm sure we can do that.

Mr. THOMPSON. If it's a Classified setting, as the Chairman said, we're fine with it.

Mr. SMITH. Yes.

Mr. THOMPSON. OK, thank you. Will Microsoft commit to being transparent with its customers about its investigation into cyber

incidents, including related to root cause, the scope of impact, and any political on-going associated threat?

Mr. SMITH. Yes, and obviously the same qualification as before. Then I would just add—and we are working to do that. A lot of what we're doing by adding to our chief information security officer infrastructure, Government structure is an ability, and really a desire to get out and share more information with customers the way you described.

Mr. THOMPSON. Thank you. So will Microsoft commit to establishing benchmarks and time frames for implementation of the CSRB recommendations, and the Secure Future Initiative and commit to proactively keeping this committee informed of its progress?

Mr. SMITH. Yes.

Mr. THOMPSON. Will Microsoft commit to performing an on-going and transparent evaluation of risk associated with business ventures and adversarial nations?

Mr. SMITH. Yes, I think we need to.

Mr. THOMPSON. Well, I look forward to the committee's on-going oversight and continued engagement with Microsoft. One of the things that we are tasked with is looking at keeping America safe, both from foreign and domestic adversaries, and obviously cyber is, in everybody's opinion, a major threat, and so—but you have to talk to us.

Mr. SMITH. Believe me, I will. You have just defined not just the mission, but the cause.

Mr. THOMPSON. Thank you.

Mr. SMITH. I think it unites all of us.

Mr. THOMPSON. Thank you. I yield back, Mr. Chair.

Chairman GREEN. The gentleman yields.

Thank you, Mr. Smith, for coming today. I'll talk a little bit more about that. I also want to thank our Members for what I think was very collaborative and cooperative, good tones of questions. We had, you know, some important things to do here, ask questions of accountability to determine the responsiveness of the company to the report. But we also had to protect because the bad guys are watching, so we had to be careful.

I want to thank you too for the time you've spent in our office just going over this stuff as well. I know you've made yourself available, both to the Ranking Member and myself, and we really appreciate that.

He asked actually most of my questions about transparency and things like that. So, I just will say this, you know, sometimes Government in this public-private partnership that we talked about a couple times, several Members brought it up, sometimes the Government can kind-of get in the way, too, and I want to ask that you, you know, educate us as much as possible. I'll give you an example of the SEC ruling on a 4-day report for a breach and those kinds of things. I'm on—some of the big cybersecurity companies, I mean the biggest in the Nation have told me it is a 7- or 8-day to fix a breach before announcing to the world that at 4 days, we've got a hole in the wall, and it takes 7 days to close the hole. We are inviting, this Government forcing companies across the country to invite the enemy to come in, right? So that's a stupid regulation. So, we need help on understanding where the Government also cre-

ates problems. So I'd appreciate anything that comes to mind over it, you pick up the phone and call us, OK?

In one of the initiatives here, we talked about cyber work force. One of the other initiatives is the synchronization of the regulations that are out there, and to make sure that we're not duplicitous, and that we're not contradictory. As I understand it, there are some regulations that are. So again, we would ask your company to help us, and the competitors who are in the room, to understand where Government kind-of gets in the way of actual cybersecurity. Because if we're causing you to have duplicitous effort, that's money that can be spent on real cybersecurity. So in this partnership, we need communication, not just on the issues that are brought up here with this breach that was identified but, you know, how we make things better, and work better on how we regulate and create compliance requirements, things like that.

Thank you, again, for your time. I thank the witness for his valuable testimony and the Members for their questions. The Members of the committee may have some additional questions. By the way, I did already get one that will probably require a Classified mechanism. We can discuss with you and the staff on how we best do that. We would ask that the witness respond to these questions in writing. Pursuant to committee rule VII(D), the hearing record will be held open for 10 days.

Without objection, the committee stands in adjournment.

Mr. SMITH. Thank you, Mr. Chairman.

[Whereupon, at 4:06 p.m., the committee was adjourned.]