Strengthening the Nation's Cybersecurity:
Lessons and Steps Forward Following the Attack on SolarWinds

Written Testimony of Brad Smith
President, Microsoft Corporation

Senate Select Committee on Intelligence
Open Hearing on the SolarWinds Hack

February 23, 2021

Chairman Warner, Vice Chairman Rubio, thank you for the opportunity to appear today to discuss the recent SolarWinds attack, contribute to an understanding of what happened, and address potential solutions for how we can work collectively to keep a cyber event of this magnitude from occurring again.

I will begin by sharing what Microsoft has learned about the SolarWinds attack. From what we know so far, this attack was sophisticated and complex. While we have completed our internal investigation of the attack's impact on Microsoft, there remains more to investigate and learn in terms of its impact on governments and other organizations around the world. No one should believe that this attack has yet been fully understood or is yet fully contained. At Microsoft we are committed to the continued sharing of what we learn. That is why I am here today.

If one thing is apparent, it's that we all have important work to do to strengthen the nation's cybersecurity. We must be prepared for even more sophisticated and well-resourced foreign attacks in the future. We will need new measures that are grounded in leadership by the public sector and even more collaboration with the private sector. We will all need to do more to help organizations large and small to secure their IT infrastructure. All this must start with more communication and sharing of information, both for more effective real-time responses during cyber incidents and to share new lessons afterwards.

Today, too many cyberattack victims keep information to themselves. We will not solve this problem through silence. It's imperative for the nation that we encourage and sometimes even *require* better information-sharing about cyberattacks.

This responsibility is especially important for the tech sector itself. For cybersecurity as for other areas, knowledge is power. Broader information-sharing is indispensable to strengthening the nation's cybersecurity protection.

After reviewing what we have learned in detail below, I will address several specific concrete areas where we believe action is essential:

- First, we need to **strengthen supply chain security** for the private and public sectors alike for both software and hardware.
- Second, we need **to broaden use of cybersecurity best practices**, including through improved cyber hygiene and a commitment to IT modernization.
- Third, we need a **national strategy to strengthen how we share threat intelligence** across the entire security community.
- Fourth, we need to **impose a clear, consistent disclosure obligation** on the private sector.
- Finally, we need to **strengthen the rules of the road for nation-state conduct** in cyberspace.

1. Background/Overview

We are here today because thousands of miles away, a capable and determined adversary of the United States executed a disciplined attack, penetrating large government agencies and key private sector companies. This sophisticated and successful attack shines a bright light on the need to significantly strengthen cybersecurity protection across all our vital enterprises, organizations, and government agencies. We must also take the necessary steps to prevent and respond more quickly to any future attacks, starting by advancing international consensus on establishing and enforcing a rules-based order online.

The US Government has attributed the attack to an "Advanced Persistent Threat Actor, likely Russian in origin."[1] While Microsoft is not able to make a definitive attribution based on the data we have seen, we do not disagree with the government's assessment. In short, and even after considerable review, we have seen no evidence that points in any other direction.

We know that what lies on the surface is only part of this attack's story, and we all should remain focused on what is not yet known. The victims that have been revealed to the public represent an important portion of the problem, but they are like the tip of the iceberg, and we do not know what lies beneath the surface. This is especially pertinent in this case because all of the attacks we've identified started "on premise," meaning on a server physically within an organization's presence. And yet we only have direct visibility to the attack when it then moved to the cloud. As a result, customers that haven't yet migrated to the cloud are more likely to be continued and undiscovered victims.

The fact that we are here today, discussing this attack, dissecting what went wrong, and identifying ways to mitigate future risk, is occurring only because my fellow witness, Kevin Mandia, and his colleagues at FireEye, chose to be open and transparent about what they found in their own systems, and to invite us at Microsoft to work with them to investigate the attack. Without this transparency, we would likely still be unaware of this campaign. In some respect, this is one of the most powerful lessons for all of us. Without this type of transparency, we will fall short in strengthening cybersecurity.

2. The Attack

At Microsoft we first became aware of the SolarWinds attack when FireEye contacted us in late November, just after Thanksgiving. They had uncovered a breach of their system and asked for our support in their internal investigation. In addition to reaching out to share threat intelligence, they took some critical steps swiftly and voluntarily, including alerting the federal government of what they found and disclosing the breach to the public.

After several days of intense research and collaboration, the story of what occurred started to come into focus. FireEye discovered that an attacker had successfully breached its on-premises network (its private data center housed in their own facility). FireEye had installed an update to software it used from SolarWinds, and when they did, they unknowingly also installed the attacker's malware, opening a back door into FireEye's private system.

While there is still more to investigate regarding how this occurred and the scale of the attack, we know SolarWinds itself had been breached through its own on-premises network, and the initial compromise happened in the fall of 2019. The Russian attackers placed malware into SolarWinds Orion software update, which was subsequently distributed to more than 17,000 customers. At Microsoft we call the initial backdoor malware installed with the Orion update Solorigate.

[1] Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA

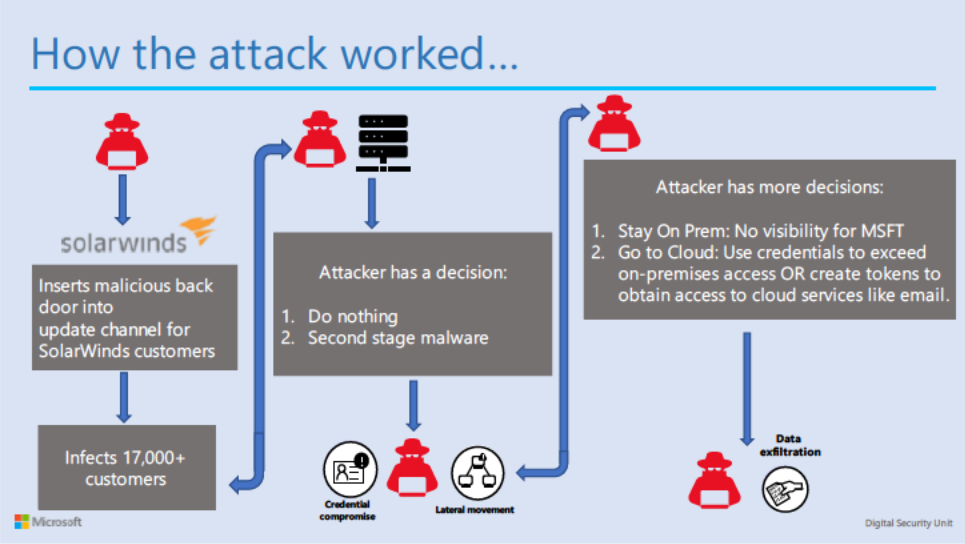
Attacks that compromise software updates have been observed since at least 2015.[2] We all recognized the potential power of this type of attack with NotPetya,[3] Russia's destructive attack on Ukraine in 2017. Much like the technique used by Russian attackers during NotPetya, the SolarWinds attack targets the civilian software supply chain. This is a particularly insidious vector as it undermines trust in the very systems technology companies use to update software, remediate vulnerabilities, and protect users from intrusions.

The SolarWinds attack can be thought of as a large-scale series of home invasions. The malware installed with the Orion update was, in effect, a key that unlocked and secretly opened the back door to over 17,000 houses, with each house representing an on-premises network, without the owner noticing the door was open. This attack worked against any network, no matter what company's technology was being used.

The Russian attacker then used information about each victim's network, transmitted to it by the malware in each house, to install a more powerful malware package in the houses that were most interesting to them. This second malware package opened a new way – let's call it a window – to communicate with the victim networks. With this new access point established, the attacker hid its presence by closing the back door so it would not be discovered.

Once inside the house, the attacker in effect turned off any security cameras – that is, it turned off event logging tools and in some cases antivirus software – and began sneaking around, looking for valuable things, like looking for keys that would give them access to the most precious possessions in the home. In network defense, we call this looking for tools and methods to elevate privileges, essentially finding a way to gain access to any guarded room or safe that houses valuable information.

In some houses the attacker found valuables, such as red-team tools or snippets of source code, which it then copied and took. Red-team tools are especially important here because they are the very tools used by cybersecurity organizations to evaluate the security posture of an enterprise system. In some cases, the Russian actors were looking for keys that would allow access to other environments, like a burglar looking for car keys inside a home. The keys they sought would give them access to the victim's cloud services, including resources like Office 365. And just like a stolen car, these cloud services can be accessed with the right set of keys.



[2] EvLog Security Note (eventid net)
[3] The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED

The SolarWinds Orion software update was the principal initial vector for many of these attacks, but it was not the only entry into these houses. In some instances we have seen, the Russian actor used aggressive password spray attacks to gain access. A password spray is when an attacker attempts to login using a variety of common or relatively simple passwords against many targets, knowing that someone in an organization is likely to have one of them as their password.[4] This is a technique that Russian actors have used many times in recent years. The attacker also appears to have leveraged other supply chain attacks[5] to create other entry points as well, and we are continuing to investigate as we do not believe all supply chain vectors have yet been discovered or made public. All told, we believe that the attacker may have used up to a dozen different means of getting into victim networks during the past year.

We have learned through our investigations that this attack was a multi-faceted campaign by this Russian attacker, but at its core it was an identity attack, a conclusion that White House Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, confirmed during a press conference on February 17th. The Russians did not just want to get inside the houses of the victims. They wanted to find the most interesting valuables, which to them meant reading, examining, and in some cases taking data and information. Just as they used many ways to initially attack their victims and open a back door, they also used a variety of ways to compromise identity.

It is important to understand this aspect of the attack: unlike some attacks that take advantage of vulnerabilities in software, this attack was based on finding and stealing the privileges, certificates, tokens or other keys within on-premises networks (which together is referred to as "identity") that would provide access to information in the same way the owner would access it. This approach was made much easier in networks where basic cybersecurity hygiene was not being observed – that is, where the keys to the safe and the car were left out in the open.

3. The Victims

One of the first steps we took was to determine if we could help identify other victims of this attack. In doing this work Microsoft has discovered a great deal, but almost certainly we have not yet learned everything there is to know about this attack. There is much we and the rest of the security community still do not know.

Microsoft has notified 60 customers, most of which are in the United States, that they were compromised and likely had data accessed in this campaign. The primary targets (50%) are information and communication technology companies, with the rest of the victims being a combination of U.S. government agencies, government contractors**,** and NGOs including civil society organizations such as think tanks and academic institutions.

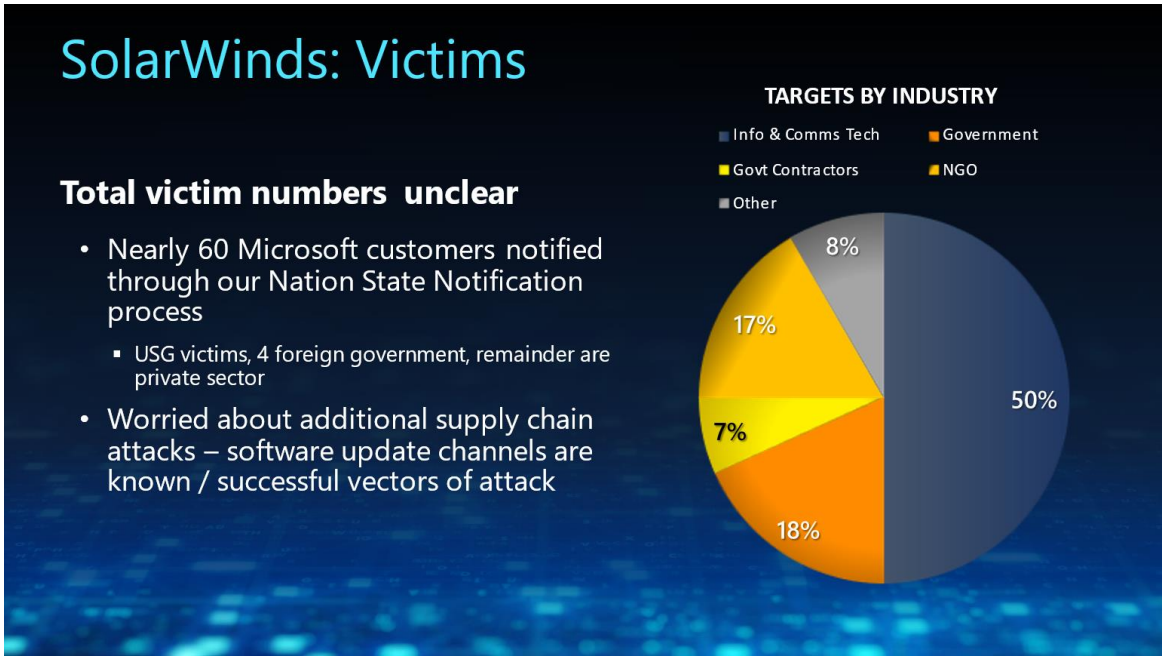
Without question, these are not the only victims who had data observed or taken. We do know that there are other companies whose customers have been compromised but who have not revealed victim information publicly. We also know from work we have done helping customers that there are victims where the Russian attacker stayed entirely within the on-premises network, and therefore are not among the 60 we discovered and notified. On February 17, Ms. Neuberger provided the government's first public estimate that the total number of victims was approximately 100 private sector companies and 9 U.S. government agencies. In addition to this estimate, we have identified additional government and private sector victims in other countries, and we believe it is highly likely that there remain other victims not yet identified, perhaps especially in regions where governments and other organizations where cloud migration is not as far advanced as it is in the United States.

In truth, no one yet knows for certain, except the Russian attacker.

---

[4] Protecting your organization against password spray attacks - Microsoft Security

[5] Mimecast says hackers abused one of its certificates to access Microsoft accounts | ZDNet



4. Microsoft's Response

To respond to this attack, Microsoft has taken an approach of detect, notify, remediate, and inform. Each of these steps is critical to incident response and in many cases the work needed to perform each step overlaps.

Detect

Armed with information learned from work with FireEye, Microsoft and other tech companies acted as a first responder. The first step, along with other anti-virus vendors, was to develop detections for the Solorigate malware so that our Microsoft Defender Antivirus technology could find and alert customers if the malware was present in their networks.[6] As we learned more about the Russian actor and the sophistication of the activity, we took more aggressive action and used Defender not just to detect, but to block the malware so it could not communicate with the attacker. Effectively, we slammed the back door shut.

We concluded that this was an essential first step, and as one commentator noted, we "released the Death Star"[7] on the Russian malware. We also worked with GoDaddy and FireEye to create a "kill switch" so that the Solorigate malware that opened the back door into victim networks would be disabled for everyone, not just our Defender customers. Despite these steps, however, we knew that the Orion update that contained the malware was installed before we could detect or disable it, sometime between March and June of 2020. By the time we blocked it, the attacker had a backdoor open into some victim networks for six to nine months, and during that time it could have opened "windows" into a large number of victim networks.

Our Microsoft Threat Intelligence Center, or MSTIC, which tracks the activity of nation-state actors, worked with the rest of Microsoft's security community to search for traces of activity by the Russian

[6] Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers - Microsoft Security
[7] Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach - GeekWire

actors, including the use of credentials and other identity tools the actor stole from victims to obtain access to Office365 (O365). The 8 trillion signals coming daily into Microsoft from our ecosystem gave us a great deal of data to work with. However, the Russian actors hid their activity in legitimate network traffic and took other sophisticated steps to avoid detection.

Microsoft's only visibility into the Russian activity was communication between victim networks and O365, Microsoft's suite of productivity tools such as email and office applications. We could not look into on-premises networks to hunt for the Russian actor, and Microsoft has information only about networks on our cloud, not those hosted on other vendors' cloud services.

We have discovered that the Russians used several different approaches to obtaining the credentials O365 uses to identify legitimate users. In one approach they used elevated privileges in victim networks to generate what are called SAML tokens. These tokens are an industry-standard way for network resources and cloud services to recognize legitimate users. They are similar to an electronic key card that proves who you are so you can get access to a building or a particular doorway. As it turns out, however, the SAML token generation approach was only used by the Russian attackers 15% of the time among the victims we have identified. In the other 85% of cases, the Russians used a variety of other methods to obtain the credentials they needed to access O365 from an on-premises network.

Notify

As Microsoft teams identified victims, we quickly notified each of these 60 customers and offered information about the attack and the indicators of compromise (IOCs) that would help them start their own investigations.[8] This is a core commitment we make to our customers: we routinely notify customers when we see evidence that they have been threatened or compromised by a nation state actor. In the two years leading up to the Microsoft Digital Defense Report[9] in September of 2020, this amounted to more than 13,000 notifications globally.

Notification is important because it allows customers to take immediate steps to protect data and communications. It also enables customers to use their own logs to track and understand where in their environment an attacker is hiding, and where it might have opened other windows or stolen other information.

Remediate

Once victims were informed of the attack, there was much to do to respond. Victims had to identify how the Russian attackers got into their network – by SolarWinds, a different supply chain vendor, a password spray, or some other vector – as well as determine all the data and information the Russians were able to access.

Dozens of the 60 victims we notified, as well as other customers, asked us for additional support in investigating and remediating the attack. In many of those cases, our Detection and Response Team (DART) was engaged and helped customers assess their networks in search of the Russian actor and its activity. In many other cases we provided consulting and indirect incident response support to customers' own security teams.

We also continued investigating our own network to see if Microsoft was a target, and we confirmed that as a SolarWinds customer we had also been attacked. We began an intensive operation to find, isolate, contain, and expel the attacker, and to understand what the Russian actor was able to do while in our network.

[8] Ensuring customers are protected from Solorigate - Microsoft Security
[9] Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise - Microsoft Security

Our investigation of the impact of this attack on our internal systems, which has just recently been completed,[10] confirms that the Russians were not able to access or use any of our services or systems to attack others. As we reported when the break was discovered,[11] we also have found no evidence that they accessed our production services or customer data or compromised our own O365 accounts.

We did detect unusual activity with a small number of internal accounts and discovered that the Russian attackers had viewed and, in a few cases, copied some subsets of source code from several source code repositories. Due to restrictions in our network, however, the Russian attackers were not able to modify any code or engineering systems, and our investigation further confirmed no changes were made. We have stopped this activity.[12]

While we of course were unhappy to learn of any network intrusion, we have concluded that the viewing and limited copying of some subsets of source code do not raise a significant security concern. This is because Microsoft manages source code through an inner source[13] approach, meaning we embrace open-source software development best practices and foster an open source-like culture by making our source code viewable by all Microsoft employees. This means we do not rely on the secrecy of source code for the security of our products, and our threat models assume that attackers have knowledge of our source code. In other words, the adversaries snuck into an additional room in our house, but it wasn't one that was guarded in a way that required especially elevated privileges or any special key to access. While the Russian actor saw and, in a few cases, copied some source code, in all cases it was just a small subset of the code for any particular product or service.

Inform

We are continuing to identify the risks and address the damage of this attack to ourselves and our customers. We have also publicly documented our efforts throughout the process,[14] publishing 31 blog posts and collecting them and other information in a centralized Resource Center open to the public. This details our findings and providing guidance for customers, hunters, and security teams that are doing their own investigations.

We applaud FireEye, SolarWinds and the handful of other companies that have been willing to speak publicly about this attack and raise awareness for hundreds more who were affected. But only a select few of the companies, organizations, or government agencies that were attacked, whose technologies or services were implicated in the attack, or that have information about this attack have been willing to come forward or to share information publicly. It is important that the private sector speak out and share relevant information so that we can all respond to an incident rapidly and efficiently and learn from each incident how to be more resilient in the future. If the industry continues to hide what we know, we cannot effectively defend ourselves.

As we testify today, industry does not know the total number of confirmed victims beyond what Microsoft and a few others have shared publicly and the recent disclosure of over 100 total American victims. Unfortunately, not all who are in a position to do so are searching hard enough to find those victims that may be still lost in the rubble. Government inquiry needs to learn what it can from those who have stepped forward but must also seek truth from those who have not. There are still too many missing pieces of the puzzle.

We need a full examination of what other cloud services and networks the Russians have accessed. Before we as a nation can secure our digital ecosystem, we need to know that the Russian attackers are no

[10] Turning the page on Solorigate and opening the next chapter for the security community - Microsoft Security
[11] Microsoft Internal Solorigate Investigation Update – Microsoft Security Response Center
[12] https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/
[13] Inner source - Wikipedia
[14] Solorigate Resource Center – updated February 5, 2021 – Microsoft Security Response Center

longer present in the dozens or hundreds of networks in which they have accessed data or information through this attack.

In addition, it is of critical importance that all organizations scan their networks with one of the leading antivirus services, like Microsoft 365 Defender. Anyone who has – or ever had – the malware on their system is at risk of this Russian actor looking at or stealing information from their network or cloud services. It's important for all of us to recognize that this Russian actor is extremely skilled at hiding and covering their tracks and we know for certain they are interested in information beyond Office 365 email.

It is also important that governments and the security community have the ability to focus on victims beyond those that Microsoft has identified. Focusing primarily on the victims that have been identified would present a selection bias that is likely to distort any analysis of the attack. It's a virtual certainty that there are victims in which the attacker has remained entirely on premises or accessed other company's cloud services.

The security community collectively also needs to take steps to defend against future such attacks. To do that, the first and most important step is for every company, organization, or agency to take even more seriously the security of identity in their networks. This can best be done by applying "zero trust"[15] principles to ensure that attackers cannot gain access to information or resources meant only for authorized users. Microsoft has published extensive guidance on how to look for this type of attack, remediate identity risks, and adopt zero trust and we recommend you review it closely.[16]

5. Government and Private Sector Collaboration

As Ms. Neuberger reported, a number of victims were U.S. government agencies. As with all our identified customers, Microsoft reached out to notify impacted government agencies, share relevant information on how to initiate a response, and identify the IOCs they could use to hunt for the Russian actor in their networks. In every case where we notified a victim, we were the first to recognize that they had been compromised. In the process of notification and subsequent communication, we observed two important opportunities for improvement.

Baseline cyber hygiene

What we found in several cases was troubling. Basic cyber hygiene and security best practices were not in place with the regularity and discipline we would expect of federal customers with the agencies' security profiles. In most cases, multi-factor authentication, least privileged access, and the other requirements to establish a "zero trust" environment were not in place. Our experience and data strongly suggest that had these steps been in place, the attacker would have had only limited success in compromising valuable data even after gaining access to agency environments.

This incident serves as a reminder that we must all remain vigilant in driving implementation of basic cyber security practices – multi-factor authentication, patching and updating, deployment of strong detection tools and logging, use of least privileged access, creation of an incident response playbook that is up to date and routinely exercised for readiness, and other vigilant work to improve our defense and resilience to attacks.

The role of the cloud in mitigating these types of attacks also cannot be understated. The success of this attack depended primarily on the Russian actor's ability to compromise on-premises identity systems. We

[15] Zero Trust Deployment Center | Microsoft Docs

[16] Solorigate AzureAd IOCs (microsoft.com); Azure AD workbook to help you assess Solorigate risk - Microsoft Tech Community; Using Zero Trust principles to protect against sophisticated attacks like Solorigate - Microsoft Security

continue to strongly recommend that identity should be moved to the cloud, where it can be defended with the latest technologies.

Despite this observation, we have been heartened by our many conversations since this attack with leaders in the relevant agencies. The Administration has quickly put skilled and knowledgeable leaders in place and has committed to improving the security of government agencies and the ecosystem generally. We are confident that Anne Neuberger, in her new role as Deputy National Security Advisor for Cyber and Emerging Technology, and other leaders in critical cybersecurity roles will apply the lessons learned and take the necessary steps to improve the government's defensive readiness.

Improved information sharing

As the SolarWinds hack unfolded, government agencies were also key stakeholders in investigating and responding to the attack. We applaud the speed with which the Cyber Unified Coordination Group put out a joint statement attributing the attack to a likely Russian actor.[17] This was one of the fastest public attributions of a nation-state attack by the United States. It takes time to get attribution right, and while we strongly support public attribution of nation state attacks, we also support taking the steps required to ensure that those statements of attribution are well-founded.

Avenues of communication between the private and public sectors, however, continue to offer room for improvement. As we look to the future, especially given our understanding of this sophisticated attack, crucial incident response details can be shared more quickly, information sharing can become more specific and detailed, and action can be taken in ways that are clearer and better coordinated.

Nonetheless, it's important to recognize the recent rapid, transparent, and effective public information sharing, especially by the NSA. In addition, CISA used the playbook it developed in successfully defending the integrity of the 2020 U.S. elections to reduce the burden of communication during a time of intense incident response effort.

There nonetheless remain important opportunities to apply recent lessons learned and strengthen the nation's cybersecurity protection. One such area would involve better implementation of the foundational principles and plans the government has crafted in collaboration with private sector partners. For example, the 2016 Presidential Policy Directive 41 (PPD 41)[18] and National Cyber Incident Response Plan (NCIRP)[19] highlight the importance of "unity of governmental effort" – and states explicitly that "the first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident." This was not our experience in observing the immediate aftermath of the SolarWinds attack. We recommend that the government reconsider the multiple leadership roles required in a cyber incident and work to establish a more unified incident response approach, with clear goals to assess, respond, and recover from large incidents going forward.

If there is a declaration of a "significant cyber incident" as contemplated in the NCIRP and PPD 41, the expectations and needs from the U.S. government to the private sector should be communicated clearly and response should be run collaboratively. A lead agency should be identified to consolidate information useful to the private sector and to ensure rapid and thorough disclosure. In our view, this is best done by a part of the government outside of law enforcement, given the latter's critical but different obligation to investigate crimes and often to keep information secret to help advance an investigation.

---

[17] Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA

[18] Presidential Policy Directive -- United States Cyber Incident Coordination | whitehouse.gov (archives.gov)

[19] National Cyber Incident Response Plan - December 2016 (cisa.gov)

The SolarWinds attack also saw imperfect incident response information sharing across the private sector and with government. There are valid limitations to what the private sector will share in order to protect business models that fund security resources and innovation. But the private sector also faces obstructive concerns of legal liability, fears of reputational damage, and outdated silos that prevent the communication and transparency that are necessary to best protect our digital ecosystem collaboratively. In this instance, while some private sector participants have been transparent, others have chosen to be less forthcoming, a failure that needs to be addressed.

For both governments and the private sector, there may be risks to exposing methods by which information is obtained. Governments rightly want to protect sources and methods of acquiring information, much of which is justifiably classified. Private sector organizations likewise do not want to reveal to adversaries how they track and discover malicious activities, because this would enable attackers to better disguise their activities in ongoing and future campaigns. In some cases, sharing is also justifiably limited due to customer privacy concerns, given that entities affected by or investigating an attack (both government and private sector) are appropriately responsible for protecting the privacy of individuals and sensitive information they control or manage on behalf of customers. As technology use continues to become even more ubiquitous throughout society , it will become even more critical to have an incident response plan that enables the public and private sectors to partner more fully, thereby ensuring the continuity of essential services and restoration of impacted functions.

6. Next Steps and Policy Recommendations

Given this recent experience and lessons learned, we believe there are several key steps the federal government and private sector can take to improve our readiness to protect against future attacks.

First, we need to strengthen supply chain security for the private sector and the U.S. Government for both software and hardware.

Across federal agencies and the broader ecosystem, organizations currently struggle to manage supplier inventories, understand dependencies, and set cybersecurity requirements for critical suppliers. Just three months ago, the Government Accountability Office highlighted that no civilian agencies manage agency-wide supply chain risk assessments or fully implement requirements for suppliers.[20] There clearly is both a need and opportunity for improvement.

There are existing best practices to draw upon, especially for software supply chain security. Any software developed or procured by federal agencies, including software that powers cloud services to which agencies subscribe, should reflect secure development practices[21] and clear commitments to maintain software, including through vulnerability management,[22] during the defined life of a product.[23] Federal agencies should also require use of integrity controls throughout the software development, testing, and delivery processes, mitigating the risk of an attacker inserting malicious code before a new software product or update is delivered to users.[24]

There are also gaps to address with urgency – and the recognition that widely deploying high-quality approaches takes time. One such gap is related to software itself. Today, most software projects are built

[20] https://www.gao.gov/assets/720/711266.pdf
[21] Microsoft Security Development Lifecycle; Resource: Secure Development Practices Archives - SAFECode; ISO - ISO/IEC 27034-1:2011 - Information technology — Security techniques — Application security — Part 1: Overview and concepts
[22] https://www microsoft.com/en-us/msrc/cvd; ISO - ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure; ISO - ISO/IEC 30111:2019 - Information technology — Security techniques — Vulnerability handling processes
[23] Microsoft Lifecycle Policy | Microsoft Docs
[24] http://safecode.org/wp-content/uploads/2018/01/SAFECode_Software_Integrity_Controls0610.pdf

by leveraging third-party components – both commercial and open source. When selecting third-party components to use, it's important to consider the impact that a vulnerability could have on the security of the larger system into which the components are integrated. Microsoft's Security Development Lifecycle requires our software engineers to maintain an accurate inventory of third-party components, a plan to respond when new vulnerabilities are discovered, and additional validations as determined by context. We're also working alongside partners to develop industry standards for enhancing transparency and improving integrity checks for third-party components, providing a consistent way for software buyers to pursue greater visibility.[25]

Another gap is related to software developers. We need to drive implementation of best practices across the vast and diverse community of developers, whether they're working at major technology companies or chasing the next big idea in someone's garage – including through better automation and security tools. At Microsoft we are working continuously to improve access to and simplify use of security tools and automation on our developer platforms, and we've extended recent security enhancements we've made to internal tools to the broader developer community through GitHub.[26] In August, Microsoft also announced that we joined industry partners in creating the Open Source Security Foundation (OpenSSF),[27] which is focused on providing the best security tools for open source developers and securing critical open source projects.[28]

As these efforts continue to mature, standards and learnings should be integrated into requirements for federal software providers. Implementation of this year's National Defense Authorization Act provides an opportunity to develop new software acquisition[29] security requirements that may be appropriate for re-use across federal agencies.

We also need to address hardware supply chain security with requirements for critical hardware components, and we need to enhance resiliency by ensuring access to trusted suppliers of critical ICT products and services. The U.S. needs a whole-of-government approach, closely coordinated with industry partners and global allies that share our commitments to responsible use of technology, human rights, and other fundamental values.

Second, we need to broaden use of cybersecurity best practices, including through improved cyber hygiene and a commitment to IT modernization.

When Microsoft's cloud services are attacked, we can detect anomalies and indicators of compromise in ways that are not possible in an on-premises environment.[30] This capability is critical to discovering, remediating, and recovering from an attack – but doesn't prevent the risk of on-premises security lapses that result in escalations of privilege that ultimately enable attackers to access cloud services.

Cloud migration is critical to improving security maturity across many organizations. At the same time, it's not a panacea; even as technology users modernize legacy systems, they need to have strong basic security practices in place. This includes fundamentals for establishing a Zero Trust environment, assessing the security of cloud providers, and re-orienting risk management activities to complement third party services and security automation.

---

[25] Software Bill of Materials | CISQ - Consortium for Information & Software Quality (it-cisq.org); in-toto | A framework to secure the integrity of software supply chains (in-toto.io)
[26] GitHub Security · GitHub; Features · Security · GitHub; DevSecOps with Azure | Microsoft Azure
[27] Home - Open Source Security Foundation (openssf.org)
[28] Microsoft Joins Open Source Security Foundation - Microsoft Security
[29] CRPT-116hrpt617.pdf (congress.gov)
[30] We've also issued guidance to support customers detecting Solarigate attack activity in on-premises networks, Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security

At a national level, Microsoft recommends that the U.S. government, and particularly CISA, drive a national effort to improve cyber hygiene, with a particular focus on identity and access management. The SolarWinds incident makes plain why all organizations, including governments, must heighten their focus on implementing basic security best practices, even as we harden technology development processes and explore other steps. It bears repeating that this attack was simultaneously sophisticated and ordinary; a sophisticated Russian adversary created and quickly shut backdoors, quietly cracked open windows, and hid its tracks as it sought ways to gain elevated privileges; but it also used known techniques like password spray and identity compromise that could have been prevented or better resisted with basic cybersecurity hygiene.

IT modernization can also help with the implementation of cyber hygiene best practices, including supply chain risk management.[31] There is no question that using cloud services for identity management can also be safer and more secure than on-premises identity systems. Cloud-based identity can be easier to maintain – with fewer moving parts for attackers to exploit and organizations to defend. It can also benefit from the use of global telemetry, rich analytics, and automation to signal when something is amiss.[32] Our ability to guard against password spray attacks, which account for more than one third of account compromises, is a good example. This tactic attacks many users with a small number of common passwords, rather than many common passwords against one user, which triggers password lockout. When a customer moves to the cloud, we can detect password spray patterns by looking at failed login attempts as "password hashes" (i.e., passwords scrambled by encryption) across millions of tenants around the world.[33] Recent Government Accountability Office reports[34] clearly demonstrate that, more broadly than supply chain or identity management, the use of cloud services can result in better security, more productivity, and lower costs. But cloud users can only fully capture these benefits if they also effectively manage their ongoing security responsibilities,[35] including by managing visibility across cloud platforms and assessing whether cloud services fit their security needs.[36] Federal agencies have not yet consistently used cloud services that have demonstrably met federal security requirements, citing resource constraints and other challenges.[37] Clear, consistent requirements and streamlined compliance programs can help agencies choose cloud services that help them prevent and respond to attacks and ultimately empower human resources to focus on complementary security operations and tasks.

Third, we need a national strategy to strengthen how we share threat intelligence across the entire security community.

While we believe that migrating to cloud services and focusing on cyber hygiene will help to prevent and limit the impact of future attacks, we also must recognize that some of the nation's adversaries are sophisticated, well-resourced, and persistent. We need to ensure that we identify and remediate the next sophisticated attack swiftly, limiting the time during which intruders can lurk in networks and quietly steal data and information.

One of the ways we can accelerate our detection of intrusions and strengthen remediation efforts is to improve threat intelligence sharing. In response to this attack, our ability to develop indicators of

---

[31] While supply chain risk management programs require alignment of people, processes, and policies as well as technology, cloud services can also help monitor remote access, protect data exchanged between suppliers and customers, and detect and diagnose issues across applications and dependencies. Supply Chain Risk Management for Zero Trust with Microsoft Azure (6 of 6) | Azure Government

[32] Using Zero Trust principles to protect against sophisticated attacks like Solorigate - Microsoft Security

[33] Advancing Password Spray Attack Detection - Microsoft Tech Community

[34] GAO-19-471, INFORMATION TECHNOLOGY: Agencies Need to Develop Modernization Plans for Critical Legacy Systems; https://www.gao.gov/assets/700/698236.pdf

[35] Shared responsibility in the cloud - Microsoft Azure | Microsoft Docs

[36] Modernizing the security operations center to better secure a remote workforce - Microsoft Security

[37] https://www.gao.gov/assets/710/703193.pdf

compromise and detect intrusions was enhanced by our early coordination with FireEye. Greater shared visibility among all responders about anomalies and consistent indicators across environments may have further accelerated or informed our activities – and those of others conducting investigations.

The current state of threat intelligence sharing across both the private and public sectors is far from where it needs to be. Our own internal experience has demonstrated that it is critical for our MSTIC team to rapidly aggregate and analyze data from across all our data centers and services, and the federal government should do the same. In addition, while parts of the federal government have been quick to seek input, information sharing with private sector first responders in a position to act has been more limited than it should be. Rapid declassification of information is essential to successful information exchange.

The time has come for a more formal and cohesive national strategy for the exchange of cybersecurity threat intelligence between the public and private sectors. This strategy should have provisions for threat intelligence sharing during incident response – when collaboration should be at its best and when competitors and others should set aside differences to focus on the security of the nation and the interconnected global technology ecosystem. But to make this strategy work in any context, foundational issues must be addressed, strengthening cross-government visibility, declassification, and trust in private sector actors to not misuse information that can facilitate threat hunting and remediations.

Fourth, we need to impose a clear, consistent disclosure obligation on the private sector.

Transparency in incident response is extremely challenging. In addition to challenges posed by threat intelligence exchange, organizations impacted by an incident fear reputational damage and liability for compromises.

But transparency also enables more effective incident response. FireEye was transparent and collaborative in response to this attack, enabling our two companies to work together more rapidly and effectively to investigate, identify victims, and support remediation. But few other companies have been willing to come forward to acknowledge what they've found and strengthen our collective response. That's not unique to this attack. Few victims are willing to share information about ransomware attacks. State and local governments, hospitals, and countless other entities are constantly under attack – and yet silence reigns. This is a recipe for making a formidable problem even worse, and it requires all of us to change.

We need to replace this silence with a clear, consistent obligation for private sector organizations to disclose when they're impacted by confirmed significant incidents. In the U.S., there is currently a patchwork of obligations in place. This includes state data breach notification requirements, which cover instances in which customer data is accessed, and federal procurement requirements, including a Department of Defense regulation that requires contactors to report cyber incidents and conduct investigations.[38] By comparison, other parts of the world have requirements that are applied more consistently across organizations operating in their jurisdictions. In the European Union, for example, all digital service providers are required to notify their competent authority of any incident having a substantial impact on the provision of a service.[39]

There are difficult tactical and organizational questions that need to be addressed in determining how to structure such an obligation. Should any obligation be balanced with incentives, such as limited liability protections? What should the threshold be for defining when incidents have a significant or substantial impact and thus need to be reported? And by what timeline should private sector actors be required to provide reports? As incident reporting requirements proliferate around the world, we have real concerns about the mismatch in expectations for quick reports with usable data and the time-intensive process of

[38] 252.204-7000 Disclosure of Information. (osd.mil)
[39] EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu)

investigating an incident and reaching meaningful conclusions about scope of impact. Also, on the government side, who should receive private sector incident reports? How will disclosed information be protected from adversaries?

Disclosure should not be limited just to the private sector. In exchange for imposing such an obligation, government should also commit to faster and more comprehensive sharing of relevant information with the relevant security community.

These are important questions, but we should not get lost in them before answering an even more fundamental question: how can we use these disclosures to strengthen incident responses and better protect the nation? A private sector disclosure obligation will foster greater visibility, which can in turn strengthen a national coordination strategy with the private sector which can increase responsiveness and agility. The government is in a unique position to facilitate a more comprehensive view and appropriate exchange of indicators of comprise and material facts about an incident.

Finally, we need to strengthen the rules of the road for nation state conduct in cyberspace.

Nation state attacks represent some of the most advanced and persistent threat activity that Microsoft tracks; nation state activity groups are focused, have the means to develop and deploy novel techniques and tactics, and are constantly working to improve their capabilities.[40] These threats impact the global technology ecosystem, which all of us rely on for everyday life and essential services.

Globally, governments and private sector and civil society partners must cooperate to establish and reinforce clear expectations for responsible behavior in cyberspace. In recent years, they've made meaningful progress. The United Nations has endorsed[41] a foundational 2015 report[42] on appropriate government behavior, and more than 1,100 organizations have signed the Paris Call for Trust and Security in Cyberspace,[43] which calls for stronger protection of democratic and electoral processes. As hospitals and COVID-19 vaccine research have been impacted by significant cyberattacks over the last year, a group of more than 100 experts has confirmed that international law prohibits nation state cyber operations that have significant harmful consequences on health care infrastructure.[44]

However, as it stands, existing rules are sometimes considered ill-defined and rarely enforced. Despite recommendations by a global group of experts,[45] the United States and like-minded allies need to speak more boldly to make clear that indiscriminate and disproportionate supply chain attacks that put technology users at risk and undermine trust in the very processes designed to protect them are out of bounds for state actors. As Anne Neuberger acknowledged last week, even if the Russian actor primarily leveraged its extraordinary potential access to exfiltrate data, the scope and scale of the attack on SolarWinds customers denote much more than an isolated case of espionage. Attacks that leverage supply chains and widely disrupt confidence in data, systems, and update processes impact many users beyond those targeted. If enough users doubt the integrity of their systems or data, the stability of cyberspace and our readiness to rely on it could be impaired.

As we strengthen rules, we also need clearer commitments and coordinated public attributions and imposition of consequences to hold nation-states accountable for cyberattacks that run afoul of

---

[40] Download Microsoft Digital Defense Report, September 2020 from Official Microsoft Download Center
[41] https://undocs.org/A/RES/74/28
[42] https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[43] https://pariscall.international/en/call
[44] The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector | Oxford Institute for Ethics, Law and Armed Conflict; The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research | Oxford Institute for Ethics, Law and Armed Conflict
[45] https://cyberstability.org/norms/#toggle-id-3

international law and norms. Today, the costs of widely disruptive nation-state activity are unclear, leaving citizens and the infrastructure they rely on at risk and undermining confidence in the stability of cyberspace.

The U.S. government has a critical leadership role in advancing international consensus on establishing and enforcing a rules-based order, and we urge policymakers to lead in ongoing international processes such as at the United Nations and to join the Paris Call for Trust and Security in Cyberspace.

We are encouraged by the recent steps taken by Congress and the new Administration, including the strong nominations and appointments and initial policy positions the Administration has taken. There remains a great deal to do, and we and others in the private sector stand ready to partner with you, your colleagues, and U.S. government agencies to improve the nation's digital safety and security.