International Journal of Innovation Scientific Research and Review
Vol. 04, Issue, 10, pp.3469-3479, October 2022
Available online at http://www.journalijisr.com
SJIF Impact Factor 4.95

IJISRR

ISSN: 2582-6131

Research Article

THE SOLAR WINDS CYBER-ATTACK, THE FEDERAL AND PRIVATE SECTOR RESPONSE, AND THE RECOMMENDATIONS AND LESSONS LEARNED

***Donald L. Buresh, Ph.D., Esq.**

Received 19th August 2022; Accepted 20th September 2022; Published online 31st October 2022

ABSTRACT

The purpose of this paper is to analyze the Solar Winds breach. The article provides a timeline that lists when the hack was discovered, what organizations found the breach, and what was the federal government and private sector's response. The article briefly outlines the federal laws and policies that address cyber-attacks, including the Economic Espionage Act of 1996, the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999, the Federal Information Security Management Acts of 2002 and 2014, the Modernizing Government Technology Act of 2018, the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2019, and Executive Order 14017. Supply chain security issues are explained along with a technical outline of the Solar Windshack, arguing that it was a logic bomb and man-in-the-middle attack. Finally, the recommendations and lessons learned are discussed from the federal government's perspective, the private sector's vantage point, and a legal view. The paper concludes by observing that the American government and private sector industries must be eternally vigilant against future cyber-attacks. These days, it is the price to be paid for becoming and remaining effective and profitable.

Keywords: Responses to a Supply Chain Attack, Solar Winds Cyber-Attack, Supply Chain Related Laws, Supply Chain Security.

INTRODUCTION

The solar wind is a stream of charged electrons, protons, and alpha particles released into space by the corona or the upper atmosphere of the Sun.[1]The heat from the solar wind warms this planet, making a home for living things and beings like you and me. And much like the solar winds from the Sun, Solar Winds Corp. (Solar Winds) sought to become the wind of life metaphorically from a technology perspective. The purpose of the firm was to breathe life into government agencies and businesses by helping them manage their data needs. However, like a supernova where a sun explodes, sending a massive amount of charged electrons, protons, and alpha particles into the vastness of space, the Solar Winds breach wreaked havoc on the federal government and American industries. In 2019 and 2020, it was the ultimate hack, where the lifeblood of organizations, the data that it collects, stores, uses, disseminates, and destroys, were put in jeopardy. Thus, understanding what occurred, the various responses, and the recommendations and lessons are paramount. It is to this end that this paper was written.

WHAT IS SOLAR WINDS, CORP.?

Solar Winds is an American software company that began in Tulsa, Oklahoma, co-founded by David and Donald Yonce.[2][3] The company developed the software product Orion.[4] The application supports governments and businesses in maintaining and managing their networks, systems, and information technology infrastructure.[5] The company's headquarters is in Austin, Texas, and has over 3,300 employees across the United States and other countries.[6][7] Solar Winds was first publicly traded in May 2009.[8] As of December 2020, Solar Winds had approximately 300,000 customers, including various federal agencies and almost all Fortune 500 companies.[9] About 33,000 public and private customers employed Orion.[10]

THE SOLAR WINDS CYBER-ATTACK

This section is divided into three subsections. The first subsection gives the timeline of the Solar Winds attack. The second subsection discusses why the Solar Winds attack was critical. The third subsection provides some reasons why the Solar Winds attack could have originated in China rather than Russia. It should be remembered that Chinese hackers have been attacking the United States for many years.[11]

[1]Nola Taylor Redd, *What Is Solar Wind?*,SPACE.COM (May 18, 2018), *available at*https://www.space.com/22215-solar-wind.html.

[2] Lori Hawkins, *SolarWindsKeeps on Growing*, STATESMAN NEWS NETWORK (UndatedDec. 12, 2018), *available at*https://www.statesman.com/business/employment/solarwinds-keeps-growing/JkhMoapafA0qdJvD5MFILM/.

[3]Liana B. Baker, Greg Roumeliotis, *SolarWindsConfirms It Is Exploring Strategic Alternatives*, REUTERS (Oct. 9, 2015), *available at*https://www.reuters.com/article/us-solarwinds-m-a/exclusive-solarwinds-in-talks-with-buyout-firms-about-a-sale-sources-idUSKCN0S31OT20151009.

[4]Saheed Oladimeji, *SolarWinds Hack Explained:Everything You Need to Know*, TECHTARGET(Jun. 16, 2021), *available at*https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[5]*Id.*

[6] Bloomberg Staff, *SolarWinds, Corp.*, BLOOMBERG (n.d.), *available at*https://www.bloomberg.com/profile/company/0OI:GR.

[7]Treva Lind, *SolarWindsblowsinto Post Falls*, SPOKANE JOURNAL OF BUSINESS (Sep. 22, 2011), *available at*https://www.spokanejournal.com/local-news/solarwinds-blows-into-post-falls/.

[8] Michael Novinson, *$286M Of SolarWinds Stock SoldBefore CEO, Hack Disclosures*, THE CHANNEL CO.: CRN (Dec. 16, 2020), *available at*https://www.crn.com/news/security/-286m-of-solarwinds-stock-sold-before-ceo-hack-disclosures.

[9]Catalin Cimpanu, *SEC Filings:SolarWindsSays 18,000 CustomersWereImpacted by Recent Hack*, ZDNET (Dec. 14, 2020), *available at*https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/.

[10]*Id.*

[11] William Howlett, *The Rise of China's Hacking Culture:DefiningChinese Hackers*, UNIVERSITY OF CALIFORNIA – SAN BERNARDINO (Jun. 2016), *available at*https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1413&context=etd.

The Solar Winds Attack Timeline

This section of the paper discusses the timeline on the Solar Winds attack. It is broken into the pre-attack, actual attack, and post-attack subsections. Table 1 displays the timeline of the attack concisely.

Pre-Attack Period

The Solar Winds attack began with a tiny strip of code on September 12, 2019.[12] According to Temple-Raston, the code checked whether the Solar Winds server was running a 32-bit or 64-bit processor.[13] The code either returned a 0 or a 1, depending on what it found.[14] The code turned out to prove whether it was possible to modify Solar Winds' signed-and-sealed software code.[15] Once the hackers realized they could engage in a supply chain attack, they understood that they could infiltrate Orion.[16] A supply chain attack is a hacking technique where an adversary Inserts malicious code or components into a trusted software application.[17] The idea behind the attack was to compromise a single supplier so that hackers could hijack its distribution system, converting any application sold, including hardware and software, into Trojan horses.[18]With the placement of a pregnant piece of code, a hacker can infect hundreds, if not thousands, of computers as a supplier provides its wares to its customers.[19]

Actual Attack Period

In February 2020, the threat actors inserted malicious code into Orion, the Solar Winds' production software, and in March 2020, Solar Winds began distributing signed software patch updates to Orion that contained the malicious code.[20] The Solar Winds attack was an SQL injection attack.[21] The questions that need to be answered are what is an SQL injection attack, who was the assailant, and how can an SQL injection attack be prevented? An SQL injection is a web security vulnerability that permits a cyber attacker to impede an application's queries to a database. It allows attackers to view data they are not authorized to see. The data might include confidential financial information, personal information, or any other data that an application can access. In many cases, a cyber attacker can modify or delete data, causing untold harm.[22] There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection examples include:

- Retrieving hidden data – an SQL query that returns specific results;
- Subverting application logic – an SQL query that interferes with an application's logic;
- UNION attacks – an SQL query that retrieves data from various database tables;
- Examining the database – an SQL query that extracts information regarding the version and structure of a database; and
- Blind SQL injection – an SQL query that results from an attacker-controlled query rather than the application's responses.[23]

For example, consider an international mutual fund application that displays an investor's portfolio using hidden data. When a user clicks on the Investments category, the browser requests the URL:

https://insecure-website.com/products?category=Investments

This prompts the application to construct an SQL query that retrieves the details of the investment portfolio from the mutual fund database.

SELECT * FROM funds WHERE category = 'Investments' AND purchase = 1

This SQL query requests that the database return all details (*) from the funds table, where the category is Investments, and released is 1. The restriction purchase = 1 is being used to hide funds that are not purchased. Presumably, purchase = 0 for funds that are not purchased.

Assuming that the application does not possess any defenses against SQL injection attacks, an attack would look like:
https://insecure-website.com/funds?category=Investments'--
This URL generates the SQL query:

SELECT * FROM funds WHERE category = 'Investments'—' AND purchase = 1

The double dashes sequence indicates an SQL comment. It implies that the rest of the query is a comment. The removes the rest of the query so that the query no longer includes AND purchase = 1. The implication is that all funds are displayed, including funds not purchased.A cyber attacker can then trigger the application to display all the funds in any category, including unknown categories.
https://insecure-website.com/funds?category=Investments'+OR+1=1--
This URL generates the SQL query:
SELECT * FROM funds WHERE category = 'Investments' OR 1=1—' AND purchase = 1

The modified query returns all items were either the category is Investments or 1 is equal to 1. The query will return all funds because one equals one is always true.[24]

Post-Attack Period

In November 2020, Fire Eye, a cyber security professional services firm, stated that it had detected a software intrusion into its systems, and on December 12, 2020, Fire Eye informed Solar Winds that Orion had been compromised.[25] On December 13, 2020, Fire Eye issued a technical analysis of the malicious software in the Orion updates.[26] On December 14, 2020, Solar Winds informed the Securities and Exchange Commission (SEC) of the cyber-attack.[27] On December 15, 2020, Microsoft and its partners acted swiftly, redirecting and preventing malicious network traffic from getting to its intended destination address.[28] On December 16, 2020, the National Security Council (NSC) staff triggered the Cyber Unified Coordination Group

[12] Dina Temple-Raston, *A 'WorstNightmare' Cyberattack: The Untold Story of the SolarWinds Attack*, NATIONAL PUBLIC RADIO (NPR) (Apr. 16, 2021), *available at*https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] Andy Greenberg, *Hacker Lexicon:What Is a Supply Chain Attack?*, WIRED (May 31, 2021), *available at*https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/.
[18] *Id.*
[19] *Id.*
[20] Vijay A. D'Souza, *SolarWindsCyberattackDemandsSignificantFederal and Private-SectorResponse (infographic)*, WATCHBLOG (Apr. 22, 2021), *available at*https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
[21] Black Kite Staff, *The SolarWinds Attack from a Hacker's Point of View*, BLACK KITE (2022), *available at*https://blackkite.com/the-solarwinds-attack-from-a-hackers-point-of-view/.
[22] Port Swigger Staff, *SQL Injection*, PORT SWIGGER (n.d.), *available at*https://portswigger.net/web-security/sql-injection.
[23] *Id.*
[24] *Id.*
[25] Vijay A. D'Souza, *supra*, note 20.
[26] *Id.*
[27] *Id.*
[28] *Id.*

(CUCG) that consisted of the Cyber security and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) that is supported by the National Security Agency (NSA).[29] On December 18, 2020, the CISA briefed Congress about the breach.[30] On December 23, 2020, Crowd Strike, a cyber security professional services company, released the Crowd Strike Reporting Tool, a software application that may be employed to identify cyber risks to the Microsoft Azure Active Directory.[31] The Microsoft Azure Active Directory is a cloud-based identity and management access service that helps employees sign in and access internal and external resources.[32] On December 24, 2020, the CISA released Sparrow, a software application that can detect malicious activity for Microsoft Azure and the Microsoft Office 365 cloud environments.[33]On December 31, 2020, Microsoft reported unusual internal company accounts and unauthorized source code viewing activity.[34] On January 5, 2021, the CUCG opined that the malicious code probably originated from Russia.[35] However, at the time, President Trump hinted that the Solar Winds hack could have come from China, although no evidence was made public.[36] Even so, it should be understood that China has been involved in several high-profile hacks and could have been responsible for the attack.[3738] On January 13, 2021, the White House appointed a Deputy National Security Adviser for Cyber and Emerging Technology (DNSA-CET) who was responsible for guiding the response to the breach by the federal government.[39] On February 8, 2021, the CISA released the Starburst (AR21-039A), and Teardrop (AR21-039B) reports that analyzed the Orion malware.[40] On February 17, 2021, the DNSA-CET stated that Russians were the likely threat actors and that the malware affected nine federal agencies.[41] On February 18, 2021, Microsoft reported that the threat actor was unsuccessful in accessing the company's code repositories in early January.[42]

Table 1. Timeline of the Solar Winds Attack.

Date	Event
September 12, 2019	Malicious code checked whether the SolarWinds server was running a 32-bit or 64-bit processor.
February 2020	Threat actors inserted malicious code into Orion, the SolarWinds production software.
March 2020	SolarWinds began distributing signed software patch updates to Orion that contained the malicious code.
November 2020	FireEye stated that it had detected a software intrusion into its systems.
December 12, 2020	FireEye informed SolarWinds that Orion had been compromised.
December 13, 2020	Fire Eye issued a technical analysis of the malicious software in the Orion updates.
December 14, 2020	Solar Winds informed the SEC of the cyber-attack.
December 15, 2020	Microsoft and its partners redirected and prevented malicious network traffic from getting to its intended destination address.
December 16, 2020	The NSC staff triggered the CUCG.
December 18, 2020	The CISA briefed Congress about the breach.
December 23, 2020	Crowd Strike released the Crowd Strike Reporting Tool.
December 24, 2020	The CISA released Sparrow, a software application to detect malicious activity
December 31, 2020	Microsoft reported usual internal company accounts and unauthorized source code viewing activity.
January 5, 2021	The CUCG opined that the malicious code probably originated from Russia.
January 13, 2021	The White House appointed a DNSA-CETwho was responsible for guiding the federal government's response to the breach.
February 8, 2021	The CISA released StarBurst (AR21-039A) and TearDrop (AR21-039B) which analyzed the Orion Malware.
February 18, 2021	Microsoft reported that the threat actor was not successful in accessing the company's source code repositories.
February 23, 2021	Solar Winds, Microsoft and Crowd Strike testified before the Senate Intelligence Committee regarding the attack.
March 10, 2021	The House Committee on Appropriations and the Homeland Security Subcommittee discussed modernizing the federal response to cyber security.
March 18, 2021	The Senate Homeland Security and Governmental Affairs Committee held a hearing on understanding and responding to the attack.
March 18, 2021	The CISA released its Hunt and Incident Response Program, a tool that permits organizations to discover compromising indicators of malicious activity.
April 15, 2021	The NSA, CISA and the FBI stated that the Russian FIS was the threat actor.
April 19, 2021	The NCS deactivated the CUCG, stating that the lessons learned will help improve the federal government's response to malicious attacks.

On February 23, 2021, Solar Winds, Microsoft, Crowd Strike, and Fire Eye testified before the Senate Intelligence Committee regarding the attack. On February 26, 2021, the House committees on Homeland Security and Oversight and Report conducted a joint hearing regarding the Solar Winds security breach.[43] On March 10, 2021, the House Committee on Appropriations and the Homeland Security Subcommittee discussed modernizing the federal response to cyber security.[44] On March 18, 2021, the Senate Homeland Security and Governmental Affairs Committee held a similar hearing on understanding and responding to the attack.[45] On the same day, the CISA released its Hunt and Incident Response Program, a software tool that allows organizations to discover compromising indicators of malicious activity.[46] On April 15, 2021, the NSA, CISA, and the FBI stated that the Russian Foreign Intelligence Service (FIS) was the threat actor, and on April 19, 2021, the NSC staff deactivated the CUGC, stating that the lessons learned will help to improve federal government responses to malicious attacks.[47]

[29]*Id.*
[30]*Id.*
[31]*Id.*
[32]Justin Hall, Kent Sharkey, Bill Anderson, & Alex Buck, *Whatis Azure Active Directory?*,MICROSOFT CORP. (Jun. 5, 2020), *available at*https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis.
[33]Vijay A. D'Souza, *supra*, note 20.
[34]*Id.*
[35]*Id.*
[36] Saheed Oladimeji, *supra*, note 4.
[37]*Seegenerally*, CSIS Staff, *Significant Cyber Incidents*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (n.d.), *available at*https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[38] Dorothy Denning, *How the ChineseCyberthreat Has Evolved*, SCIENTIFIC AMERICAN (REPRINTED FROM THE CONVERSATION (Oct. 7, 2017), *available at*https://www.scientificamerican.com/article/how-the-chinese-cyberthreat-has-evolved/.
[39]Vijay A. D'Souza, *supra*, note 20.
[40]*Id.*
[41]*Id.*
[42]*Id.*
[43]*Id.*
[44]*Id.*
[45]*Id.*
[46]*Id.*
[47]*Id.*

Why Is the Solar Winds Hack Important?

A critical issue with any software application or platform is how an application provider releases updates and patches to its users.[48] Like many software companies, Solar Winds created installation software that pushed updates and patches to its users.[49] The threat actors were the instructors in a "master class in novel hacking techniques."[50] The hack (1) altered sealed software code,(2) generated a system that employed domain names in choosing victims, and (3) copied the Orion communication protocols to hide the malicious code in plain sight.[51] The hackers sanitized the crime scene so that investigators would have difficulty authenticating the culprit.[52] Even though it was claimed that the Russian FIS was responsible for the hack, the level of expertise was extraordinary, where the code was elegant and innovative.[53] It should be noted that the Russian government denied any responsibility for the Solar Winds hack.[54] Instead, Sergei Naryshkin, the Russian Intelligence Chief, suggested that the United States government was accountable for the attack.[55] According to Bing et. al, Chinese hackers could also have been responsible for the malware because the suspected Chinese threat actors directed an attack against the National Finance Center (NFC), the payroll agency of the United States Department of Agriculture.[56]

How the Solar Winds Attack Could Have Been Prevented

The effective way to prevent an SQL injection attack is to generate a routine that tests SQL queries for phrases such as "1=1." The routine can either be part of a web page or the initial routine executed when control is transferred to the mutual fund server. The issue with the first solution is that web pages are written in Hyper Text Markup Language (HTML).[57] HTML is an interpretive language, meaning an interpreter converts HTML statements into executable code every time it executes a statement. In contrast, in a compiled language, such as Visual Basic, the source code is converted into executable code before the executable code is ever executed on a system.With interpretive languages, performance is a critical issue because the fewer times application source code has to be converted into executable code, the faster the application runs. Thus, for the sake of performance, the routine should probably reside on the application server. The logic of the routine is likely to be quite complex, so placing the routine on the server will not inhibit the website's performance.The suggested routine will work, provided that the routine is called whenever a user enters data into an edit box or requests information by clicking on an object. The limitation of this solution is that an extensive systems analysis of a web application must be conducted so that every edit box or object calls the suggested routine. If an edit box or object does not call the suggested routine, this failure results in a vulnerability that a cyber attacker can exploit. The suggested routine is only as good as its weakest point. Failure of an edit box or object to access the suggested routine is the weakest point in the solution to preventing SQL injections.

The Chinese Connection to the Solar Winds Attack

Solar Winds reported a suspected Chinese attack that did not employ *StarBurst*, the name given to the Solar Winds attack by Solar Winds and Crowd Strike,[58] but rather a different piece of malware that the firm identified as *Supernova*.[59] According to Solar Winds, the Supernova code that was embedded in the Orion Platform was not a malicious supply chain attack.[60] The malware was independently put on a server that required unauthorized access to a customer's network but was designed to seem as if it was included in a Solar Winds product.[61]On September 12, 2019, the Solar Winds attack began with a tiny strip of code that checked to see whether the processor running on a computer was either a 32-bit or 64-bit processor.[62]The threat actor likely employed multiple proof-of-concept code snippets to test whether a supply chain hack was viable. The action would be risk-averse because the hack could still proceed if the victim discovered one proof-of-concept piece of code. After all, the second and additional code snippets would also show that the hack could be successful.

FEDERAL GOVERNMENT AND PRIVATE INDUSTRY'S RESPONSE

This section outlines the federal government's response to the Solar Winds breach. It also highlights the private sector's response to the attack. In evaluating these reactions to the cyber-attack, it should be understood that there are differences between the objectives and goals of the federal government and the private sector. The reason is that private entities are more susceptible to potential litigation from stockholders and stakeholders.

Federal Government's Response

From the timeline listed above, the federal government held numerous agency and Congressional meetings discussing what happened during the Solar Winds attack and what measures could be taken to defend against a future attack. One of the reasons why the Solar Winds attack was significant is because, according to Crowd Strike,the average *dwell time* in 2019 was 95 days or just over three months.Whereas in the Solar Winds attack, fourteen or more months elapsed before the attack was discovered.[63] The dwell time is the difference between when an attack is found and when an attacker initially gains access to a system.[64] In response to the attack, the initial actions of the U.S. Government included: (1) imposing new sanctions against several Russian organizations; (2) attributing the breach to the Russian FIS; and (3) issuing several interagency reports that detailed technical information regarding the tools and methods employed by the Russian hackers (i.e., an NSA-CISA-FBI advisory and the CISA Malware Analysis Report).[65] Even though the intelligence community labeled the Solar Winds attack as an espionage campaign, the federal government framed its response,

---

[48] Chris Jaikaran, *SolarWinds Attack–No Easy Fix*, CONGRESSIONAL RESEARCH SERVICE (Jan. 6, 2021), *available at*https://crsreports.congress.gov/product/pdf/IN/IN11559.
[49] *Id.*
[50] Dina Temple-Raston, *supra*, 12.
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] Mia Jankowicz, *Russia's Intelligence Chief Suggestedwithout Evidence that the US and UK Orchestrated the SolarWinds Hack thatBreached US GovernmentAgencies*, BUSINESS INSIDER (May 18, 2021), *available at* https://www.businessinsider.com/russia-intel-chief-suggests-us-uk-behind-solarwinds-hack-2021-5.
[55] *Id.*
[56] Christopher Bing, Jack Stubbs, Raphael Satter, &Joseph Menn, *Exclusive:SuspectedChinese Hackers UsedSolarWinds Bug to Spy on U.S. Payroll Agency*, REUTERS (Feb. 2, 2021) *available at*https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8.
[57] *HTML & CSS*, W3C (n.d.), *available at*https://www.w3.org/standards/webdesign/htmlcss.
[58] Saheed Oladimeji, *supra*, note 4. The attackwasinitiallycalled*Solorigate*by Microsoft Corp, but the companychanged the name of the attack in March 2021 to *Nobelium*.
[59] SolarWinds Staff, *SolarWinds Security Advisory*, SOLARWINDS, CORP. (Apr. 6, 2021), *available at*https://www.solarwinds.com/sa-overview/securityadvisory#anchor2.
[60] *Id.*
[61] *Id.*
[62] Dina Temple-Raston, *supra*, note 12.
[63] Saheed Oladimeji, *supra*, note 4.
[64] *Id.*
[65] Morrison Foerster Staff, *U.S. GovernmentResponds to SolarWinds Hack, Seeks to Establish New Norms for Cyber Espionage*, MORRISON FOERSTER (Apr. 19, 2021), *available at*https://www.mofo.com/resources/insights/210419-us-government-responds-solarwinds-hack.html.

stating that cyber-espionage campaigns should not attack private-sector computer systems, where the consequence is millions of dollars of mitigation costs that threaten public safety.[66] The problem with this stance is that the federal government and its private contractors are so intertwined that cyber-attacking the federal government necessarily involves cyber-attacking private entities. It is the nature of the military-industrial complex.The Solar Winds breach is an example of Russian, and probably Chinese and other state actors, either friend or foe, exploiting cyber supply chain vulnerabilities. Recently, the Commerce Department distributed an interim final rule to fulfill the provisions of Executive Order 13873 on *Securing the Information and Communications Technology and Services (ICTS) Supply Chain*.[67] Based on the content of Executive Order 13873, organizations should expect increasing supply chain regulation, regardless of whether a firm does business with the federal government.[6869] As for government contractors, they will likely bear the brunt of the additional upcoming federal regulation.[70] In the future, it can be anticipated that the federal government will demand baseline security enhancements such as mandatory two-factor authentication and encryption of sensitive data.[71] Two-factor authentication is a two-step process that employs two different authentication factors or methods to identify an individual.[72] By adding another layer of security beyond a password or pass code, two-factor authentication makes it more challenging, but not necessarily impossible, for an attacker to gain unauthorized access to a system.[73]

Private Industry's Response

It should be remembered that the private sector and not the federal government discovered the Solar Winds attack coupled with a vigorous federal government response.[74] The challenge is to prevent future attacks, quickly find out who the intruder is and how much cyber destruction was done.[75] One issue that is of manifest importance is that there are simply not enough qualified cyber security professionals to address an attack of the magnitude of the Solar Winds attack.[76] Private entities would be well encouraged to expand the market for trained cyber security professionals by increasing their staff requirements and engaging in substantial training efforts.[77] Sharing cyber information with the federal government and other private organizations is also critical in this era where cyber-attacks transcend corporate boundaries.[78] According to Giles, at least five urgent challenges face Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) in light of the Solar Winds attack.[79] First, when a breach has been found, all changes or updates must be rolled back to a known secure state.[80] This is easier said than done. Because the average dwell time in 2019 was 95 days,[81] there is an incentive to roll back changes or updates only three months. In the case of the Solar Winds attack, this would be a mistake because it was documented that the breach lasted for 14 months.[82] What should the rollback date be? The response depends on the length of the dwell time and when the attack was first initiated. This is an open question whose answer depends on the circumstances at hand.Second, Giles opined that CIOs and CISOs should search for ways to limit the inter-connectivity of vendor software by reviewing egress controls, network servers, and internal databases.[83] The problem with minimizing vendor access is that the principles of total quality and just-in-time inventory require the virtually merging buyer and seller communications and databases to ensure low-cost and high-quality products and services.[8485] Third, CIOs and CISOs are responsible for determining the extent of cyber supply chain attacks and the areas within an organization affected by the hack.[86] This is no mean feat, and there is no royal road in determining the breadth of an attack. In some sense, it is a hit-or-miss proposition to discover how extensive was an attack because the secure rollback date is, in most instances, unknown and sometimes unknowableFourth, CIOs and CISOs must balance between short-term innovation against security.[87] This is difficult, given the tremendous market pressure to be first or near the first to market. In marketing strategy, there is a well-known competitive first-mover advantage (FMA) in establishing brand recognition, customer loyalty, and early acquisition of resources before competitors enter a market segment.[8889] This must be considered by companies when addressing cyber security in general and cyber supply chain security in particular. It should be remembered that traditionally the balance has favored FMA and time to market over security. Finally, CIOs and CISOs are responsible for assessing whether supplier code has been breached.[90] According to Giles, the CISA expected to find additional access points as part of their ongoing investigation.[91] In particular, Microsoft stated that it notified at least 40 customers that may have been affected by the Solar Winds attack. Fortunately, Microsoft discovered no evidence indicating that its own systems were used to attack others.[92] This information is heartwarming, even though Microsoft investigations were continuing.[93] Other companies such as Cisco were attempting to identify access points to future supply chain attacks.[94]The result is the need for continuous corporate vigilance. An organization cannot sit on its laurels, thinking that it has done all it can do. Hackers are very clever individuals, and although companies may never catch up to the unauthorized activities of threat actors, they must stay not too far behind.

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Dina Temple-Raston, *Biden Order To Require New Cybersecurity Standards In Response To SolarWinds Attack*, NATIONAL PUBLIC RADIO (NPR) (Apr. 2021), *available at*https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att.
[70] Morrison Foerster Staff, *supra*, note 64.
[71] *Id.*
[72] Linda Rosencrance, Peter Loshin, &Michael Cobb, *Two-Factor Authentication (2FA)*, TECHTARGET(Last updatedJul. 2021), *available at*https://searchsecurity.techtarget.com/definition/two-factor-authentication.
[73] *Id.*
[74] Gordon Bitko, *What Public And PrivateSector Leaders Can Do To Stop The Next SolarWinds Hack*, FORBES (Dec. 22, 2020), *available at*https://www.forbes.com/sites/gordonbitko/2020/12/22/what-public-and-private-sector-leaders-can-do-to-stop-the-next-solarwinds-hack/?sh=4be5ea703814.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] Martin Giles, *The SolarWindsBreach Poses Five Urgent Cybersecurity Challenges For CIOs*, FORBES (Dec. 20, 2020), *available at* https://www.forbes.com/sites/martingiles/2020/12/17/solarwinds-hackers-five-cybersecurity-challenges-for-cios/?sh=33483adf21b6.
[80] *Id.*
[81] Saheed Oladimeji, *supra*, note 4.
[82] *Id.*
[83] Martin Giles, *supra*, note 78.
[84] ROBERTA S. RUSSELL, & BERNHARD W. TAYLOR III, OPERATIONS MANAGEMENT:FOCUSING ON QUALITY AND COMPETITIVENESS (Prentice-Hall, Inc. 2nd ed. 1998).
[85] JAMES R. EVANS, & WILLIAM R. LINDSEY, THE MANAGEMENT AND CONTROL OF QUALITY (South Western CollegePublishing 4th ed. 1999).
[86] Martin Giles, *supra*, note 78.
[87] *Id.*
[88] MICHAEL E. PORTER, COMPETITIVESTRATEGY: TECHNIQUES FOR ANALYZING INDUSTRIES AND COMPETITORS (The Free Press 1980).
[89] MICHAEL E. PORTER, COMPETITIVEADVANTAGE:CREATING AND SUSTAINING SUPERIOR PERFORMANCE (The Free Press 1985).
[90] Martin Giles, *supra*, note 73.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*

LAWS AND POLICIES REGARDING CYBER-ATTACKS

Several federal laws deal with cyber security, privacy, and espionage. This paper briefly outlines some of the more notable laws that have received public attention in recent years. The subsections include discussions on the Economic Espionage Act of 1996, the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999, the Federal Information Security Management Act of 2002, the Modernizing Government Technology Act of 2017, the Setting Every Community Up for Retirement Enhancement Act of 2019, and Executive Order 14017.

Economic Espionage Act of 1996

According to Johnson, the Economic Espionage Act (EEA) of 1996 (Public Law 104–294, 110 Stat. 3488) became law on October 11, 1996.[95] The law addresses industrial espionage or the misappropriation and subsequent acquisition of trade secrets knowingly or with the intent that the theft will profit a foreign government.[96] The penalties for violating the EEA include fines up to $500,000 and imprisonment for a maximum of 15 years for individuals, and fines not to exceed $10 million for organizations.[97] The theft of a trade secret that has been placed in interstate or international commerce is up to 10 years for individuals (no fines) and $5 million for organizations.[98] A trade secret means "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[99] The trade secret owner must take reasonable steps to protect it, and the trade secret must possess economic value where the public cannot readily ascertain it.[100] In general, the protection of the trade secret may or may not be protected by cyber means. In general, the Act does not deal with cyber breaches by a threat actor.

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act (HIPPA) of 1996 is one of the three major cyber security laws. HIPPA created national standards to safeguard sensitive patient health information from being revealed without the consent or knowledge of a patient.[101] The HIPPA Privacy Rule is concerned with disclosing protected health information about individuals by organizations subject to the rule.[102] These individuals and organizations are called *covered entities*.[103] The rule also contains standards that ensure that the health information about an individual is protected while at the same time allowing for the flow of health information so that people receive quality health care.[104] The entities that are covered by the Privacy Rule include healthcare providers, health plans, healthcare clearinghouses, and business associates.[105] A covered entity is allowed, but not required, to employ and disclose protected health information without authorization from a person for various reasons, including, but not limited to, treatment, payment, and when required by law.[106] The HIPPA security rules safeguard a subset of the health information covered by the Privacy Rule.[107] The Security Rule shields the health information that a covered entity creates, receives, maintains, or transmits as an electronic message.[108] This information is called *electronically protected health information* (e-PHI) and cannot be communicated orally or in writing.[109] To comply with the HIPPA Security Rule, a covered entity must: (1) warrant the confidentiality, integrity, and availability of all electronically protected health information; (2) detect and protect the information against threats; (3) prevent unauthorized uses and disclosures of health information; and (4) certify that a covered entity's employees comply.[110] As one can see, it is e-PHI that may be the object of a cyber-attack.

Gramm-Leach-Bliley Act of 1999

The Gramm-Leach-Bliley Act (GLBA) of 1999 is the second of the three major cyber security laws currently in place. It is also known as the Financial Modernization Act of 1999 because it controls how financial institutions handle the private information of individuals.[111] There are three sections in theGLBA, the Financial Privacy Rule, the Safeguards Rule, and the Pretexting provisions.[112] The Financial Rule controls how financial information is collected and disclosed.The Safeguards Rule states that financial institutions are required to implement a security program to protect financial information.And thePretexting provisions forbid pretexting or obtaining financial information using false pretenses.[113] The GLBA also demands that financial institutions notify their customers regarding their privacy policies explaining their information-sharing practices.[114] Although the GLBA repealed significant parts of the Glass-Steagall Banking Act of 1933 and the Bank Holding Company Act of 1956, its purpose was to warrant that financial institutions and their affiliates protect the confidentiality of personally identifiable information (PII) collected in paper or electronic form, thereby complying with rigorous data security guidelines.[115] The data covered by the GLBA includes addresses, bank accounts, biometric data, birth dates, car dealers, credit history, education level and performance, employment data, Internet data, geolocation data, names, personal income, Social Security data, and tax information.[116] It also safeguards any inferences drawn from this data. Covered entities consist of accountants, ATM operators, car rental companies, courier services, credit reporting companies, credit unions, debt collectors, financial advisory firms, hedge funds, non-bank mortgage lenders, payday lenders, property appraisers, real estate firms, retailers, stockbrokers, tax preparers, and universities.[117] A financial institution that does not comply with the GLBA may be fined up to $100,000 per violation, while its officers and directors are subject to fines of up to $10,000, five years in prison, or both.[118] One of the benefits of the GLBA is that

[95] LEIGHTON JOHNSON, IN SECURITY CONTROLS EVALUATION, TESTING, AND ASSESSMENTHANDBOOK (Academic Press 2nd ed. 2020), https://doi.org/10.1016/C2018-0-03706-8.
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.* at 9-25.
[100] *Id.*
[101] CDC Staff, *HealthInsurancePortability and AccountabilityAct of 1996 (HIPAA)*, CENTERS FOR DISEASE CONTROL AND PREVENTION (Last reviewed Sep. 18, 2018), *available at*https://www.cdc.gov/phlp/publications/topic/hipaa.html.
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] Gary Kranz, *Gramm-Leach-BlileyAct (GLBA)*, TECHTARGET(Jun. 2021), *available at*https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act.
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*

financial institutions have become well aware of the security risks posed by hackers that desire to obtain financial information for illicit gain.[119] The GLBA covers financial institutions and would not have addressed the Solar Winds breach because Solar Winds was not a covered entity.

Federal Information Security Management Act of 2002 and 2014

The Federal Information Security Management Act (FISMA) is the third primary cyber security law in the United States. The original Act of 2002 was included in the E-Government Act (Public Law 107-347) of 2002, was passed in December of that year.[120] FISMA 2002 required that federal agencies develop, document, and implement an information security program that sustained the agency's operations and assets, even when those operations and assets were run by other agencies, contractors, or other sources.[121] FISMA of 2014 amended FISMA of 2002 by strengthening the employment of continuous monitoring systems while at the same time reducing the overall reporting requirements and increasing an agency's focus on the compliance and reporting of breaches in security.[122] FISMA 2014 also obliged the Office of Management and Budget (OMB) to amend and revise OMB Circular A-130, thereby promoting changes in reporting as technology progressed.[123] Together with the Paperwork Reduction Act (PRA) of 1995 and the Information Technology Management Reform Act (ITMRA) of 1996, also known as the Clinger-Cohen Act, FISMA of 2014 stressed a risk-based policy for cost-effective security.[124] Via Circular A-130, the OMB demanded that agencies (1) plan for security, (2) ensure that specific individuals were responsible for security, (3) review security controls periodically, and (4) authorize system processing periodically before operations begin.[125] FISMA of 2014 ensured that federal agencies protect agency information against unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by an agency or one of its contractors for the agency.[126] FISMA of 2014 also underscored that those federal agencies had to comply with NIST security standards and guidelines.[127] However, from a cyber security perspective, FISMA of 2002 and 2014 does not address the security needs made plain by the Solar Winds attack. Both Acts focus more on how a federal agency protects its data than how it interacts with the software firm whose application protects agency data. Simply stated, FISMA of 2002 and 2014 are not sufficiently specific to deal with the Solar Winds breach.

Modernizing Government Technology Act of 2018

The Modernizing Government Technology Act (MGTA) of 2018 is a vital component of the National Defense Authorization Act (NDAA) that was passed on December 12, 2017.[128] The Act allowed federal agencies to invest in modern technological solutions that improved the delivery of services to the public, ensure the security of sensitive systems and data, and save taxpayer money.[129] The MGTA provided for 2018 and 2019 an annual Technology Modernization Fund of $250 million for financial, operational, technological projects.[130] MGTA also created a Technological Modernization Board whose purpose was to assess proposals and recommend the GSA Administrator to fund specific projects.[131] The MGTA mandated developing a proposal submission process and required the OMB to provide additional guidance to federal agencies.[132] Finally, MGTA authorized all Chief Financial Officer's Act (CFOA) of 1990 agencies to generate an Information Technology working capital fund to (1) improve, retire, or replace existing information technology systems including cyber security systems, (2) transition legacy systems to the commercial cloud, (3) assist and support risk-based and cost-effective technologies that address cyber threats, (4) reimburse any funds transferred to an agency from the Technology Modernization Fund, and (5) increase funds for any program, project, or activity not denied or restricted by Congress.[133] Even so, MGTA in no way deals with the needs that were exposed by the Solar Winds attack. The Act helps federal agencies develop better technological solutions but does not explicitly address the issues and damages experienced because of the breach.

Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2019

The Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology (SECURE IT) Act of 2019 required the Secretary of Homeland Security to "generate a security vulnerability disclosure policy, to establish a bug bounty program for the Department of Homeland Security, to amend title 41, United States Code, to provide for Federal acquisition supply chain security, and for other purposes."[134]The Act consisted of two titles, where Title I addressed the Department of Homeland Security matters and Title II dealt with the federal acquisition of supply chain security.[135]The Act was concerned with identifying and promulgating best practices and procedures and reporting on vulnerabilities discovered.[136]From a cyber security perspective, SECURE IT needs to be strengthened so that federal agencies can work effectively with private actors in mitigating and preventing cyber-attacks when and after an attack occurs.

Executive Order 14017

When the Solar Winds cyber-attack was discovered in November 2020 by Fire Eye,[137] it became readily apparent that both the federal government and Solar Winds had dropped the ball. In 2019, the average dwell time was 95 days, whereas the dwell time for the Solar Winds hack was approximately 14 months.[138] The eleven-month difference in dwell time was significant from both cyber security and statistical perspectives. Members of Congress and those in President Biden's administration recognized that something needed to be done, and done quickly at that.On February 24, 2021, President Biden issued Executive Order 14017 entitled, *Executive Order on America's Supply Chains*.[139] Executive Order 14017 emphatically declared that the:"United States needs resilient, diverse, and secure supply chains

[119] *Id.*
[120] NIST Staff, *Federal Information Security ModernizationAct (FISMA) Background*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Updated Sep. 28, 2021), *available at*https://csrc.nist.gov/projects/risk-management/fisma-background.
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] Mick Mulvaney, *Implementation of the ModernizingGovernment Technology Act*, OFFICE OF MANAGEMENT AND BUDGET (Feb. 27, 2018), *available at*http://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf.
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *H.R.7327 - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*, CONGRESS.GOV (Dec. 21, 2018) *available at*https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf.
[135] *Id.*
[136] *Id.*
[137] Vijay A. D'Souza, *supra*, note 20.
[138] Saheed Oladimeji, *supra*, note 4.
[139] Joseph Biden, *ExecutiveOrder on America'sSupplyChains*, THE WHITE HOUSE (Feb. 24, 2021), *available at*https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services. Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs."[140] From a cyber security perspective, Executive Order 14017 was what was exactly needed. It was an administrative policy that coordinated the efforts of the various Cabinet departments regarding how to accomplish supply chain security.[141] The Order charged the Assistant to the President for National Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP) to work together in ensuring that the executive branch synchronizes their actions through the interagency process identified in National Security Memorandum, dated February 24, 2021 (Renewing the National Security Council System).[142] The Order obliged the heads of federal agencies to consult outside stakeholders, such as industry leaders, academics, non-governmental organizations, communities, labor unions, and State, local, and Tribal governments to fulfill the policies contained in the Order.[143] Executive Order 14017 looked at the United States economy as a whole by providing both general and specific guidelines to protect American supply chains from digital threats. In particular, the Order gave seven specific recommendations to ensure that the Solar Winds attack would not happen again. The content of these recommendations was quite extensive and will be discussed below.

SUPPLY CHAIN SECURITY ISSUES

In this section, supply chain security is defined with the elements of cyber supply chain security discussed. Examples of supply chain security are provided, and a high-level perspective of supply chain security is outlined. In the second subsection, a cyber supply chain attack is discussed, where logic bombs and the man-in-the-middle attack are examined in some detail.

Supply Chain Security Explained

In supply chain management, supply chain security deals with the risk management of external suppliers, vendors, logistics, and transportation.[144] The idea behind supply chain security is to identify, analyze, and then mitigate intrinsic risks in working with other entities contained in a supply chain.[145] Supply chain security consists of the physical security of products and cyber security for software and services.[146] Because supply chains are diverse, there is no standardized set of supply chain guidelines or best practices.[147] However, an effective supply chain strategy demands that firms adhere to practical risk management principles and cyber defense strategies while addressing government protocols and regulations.[148] According to the National Institute of Standards and Technology (NIST), secure cyber supply chain principles include (1) developing defenses that presumed that the firm's supply chain would be breached, (2) understanding that cyber security is not merely a technological problem, but a people, process, and knowledge problem, and (3) removing the gap between physical security and cyber security.[149] Cyber supply chain risks are extensive and cover issues such as:

- Third-party service providers that possess physical or cyber access to information systems or source code;
- Poor information security practices by suppliers;
- Compromised hardware or software purchased from vendors;
- Software security vulnerabilities that exist in supply chain or supplier systems;
- Counterfeit hardware or hardware containing embedded malware; and
- Third-party data storage or data aggregators.[150]

Although best practice tactics can be pretty detailed,[151] five general-purpose supply chain security strategies can act as a guiding framework that includes (1) training of all employees regarding best practices; (2) limiting permissions; (3) segmenting networks; (4) ensuring redundancy; and (5) recognizing that cyber security supply chain security is essential.[152]

A Supply Chain Attack Described

According to Saydjari, a cyber supply chain attack assaults the integrity of a supply chain.[153] A threat actor strikes an application's development or distribution channel by inserting malicious code that may be activated later when the application is deployed on a customer site.[154] Essentially, a cyber supply chain attack is a *logic bomb*, where a logic bomb is a "string of malicious code inserted intentionally into a program to harm a network when certain conditions are met."[155] The term is derived from the notion that code "explodes" when it is triggered by a specific event, such as a pre-specified date or time, the removal of a given record, or when launched by a threat actor.[156] The damage potential of a logic bomb varies, but it can severely cripple or terminate an entity.[157] In this case, a threat actor invoked the logic bomb and may have severely crippled both Solar Winds and its customers.Another feature of the Solar Winds attack was that it employed a *man-in-the-middle* attack. A man-in-the-middle attack occurs when a threat actor places themselves between a sender and receiver of data, where the threat actor is unknown to both parties.[158] The threat actor collects the sender's communication, changes it, and transmits the altered communication to the receiver, attempting to dupe the receiver into believing that the message came directly from the sender.[159] The issue with the man-in-the-middle attack is that the confidentiality and integrity of the data are lost because a threat actor can recalculate a checksum before sending the altered data.[160] A checksum is "a sum derived from the bits of a segment of computer data that is calculated

[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] Gavin Wright, &Sarah Lewis, *Supply Chain Security*, TECHTARGET(Apr. 2021), *available at* https://searcherp.techtarget.com/definition/supply-chain-security.
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] NIST Staff, *Best Practices in Cyber Supply Chain Risk Management*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (n.d.), *available at*https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.
[150] *Id.*
[151] *Id.*
[152] Shannon Flynn, *5 Strategies for Cybersecurity in Supply Chain Management*, EPSNEWS (Aug. 27, 2021), *available at*https://epsnews.com/2021/08/27/5-strategies-for-cybersecurity-in-supply-chain-management/.
[153] O. SAMI SAYDJARI, ENGINEERING TRUSTWORTHYSYSTEMS:GETCYBERSECURITY RIGHT THE FIRST TIME (McGraw-Hill Publishers 2018).
[154] *Id.*
[155] Rahul Awati, &Laura Fitzgibbons, *Logic Bomb*, TECHTARGET(n.d.), *available at*https://searchsecurity.techtarget.com/definition/logic-bomb.
[156] *Id.*
[157] *Id.*
[158] O. Sami Saydjari,*supra*, note 152.
[159] *Id.*
[160] *Id.*

before and after transmission or storage to assure that the data is free from errors or tampering."[161] The receiver would never know that the data had been corrupted because it would calculate the same checksum sent to them by the threat actor and not the original sender.[162] A pair of cryptographic functions, called *sign-and-verify*, should be employed to prevent a man-in-the-middle attacker from just recalculating the checksum and passing the resulting data onto the receiver. The signing process uses the input data, and the sender's private key is called a *digital signature*.[163] The receiver employs a corresponding verification process that uses the digital signature and the sender's public key, where the result is valid if the data matches the digital signature or invalid if there is a difference.[164] Thus, a digital signature may defeat a man-in-the-middle attack. It can probably be inferred from the facts provided about the Solar Winds attack is that the company likely used checksums to ensure the integrity of customer data. It is also reasonable to conclude that Solar Winds simply failed to employ digital signature technology in Orion.

RECOMMENDATIONS AND LESSONS LEARNED

This section is divided into three subsections. The first subsection addresses the recommendations and lessons learned by the federal government regarding the Solar Winds cyber-attack. The second subsection deals with the proposals and lessons learned by the private sector. The final subsection focuses on the suggestions and the lessons learned from a legal perspective.

From the Federal Government's Perspective

On February 24, 2021, President Biden issued Executive Order 14017 that contained in Section 5 seven specific recommendations in dealing with supply chain security.[165] The Executive Order required that the Departments of Commerce, Energy, Defense, and Health and Human Services generate initial reports, identifying risks in semiconductor manufacturing and advanced packing supply chains, in the high-capacities supply chains, critical minerals and other strategic materials supply chains, and the pharmaceuticals and active pharmaceutical ingredients supply chains, respectively.[166]Within one year from the date of the Order, the Secretaries of Defense, Health and Human Services, Commerce, Energy, Transportation, and Agriculture were required to create reports regarding the supply chain threats in their areas of dominion, such as but not limited to, critical or essential goods and materials, manufacturing capabilities, defense, intelligence, health, climate, education, economics, and geopolitics.[167] Even so, the year delay in implementing supply chain mitigation by the federal government has provided threat actors with a significant window to instigate another supply chain cyber-attack.The Order also required APNSA and the APEP to coordinate with the leaders of the appropriate federal agencies to provide additional reports as necessary and make recommendations concerning the:

- Strengthening America's supply chains;
- Ensuring that supply chain analyses and actions are more effective from a statutory, regulatory, procedural, and institutional perspective;
- Establishing a quadrennial supply chain review about processes and timelines;
- Engaging allies and partners in coordinating diplomatic, economic, security, trade policy, informational, and other actions;
- Insulating supply chain analyses form conflicts of interest, corruption, or the appearance of impropriety to promote integrity and public confidence;
- Reforming domestic and international trade rules and agreements;
- Educating a company's workforce in cyber security principles; and
- Specifying steps to assure that the government's supply chain policy (1) supports small businesses, (2) prevents monopolies from occurring, (3) considers climate and environmental impact,(4) promotes economic growth in communities of color and distressed areas, and (5) disperses economic activity across the United States.[168]

These strides are significant because they may translate into direct action by government agencies and private sector organizations.

From the Private Sector's Perspective

According to Novinson, there are twelve technical lessons to be learned from the Solar Winds breach.[169] First, firms should dump on-premise Microsoft Active Directory because an on-premise Active Directory must be synchronized with its cloud counterpart.[170] Given the complexity, the Active Directory is just too difficult to protect. Second, a firm needs to know the origin of the code.[171] The Solar Winds attack forced companies to question vendor build cycles and scrutinize the software that they are using. Guardrails should be built around corporate code vaults because hackers perceive corporate software's the crown jewels of an organization.Third, companies should inspect suppliers continuously.[172] This is important because most businesses examine a vendor's security practices when first agreeing to do business with them but then do not analyze these security practices periodically. Also, rather than merely asking simple security questions, firms should ask penetrating questions about data security to warranty supplier security procedures. Fourth, entities should track and test all components employed in their products.[173] It is critical that organizations clearly understand and appreciate the variety of IT and cyber infrastructure components. Vendors should also track and trace the parts or applications delivered to a customer, periodically testing and evaluating each element.Fifth, businesses should rigorously examine the traffic leaving their networks.[174] Corporations should possess a similar arduous protection rule for traffic leaving their network for traffic entering their network. According to Novinson, if companies had configured their serves to only permit access by known organizations, the effect of the Solar Winds attack would have been contained.[175] Sixth, organizations should break an infected supply chain as soon as possible because it is difficult to reconstruct what happened during a breach.[176]Suppose a firm gives third-party privileged access to its crown jewels of data. In that case, the company should build extensive security around the third-party software to prevent breaches like the Solar Winds hack.

[161] *Checksum*, MERRIAM-WEBSTER DICTIONARY (n.d.), *available at*https://www.merriam-webster.com/dictionary/checksum.
[162] O. Sami Saydjari,*supra*, note 152.
[163] *Id.*
[164] *Id.*
[165] Joseph Biden, *supra*, note 138.
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] Michael Novinson, *12 LessonsLearned from SolarWindsBreach: RSA Conference*, THE CHANNEL: CRN (May 21, 2021), *available at*https://www.crn.com.au/news/12-lessons-learned-from-solarwinds-breach-rsa-conference-564841.
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*

Seventh, companies must understand where their data is located.[177] Organizations process and protect large amounts of data. Suppose they do not appreciate who accesses the vast amounts of data that are under their protection. In that case, they will simply be unaware when a hacker obtains their data for nefarious ends. Companies should insist on instituting a zero-trust policy enclosing their most privileged accounts and constantly monitor the Active Directory to spot its weaknesses. Eighth, it should be remembered that an organization cannot stop what it cannot see.[178] Firms should comprehend every process, network connection, and system change within their environment, indexing and searching events with intelligence. In other words, understand how an adversary will likely take a corporate asset.Ninth, firms should increase network visibility and segmentation to identify what assets are currently being employed to confirm the priority of critical assets.[179] Because Solar Winds publicized the attack, their customers and other third parties strengthened their security programs, mapped out what needed to be protected, and focused on finding misconfigured software patches, so that threat actors found it more difficult to gain unauthorized access. Tenth, entities should insist that the right or correct security architecture is firmly in place.[180] Although it is unrealistic for a firm to audit all of its vendors and for a supplier to have all their customers audit them, by prioritizing what vendors to audit, a company could take a balanced approach to security, ensuring that there is a zero-trust policy in place for the high-profile vendors by presuming that the vendor software is likely infected. The burden of proof is on the supplier to demonstrate that their software is not infected.Eleventh, organizations need to stress security during an application development process.[181] Audit trails indicating how a firm deals with internal and external cyber threats are critical. The software development process is quite vulnerable to a hacking attack because once the development process is completed, the entity may not go back and audit its code. It may assume that the code is correct and no malware is present. Finally, an organization may want to reconsider using firewalls and other traditional security appliances seriously.[182] The reason is quite simple. Under the conventional access model, once a person has gotten beyond a firewall, they may have unfettered access to a corporate network. Novinson recommended connecting users directly to only the applications that they are privileged to use.[183] This Act would defeat the firewall-based approach to security.

From a Legal Perspective

When an organization suffers a cyber-attack, there are various legal issues that counsel should address when negotiating a cyber contract.[184] An organization should ask itself what happens when a security solution fails. First, the vendor selection process should be reevaluated by examining who in the organization selected a supplier, what criteria were employed in the selection process, and whether supplier security was part of the selection process by ensuring that a formal review process exists. The firm should perform an independent risk analysis of a supplier's security position, where counsel is proactive in the process by advising their client only to choose vendors that comply with government and industry security regulations. In a Request for Proposal (RFP) process, a company should obtain security commitments from vendors during negotiations.[185] Counsel should insist that the proper security requirements are contained in supplier contracts. Counsel should suggest that existing contracts be reviewed and renegotiated if appropriate and feasible. The Solar Winds attack demonstrated that contractually requiring that vendors take proper precautions is insufficient. The security posture of a supplier should be validated via independent reviews and audits if practicable. Counsel should demand that audit rights be included in contracts as well as notice of a security breach.[186] Counsel should advise their clients to have their names removed from customer lists. This action alone will hinder threat actors from determining what suppliers a firm employs.[187] Counsel should point out that all-in-one solutions such as Solar Winds imply that threat actors need only use a single point of entry in attempting to gain control over an entire system. A well-managed diversified set of IT tools reduces the risk of unauthorized access.[188] Users typically demand faster, more integrated technology with additional functionality because, in IT, performance is the name of the game. Such solutions increase the complexity of multifaceted systems, thereby making them more challenging to secure. Counsel should collaborate with an IT department to (1) analyze the risks associated with complex software tools, (2) promote cyber security training for all of a firm's employees, and (3) show the adverse effects of a breach.[189] The corporation should review all user application privileges to ensure that users have the least privileges needed to do their job. It should be remembered that applications with administrative access can robotically act as a proxy for a user, system, or application and that this is precisely how the Solar Winds hack occurred. Counsel should promote and participate in periodic privilege reviews.[190] Finally, counsel should ensure that an organization has adequate policies and resources in place so that the entity can quickly respond to a data breach. Counsel should possess legal expertise regarding breach-notification, privacy laws, and third-party incident response organizations.[191]

CONCLUSION

The Solar Winds attack was a wakeup for the United States in particular and the international business community in general. The length of the dwell time and the extent of organizations infected demonstrated the resolve of threat actors to invade and corrupt the federal government and a variety of American industries. Industries that are essential or critical to the American economy were seriously affected by the breach. There is an adage that eternal vigilance is the price of freedom. In the ever-changing economic and technological environment these days, the saying takes on new meaning. Suppose the United States government, state governments, and even local governments, along with private industry, want to be effective in the future. In that case, they must establish barriers so that would-be hackers find it difficult to invade their systems and monitor these barriers with vigor. Nothing less than that will suffice.

DONALD L. BURESH BIOGRAPHY

Donald L. Buresh earned his Ph.D. in the management of engineering and technology from North central University. His dissertation

[177] *Id.*
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] Carina Mendola,& Brett Creasy, *LessonsLearned from the SolarWinds Hack: WhatWentWrong& How Can Lawyers Help Mitigate the Risk of Cyberattacks*, ASSOCIATION OF CORPORATECOUNSEL (n.d.), *available at*https://www.acc.com/sites/default/files/2021-02/Lessons%20Learned%20from%20the%20SolarWinds%20Hack.pdf.
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] *Id.*

assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School). Dr. Buresh received an M.P.S. in cyber security policy and an M.S. in cyber security concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He is a member of the Florida Bar, has over 25 years of paid professional experience in Information Technology, and has taught economics, project management, and negotiation at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée and foil at a local fencing club. He is a member of the Florida Bar.

MISCELLANEOUS CONSIDERATIONS

Author Contributions: The author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement : Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Acknowledgements: Not applicable.

ABBREVIATIONS:

The following abbreviations are used in this manuscript:

APEP	Assistant to the President for Economic Policy
APNSA	Assistant to the President for National Security Affairs
CIO	Chief Information Officer
CISA	Cyber security and Infrastructure Security Agency
CISO	Chief Information Security Officer
CUCG	Cyber Unified Coordination Group
DNSA-CET	Deputy National Security Adviser for Cyber Emerging Technology
EEA	Economic Espionage Act
e-PHI	Electronically Protected Health Information
FBI	Federal Bureau of Investigation
FIS	Russian Foreign Intelligence Service
FISMA	Federal Information Security Management Act
FMA	First Mover Advantage
GLBA	Gramm-Leach-Bliley Act
HIPPA	Health Insurance Portability and Accountability Act
MGTA	Modernizing Government Technology Act
NDAA	National Defense Authorization Act
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
RFP	Request for Proposal
SECURE IT	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act
Solar Winds	Solar Winds Corp.

****