International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

Enterprise Risk Management Post Solar Winds Hack

Dr. Shetia C. Butler Lamar
Savannah State University
USA

Michelle Kuralt
Columbus State University
USA

Carolyn Zidor-Guerrier
Columbus State University
USA

ABSTRACT

Along with the rising demand for companies to facilitate business functions more efficiently, information technology has increasingly become a vehicle to bring about the convenience and efficiency that companies require to promote effective business operations. With such reliance upon information technology solutions comes the potential for companies to become more vulnerable to possible security incidents with their increased reliance upon third-party vendors for software solutions.

This paper seeks to explore the software company SolarWinds and analyze its 2020 security breach. This paper will discuss how the SolarWinds breach occurred, how IT Security Professionals perceived it, and the vulnerabilities within the SolarWinds system before the breach. It will also analyze and evaluate the lessons learned from the SolarWinds breach and explore security measures implemented after the attack

Introduction

Overview of SolarWinds company and breach

SolarWinds is a company focused on developing software for businesses to help them manage their networks, systems, and Information Technology infrastructure. The company's products include network management, systems management, database management, IT security, and application management. (SolarWinds, 2021) SolarWinds creates network monitoring and logs analysis tools to detect performance issues and data breaches (SolarWinds, 2021). In the year 2020, the company was the subject of a data breach which led to one of the most sophisticated and broad-reaching attacks in cybersecurity history. The company had 33,000 customers who used their software system, Orion. However, approximately 18,000 customers were affected since they had downloaded the update that was available at the time (Jibilian & Canales, 2021). Private companies like Microsoft, Cisco, Intel, and Deloitte were breached along with other organizations like the California Department of State Hospitals and Kent State University (Jibilian & Canales, 2021). There were multiple branches of the United States government among their affected customers (CISA,2021), including the Department of Homeland Security and the Treasury Department (Jibilian & Canales, 2021).

Literature Review

How did the attack happen?

The U.S. Government has officially attributed the attack to Russia and has issued sanctions against Russia for it (Holland, 2021). The Russian advanced persistent threat group infiltrated the SolarWinds network monitoring software and used that foothold to monitor the affected organizations. (Center for Internet Security, 2021). Hackers broke into their system and added malicious code into the company's software system, Orion (Jibilian & Canales, 2021). That code created a backdoor to their customers' systems, and it allowed hackers to install even more malware. As a result, it allowed hackers to spy on organizations(Jibilian & Canales, 2021**).** The hackers even obtained access to Department of Homeland Security email accounts. (Associated Press, 2021) The attack was especially nefarious given that the SolarWinds software was relied upon by these enterprises to detect breaches; instead, the software introduced a new vulnerability into the networks it monitored. The hackers infiltrated some networks as far back as December of 2019, but were only discovered in December of 2020 (Center for Internet Security, 2021).

MITRE has assigned the vulnerabilities associated with the SolarWinds hack the CVE-IDs of CVE-2020-10148, CVE-2020-13169, CVE-2020-14005, and CVE-2020-14007 (Center for Internet Security, 2020, MITRE, 2020). The malicious code that was used is known as SUNBURST (Wolf et al, 2021). It can lay dormant and hidden while it is inactive, and it creates backdoors when activated that can allow third parties to gain unauthorized access to a software ecosystem (Wolf et al, 2021). The potential impacts of hacks facilitated using SUNBURST are significant given that once a backdoor gets created, hackers can pose future threats by subsequently

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

accessing the infected system to potentially navigate other network areas, establish additional persistence, and orchestrate other malicious schemes. Perhaps most threatening, SUNBURST can function in many cases even after the malware gets removed (Wolf et al., 2021).

CrowdStrike, a security firm investigating the hack, mentioned a third malware strain, Sunspot, was part of the attack along with SUNBURST and Teardrop. The security firm believed that Sunspot was the malware that was firstly used in September 2019, when hackers first breached the internal network of SolarWinds (Cimpanu,2021). This malware ran on the build server to build commands. When it detected a build command, Sunspot would then replace the source code files inside the Orion app with apps loaded with SUNBURST. Such an act prompted Orion app versions to install SUNBURST as well. Once installed, SUNBURST was activated inside the internal networks of SolarWinds customers. It collected data on the victims and sent information back to the hackers (Cimpanu, 2021). If a victim seemed significant enough to compromise, Teardrop was deployed on these systems, and SUNBURST removed itself from insignificant or too high-risk of networks (Cimpanu, 2021). Once the attackers were established on affected systems, they started exploiting vulnerabilities in Microsoft's code to move within networks, gain access to emails, and gain access to other sensitive information (Bajak, 2021).

How did Security Professionals perceive the attack?

Members of the IEEE Security & Privacy editorial board described the attack as the result of inadequate cyber defenses, an exploit of insiders, and an exploit of privileges in the software supply chains (Peisert et al., 2021). These professionals pointed out several revelations about the attack including that: network management software is not secure, adding more tools does not add enhanced security, security procedures are designed for first-party software, and that software supply-chain attacks are as important as,if not more importanthan hardware supply-chain attacks (Peisert et al, 2021). They also stated that although combining software code and libraries from various sources may be a good approach for developing tools quickly and inexpensively; it may not be quite as effective with regard to developing tools securely. (Peisert et al, 2021).

Bruce Schneier, a cybersecurity professional, stated that the software that is managing our critical networks is not secure because the market does not reward security (Peisert et al., 2021). Hamed Okhravi, another cybersecurity professional, indicated that with every new tool, while it might reduce parts of the attack surface, it also adds a new attack surface: vulnerabilities within the tool itself become a new possible vector of compromise for the system (Peisert et al., 2021). A system can likely become more secure by removing its unnecessary services, libraries, and features, to shrink its attack surface. (Peisert et al., 2021) Carl Landwehr, another professional, offered that a possibility for preventing such attacks might be to develop tools that would help consumers of updates assess their security more deeply than merely checking that a digital signature is valid (Peisert et al.,2021). From cybersecurity professional Mohammad Mannan's perspective, security products should not harm and should be designed with failure in mind identical to the scrutiny placed on the development of medicines. (Peisert et al.,2021) In another observation, James Bret Michael indicated that although precautionary measures must be applied in response to the SolarWinds attack, overreaction by governments could have a profoundly negative effect on global innovation (Peisert et al., 2021). Therefore, new approaches to security should be explored "in the near- (e.g., cloud hypervisors pushing security rather than individual customers patching or not), mid- (e.g., zero-trust, or something like it), and long-term (e.g., quantum-based approaches)" (Peisert et al., 2021). A market security requirement needs to get established to address motivation (Peisert et al., 2021).

Details

SolarWinds' Existing Software Supply Chain Vulnerabilities

Korolov (2021) defined a supply chain attack as an attack that occurs when someone infiltrates a targeted system through an outside partner or provider with access to the targeted network systems and data. In this case, SolarWinds's organization was breached to gain a foothold in the organizations it supplied software to (Sayegh, 2021). Vulnerabilities within Microsoft's code allowed for significant damage once the attackers were within the affected networks (Bajak, 2021). The exploitation of the intrinsic trust placed in Microsoft products is yet another example of supply chain attacks (Bajak, 2021). Supply chain attacks rely upon the built-in trust given to the third party (Sayegh, 2021). Korolov (2021) noted that any company that provides software or hardware for other organizations could become potential targets for attackers. Korolov (2021) further observed that even security vendors could become potential targets; as an example, FireEye got targeted during the SolarWinds attack. Microsoft itself was infiltrated during the SolarWinds hack and had part of its source code stolen (Bajak, 2021). Commercial software is not the only target of such attacks. Open-source software happened to be an issue for enterprises. These attackers do not have to wait for a vulnerability to appear in open-source software since they can choose to compromise the development or distribution process in the open-source (Korolov, 2021).

According to Wolff et al. (2021), the burden of security is not the sole responsibility of the software vendor and companies that directly employ their systems. In fact, contractors who connect to these systems also have a responsibility to support the supply chain security by establishing an awareness of potential threats through information gathering, analysis, and implementing risk mitigation and remediation actions. In regard to supply chain attacks, contractors should take steps to manage and mitigate

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

cybersecurity supply chain risk. This can be accomplished by establishing an awareness of the relative cybersecurity laws, regulations, and standards. They should also review their policy and contractual obligations about protecting sensitive and proprietary government and business information as outlined by various levels of government (Wolff et al., 2021).

Wolff et al. (2021) presented the supply-chain security risks faced by contractors in three categories. They spoke of the failure of maintaining complete, current inventory of subcontractors accessing sensitive data and information, and how data and information, are protected (Wolff et al, 2021). There is also a lack of established processes for risk assessment and an absence of developed risk-based and cybersecurity supply-chain risk mitigation and remediation strategy (Wolff et al, 2021). Therefore, when it comes to the topic of supply-chain security, contractors should assume a shared responsibility and seek to maintain appropriate access controls, risk assessments, and risk management plans to secure their assets.

Lessons Learned from the SolarWinds Attack

Cybersecurity experts need to be involved at every level of Enterprise Architecture planning. These experts can provide valuable insight into security issues related to planning, procurement, implementation, and monitoring (Abadir, 2021). Cybersecurity experts may anticipate security issues that could arise and can offer safer alternatives. There is a plethora of cybersecurity tools out there. Some of these tools may provide unintended overlapping services with pre-existing products. They can also introduce new risks which the enterprise is not prepared to handle. The intrinsic trust granted to the third and fourth parties is an inherent weakness that can get exploited. An enterprise may be a veritable cyber fortress, but all the defenses may be for naught if third parties are given the keys to the kingdom and can bypass the cyber defenses. Too many enterprises focus exclusively on perimeter defense and not enough on defense in depth. The zero trust model discussed later in this paper addresses a potential solution to this problem.

Applying cybersecurity best practices is significant. Kevin Thompson, a former SolarWinds CEO, testified before Congress and stated that one of the ways the company may have gotten breached was because an intern had the weak password of "solarwinds123" for a file transfer server. The intern posted the password online, and it remained there for two years (Sands, 2021). The former CEO also theorized that the company could have gotten breached was due to brute-force compromises of passwords (Sands, 2021). Industry best practices should not be overlooked and could be significant in assisting enterprises to remain secure. Enterprises should encourage the use of strong passwords and the implementation of password changes. Former employees ' passwords should get deleted in the system, and enterprises should use account lockouts after multiple incorrect password guesses. They should also enforce multi-factor authentication and have acceptable use policies against posting passwords online.

Discussion

Overview of Security Measures in Response to the SolarWinds Attack

With regard to the security measures that have resulted from the SolarWinds attack, the extant literature suggests that more work must be done to prevent and mitigate risks. The following suggestions have been made: applying a zero trust model, increasing the scrutiny related to cybersecurity and enterprise security, requiring vendor compliance audits, developing new laws, enhancing levels of software development, understanding the implications that previous attacks have on organizations, enhancing internal policies and procedures, and contractor management and mitigating supply chain risks.

Zero Trust

The zero trust model includes some concepts such as network segmentation, strong authentication measures, continuous monitoring, and the principle of least privilege that cybersecurity professionals may already be familiar with (NSA, 2021). Zero trust is more of a shift in philosophy rather than being yet another new tool (NSA, 2021). The zero trust philosophy starts with the premise that attackers have already infiltrated a system and entails working to mitigate the damage (NSA, 2021).

Various attributes of the Microsoft system, including the single sign-on model, allowed the attackers to have easier access to sensitive information once networks were infiltrated (Bajak, 2021). The single sign-on model facilitates easy navigation within systems for authorized users; however, once authentication information has been compromised, the attackers could easily navigate within all systems without needing to use separate authentication information for other systems. Coupled with the fact that many organizations provide administrator access to far too many individuals who do not need this access, and this results in an increase in the amount of data that attackers have access to once they compromise authentication credentials. Zero trust would reduce the use of single sign-on services despite its convenience because the risks of exposure are too significant when credentials are compromised.

No company's code should be given 100% trust. Part of why the SolarWinds attack was especially nefarious is because the attackers managed to infiltrate SolarWinds, changed the source code in its software in an undetected manner, sent out updates which appeared to be legitimate and and the updates appeared to have a kind of digital factory seal which had not been tampered with (Temple-Raston, 2021). Given that the alterations to the SolarWinds software were undetectable prior to the breach becoming known, no code for any company should be assumed to be safe (Temple-Raston, 2021). Given that Microsoft's source code was among the things that the SolarWinds hackers obtained access to, it is

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

especially important that less trust be placed in Microsoft products (Bajak, 2021) .

In the case of the SolarWinds breach, since the malware entered the program before it was even a program, such an incident makes some security advice ineffective in defending against that type of attack. ; for instance, a company should only install signed versions. The affected customers did in fact install signed versions, but the malware was part of the signed version. Other common security advice is that a company should update to the latest version, but the organizations which were breached did exactly that except the updates had been subverted (Vaughan-Nichols, 2021). Vaughan-Nichols (2021) believed that using open-source could be a solution. Although open-source software can still be vulnerable to attacks, the code can be audited by other people besides their developers. Open source software allows more people to look for possible issues and address them before they become significant.

Increased Scrutiny

One cybersecurity expert proposed that there should be a paradigm shift in terms of how we view cybersecurity and enterprises should, "manage your data like you manage your money" (Radichel, 2020). Organizations currently use accounting methods to ensure that money is tracked and no fraudulent transactions appear (Radichel, 2020). Every financial transaction is verified to make sure it is a valid transaction (Radichel, 2020). With many of these data breaches, including the SolarWinds breach, the attackers relied on command and control (C2) traffic to communicate with the hackers and execute their wishes (Radichel, 2020). Although the attackers used obfuscation techniques to hide the C2 traffic, it could still potentially show up in logs and be detectable (Radichel, 2020). While networks do create an enormous amount of network traffic logs, if there was a policy in place requiring all traffic to be cross-checked to ensure its validity, then more attacks could be detected. This paradigm shift would require a substantial increase in resources expended on log analysis.

Logs are not the only thing that needs to be carefully analyzed. FireEye's CEO, Kevin Mandia, told CNN that what caused the company to initiate an incident response investigation was when the hackers attempted to add a new phone number to FireEye's network for multi-factor authentication purposes (CNN, 2021). A security investigator did not just add the new phone number, but instead contacted the employee whose account the phone number change was requested for and asked whether the request came from the employee (CNN, 2021). The employee told the investigator that the phone number did not belong to the employee (CNN, 2021). This security investigator was the first person within over 18,000 companies and multiple government agencies to realize there was potentially a breach. Verifying changes to authentication information is extremely important for companies to engage in when granting access.

Compliance Audits for Vendors

It is not within the budget of most enterprises, and would be an inefficient use of capital, to do continuous full audits of vendors. What is feasible though is to ask vendors to provide documentation to show their compliance with cybersecurity regulations and best practices. (Abadir, 2021). Clauses should be included in Service Level Agreements and other contracts to require vendors to provide these artifacts as proof of compliance. (Abadir, 2021). There should also be provisions in contracts to allow for both periodic and on-demand assessments of vendors. (Abadir, 2021).

Third-party providers need to provide documentation to their customers so when a vulnerability becomes publicized, the customer can quickly assess whether their version of the software was among those affected by it (Abdair, 2021). Burton (2021) stated that organizations should architect not only their enterprise, but they should also do so for their business ecosystem. She mentioned the importance of inputting the services or solution providers' internal architecture into the organizations' enterprise architecture (EA) repository (Burton, 2021). Organizations should require that these third-party vendors provide clear and updated architecture diagrams. Policies and principles on scalability, security, reliability, and extensibility need to be documented, and these third-party providers must adhere to them. Organizations may not typically possess the complete picture of a third party vendor's internal architecture; however, it is beneficial to include that information in the EA documentation repository. Such information could better prepare organizations to assess a possible incident's impact and address issues quickly (Burton, 2021).

Law Changes

It may be time for laws to be changed to require greater information sharing and reporting of data breaches. Current laws allow organizations to share information with the Department of Homeland Security, but in 2018 only nine organizations did so (Uberti, 2021). With the increase in advanced persistent threats, it seems evident that more attacks will take place and could have a significant impact across industries. Requiring mandatory reporting to a centralized agency can help the odds of trends being spotted and may help prevent or mitigate attacks.

In July of 2020, one organization did detect what they thought was a bad update for SolarWinds, but they did not report it. (Temple-Raston, 2021). In September of 2020, Palo Alto Networks found a problem with a backdoor in the Orion software, but they did not have enough information to discover the full extent of the problem (Temple-Raston, 2021). It was not until December of 2020 that the SolarWinds breach was discovered (Temple-Raston, 2021). Had there been greater pooling of information, the attack could have been detected sooner.

Currently the NSA can monitor foreign computer traffic, but it cannot monitor the traffic once it enters the

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

United States (Myre, 2021). The Russian attackers rented servers within the United States to take advantage of this blind spot (Myre, 2021). The Constitution does not allow generic, warrantless monitoring of domestic computer traffic (Myre, 2021). While circumventing the Constitution would be inadvisable, mandatory reporting of cyber breaches does seem like a reasonable measure to take.

Enhanced Software development

The SolarWinds attack exposed several software supply chain insufficiencies related to software development and maintenance, intrusion detection, and confinement. The attack also revealed the need for more work towards gaining the benefits of software and related updates while avoiding the potential risks that updates can introduce (Massacci, Jaeger, and Peisert, 2021). Researchers suggest that the frequency of software updates may promote higher levels of vulnerability, and users should conduct a risk-benefit analysis to evaluate the safety of installing software updates (Massacci, Jaeger, and Peisert, 2021).

Massacci et al., (2021) even question the necessity of software updates and suggest that they potentially introduce new vulnerabilities that can compromise the software supply chain. They offer that new systems should consider features that support protecting their supply chains and allow customers to restrict new features. Their suggestion promotes empowering users to decide which updates to accept and reject. Their suggestion allows the software vendor to relinquish some of the burden of ensuring software and supply chain security and shifts the responsibility to the user/client.

Conclusion

The SolarWinds attack has made it necessary for the government and commercial organizations to reevaluate how they approach understanding security systems, supply chain risks, contractor responsibilities, and cybersecurity in general. According to Wolff et al. (2021), the most significant takeaway from the attack besides its direct impacts relates to the implications that it has for the future of government and organizations. There is a necessity for the government and organizations to understand the nature of the incident, its impact, and how they can use this knowledge to support contractors across all sectors. When it comes to investigating and mitigating risks, contractors should implement and enforce internal policies and procedures. They should adhere to industry best practices to investigate incidents and incorporate guidance from the government and industry related to the SolarWinds attack into their incident response efforts (Wolff et al., 2021). Bowman (2021) suggested that the federal government must get a better handle on cyberspace security; to ensure that the technology that we now securely and comfortably use does not slowly transition into a vehicle for insecurity and discomfort. Law changes may be a necessary part of this federal response.

The SolarWinds attack exposed the harsh reality that even the systems we rely on for the management and security of technology are vulnerable to attacks. In fact, they have the potential to promote higher levels of vulnerability given that they undergo frequent updates and are typically used within many of the most secured network environments and supply chains. For hackers and other cybercriminals, these systems get targeted because exposing vulnerabilities in these systems promotes their ability to access other secured systems and related information. Contractors are just as responsible for cybersecurity as the companies whose support software systems they deploy. It is the contractor's responsibility to take ownership of securing their own supply chain and related assets. Therefore, in recognition of this reality, IT professionals have an enhanced responsibility to ensure the security not only of internal assets but also of the systems they employ to promote enhanced security.

References

Abadir, S. (2021, March 24). *Top Risk Management Lessons from the SolarWinds Hack*. BrightTalk. Retrieved from https://www.brighttalk.com/webcast/15953/473372?utm_source=brighttalk-portal&utm_medium=web&utm_content=Top%20Risk%20Management%20Lessons%20from%20the%20SolarWinds%20Hack&utm_term=search-result-1&utm_campaign=webcasts-searchresults-feed

Akhtar, N. (2020). Latest trends in the Cybersecurity after the solar wind hacking attack. *Foundation University Journal of Engineering and Applied Science (FUJEAS)*, *1*(2), 14-24. Retrieved from: https://fui.edu.pk/fjs/index.php/fujeas/article/view/347/139

Associated Press. (2021, March 29). *SolarWinds hack got emails of DHS head and other top officials*. Retrieved from NBC News: https://www.msn.com/en-us/news/us/solarwinds-hack-got-emails-of-dhs-head-and -other-top-officials/ar-BB1f5prA

Bajak, F. (2021, April 17). *SolarWinds hacking campaign puts Microsoft in the hot seat*. Retrieved from AP News: https://apnews.com/article/politics-malware-national-security-email-software-f51 e53523312b87121146de8fd7c0020

Barskey, N. (2020, December 26). *The Solar Winds Breach Reinforces Why Boards and Audit Committees Need More Tech Expertise*. Retrieved from Forbes: https://www.forbes.com/sites/noahbarsky/2020/12/26/solarwinds-cybersecurity-breach-re inforces-board-technology-needs/?sh=3a56ad9c3e67

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

Bowman, J. (2021). *How the United States is Losing the Fight to Secure Cyberspace*.

Burton, B. (2021, February 18). *The SolarWinds Hack and the need to Architect your Ecosystem*. Aragon Research. Retrieved from https://aragonresearch.com/the-solarwinds-hack-and-the-need-to-architect-your-ecosyste m/

Center for Internet Security. (2021, March 15). *The Solar Winds Cyber-Attack: What You Need to Know*. Retrieved from Center for Internet Security: https://www.cisecurity.org/solarwinds/

Cimpanu, C. (2021, January 12*). Third malware Strain discovered in SolarWinds supply chain attack.* Zdnet. Retrieved from https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chai n-attack/#:~:text=In%20a%20report%20published%20today,components%20into%20lar ger%20software%20applications.

CISA. (2021, January 5). *Joint State 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)*. Retrieved from CISA: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

CNN. (2021, February 24). *FireEye CEO on how the SolarWinds hack was discovered*. Retrieved from CNN: https://www.cnn.com/videos/business/2021/02/24/fireeye-ceo-solarwinds-hack.cnnbusine ss

Holland, J. (2021, April 16). *Biden's Russia Strike Marks Shift in U.S. Cybersecurity Strategy*. Retrieved from Bloomberg Law: https://news.bloomberglaw.com/tech-and-telecom-law/bidens-russia-strike-marks-shift-in -u-s-cybersecurity-strategy

Jibilian, I. & Canales, K. (2021, February 25*). Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal. Insider*. Business Insider. Retrieved from https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cybersecurity-2020-12?amp

Kindervag, J. (2021, April 7). *John Kindervag: 'The Hallmark of Zero Trust is Simplicity'*. Retrieved from Wall Street Journal: https://deloitte.wsj.com/cio/2021/04/07/john-kindervag-the-hallmark-of-zero-trust-is-sim plicity/

Korolov, M. (2021, February 4). Supply chain attacks show why you should be wary of third-party providers. CSO. Retrieved from https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-shouldbe-wary-of-third-party-providers.html

Massacci, F., Jaeger, T., & Peisert, S. (2021). SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing With the Devil?. *IEEE Security & Privacy*, *19*(02), 14-19.

Myre, G. (2021, April 6). *After a Major Hack, U.S. Looks to Fix a Cyber 'Blind Spot'*. NPR.Retrieved from NPR: ttps://deloitte.wsj.com/cio/2021/04/07/john-kindervag-the-hallmark-of-zero-trust-is-simpl icity/

NSA. (2021, February). *Embracing a Zero Trust Security Model*. Retrieved from NSA: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SE CURITY_MODEL_UOO115131-21.PDF

NSA. (2021, February 25). *NSA Issues Guidance on Zero Trust Security Model*. Retrieved from NSA: https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2515176/nsa-is sues-guidance-on-zero-trust-security-model/

Peisert, S., Schneier. B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A.,& Bret Michael, J.(2021). "Perspectives on the SolarWinds Incident." *IEEE Security & Privacy* 19 (02), 7-13.

Radichel, T. (2020, Mar 11). *Manage your data like you manage your money*. Retrieved from 2nd Sight Lab: https://medium.com/cloud-security/manage-your-data-like-you-manage-your-money-b07 3bbf1250

Sands, B. F. (2021, February 26). *Former SolarWinds CEO blames intern for 'solarwinds123' password leak*. Retrieved from CNN: https://www.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html

Sayegh, E. (2021, February 11). *Solar Winds Hack-From Supply Chain Risk to Full Spectrum Awareness*. Retrieved from Forbes:https://www.forbes.com/sites/emilsayegh/2021/02/11/from-supply-chain-risk-to-full-spec trum-awareness/?sh=654d5eb23854

Solar Winds. (2021). *Solar Winds*. Retrieved from Solar Winds: https://www.solarwinds.com/

Temple-Raston, D. (2021, April 16). *A 'Worst Nightmare' Cyberattack:The Untold Story of the SolarWinds Hack*. Retrieved from NPR: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

International Journal of Business and Applied Social Science (IJBASS)

E-ISSN: 2469-6501
VOL: 7, ISSUE: 9
September/2021
DOI: http://dx.doi.org/10.33642/ijbass.v7n9p2

Uberti, D. (2021, April 1). *After Solar Winds, Lawmakers Want Companies to Come Clean About Cyberattacks*. Retrieved from WSJ: https://www.wsj.com/articles/after-solarwinds-lawmakers-want-companies-to-come-clea n-about-cyberattacks-11617269402

Vaughan-Nichols, S. (2021, January 14). SolarWinds defense: How to stop similar attacks. Zero Day. Retrieved from https://www.zdnet.com/article/solarwinds-defense-how-to-stop-similar-attacks/

Wolff, E. D., GroWlEy, K. M., & GruDEn, M. G. Navigating the SolarWinds Supply Chain Attack.