BITSIGHT
The Standard in SECURITY RATINGS

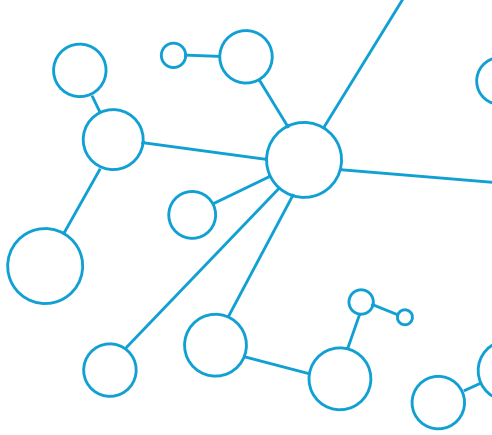
WHITE PAPER

The Future of Supply Chain Cyber Risk Management After SolarWinds

Report on Salon with Richard A. Clarke and Stephen Boyer

February 2021

Table of Contents



1. Introduction

On January 27, 2021, BitSight hosted a salon discussion about the future of supply chain cyber risk management in the wake of the SolarWinds hacking campaign.

Stephen Boyer, Chief Technology Officer and Co-Founder of BitSight, and Richard A. Clarke, Chairman of Good Harbor Security Risk Management, provided their analysis of the incident, as well as insights from advising industry Chief Information Security Officers, Chief Executive Officers, and Boards.

Following their opening remark and a discussion facilitated by Jacob Olcott, Vice President of Communications and Government Affairs for BitSight, an audience of cyber security and risk management executives from the private and public sector shared their own perspectives in a Question & Answer forum under Chatham House Rules.

This report records key observations and conclusions from those discussions.

"Several security vendors have disclosed SolarWinds-related incidents spanning varying stages of the attack. That this subgroup of victims was consistently targeted and compromised is an alarming development."

- STEPHEN BOYER

2. SolarWinds: Knowns and Unknowns | Opening Remarks by Stephen Boyer

Stephen Boyer initiated the discussion with an overview of the attack and the most recent developments gleaned from BitSight's analysis.

Q: Stephen, could you provide an overview of what we know about the SolarWinds incident, and any major developments to date?

The SolarWinds-based supply chain cyber attack is an ongoing major incident which will take at least a year to remedy and many months to fully comprehend, but there are known indicators from which to draw some salient implications. As with any crisis, early reports are often inaccurate. As details continue to emerge, the astounding scope and sophistication of the operation will become clearer.

In December 2020, SolarWinds confirmed that their network had been penetrated by a malicious actor, and a complex malware program infected software updates for its Orion program. The program comprised a multi-stage process, scanning networks to detect security tools it could avoid or disable, and stealthily connecting to the attacker's command and control servers. The malware persisted for months before initial detection.

Early reports indicated that up to 18,000 customer networks were affected, including major technology firms and governments. Current data indicate that infected customers are fewer in number than initial reports. However, several security vendors have disclosed SolarWinds-related incidents spanning varying stages of the attack. That this subgroup of victims was consistently targeted and compromised is an alarming development.

SolarWinds appears to have owned "the keys to the kingdom" for many organizations, possessing the ability to update software, patch systems, manage virtualization systems, monitor networks, and more. According to BitSight ratings, very few organizations classified SolarWinds as a critical vendor. It was an ideal target for disseminating an attack. While the market has largely responded by removing vulnerable versions of SolarWinds products, there are organizations with "trojanized" versions of SolarWinds connected to the Internet still using it now.

"It is easy to point fingers after the fact. Nonetheless, understanding the failures that contributed to disaster is a first step in learning how to prevent them."

- RICHARD CLARKE

3. Learning from Failure |
Opening Remarks from Richard A. Clarke

Q: Dick, you've identified distinct failures that occurred to get us to this position. What are these failures?

Richard Clarke observed that, "it is easy to point fingers after the fact. Nonetheless, understanding the failures that contributed to disaster is a first step in learning how to prevent them." He recognized six overarching failures of processes and institutions that warrant reflection if we hope to combat these challenges.

i. Failure of Warning

Some commentators have referred to the SolarWinds poisoned update as a "new attack vector." In fact, a different Russian intelligence agency than the one that conducted the SolarWinds hack similarly used a widely distributed and trusted software update to penetrate networks in 2017, that time targeting organizations in Ukraine. That 2017 Russian attack, NotPetya, was conducted by Russia's military intelligence unit known as GRU and irreversibly encrypted all software on networks it accessed, causing corporations to cease operations for weeks.

After the 2017 attack, many cyber security professionals began to worry about widely used software updates as an attack vector. More recently, the U.S. Cyberspace Solarium Commission identified trusted supply chains as an important issue. But, the U.S. failed to follow through on our realization of risk and do the things that could have prevented this attack.

ii. Failure of US Intelligence

U.S. Cyber Command and the National Security Agency have touted a "defend forward" strategy for taking on cybersecurity challenges. Despite all of the sophisticated technology deployed to enable this strategy, it provided little to no deterrence for the attackers that compromised SolarWinds and did not appear to provide warning of the hacking campaign, either before it happened or for months afterward.

iii. Failure of Shared Assessments of Supply Chain

Despite an increasing awareness in the industry about supply chain security and the origins of code, corporations and governments did not adequately assess the cyber security of companies from whom they accept software updates. There were ample signs that SolarWinds as a company was not taking cyber security seriously enough. They appear to have had no Chief Information Security Officer and to have had a low security score from a reliable external evaluation product. Word had spread that they had left a password ("solarwinds123") for their update server visible to anyone on a development site. Anyone doing serious supply chain risk assessments would have flagged the company as a risk.

"Corporations and agencies do not have effective methodologies to scan or test software updates prior to their acceptance and use on networks."

- RICHARD CLARKE

iv. Failure of Software Development and Testing

Corporations and agencies do not have effective methodologies to scan or test software updates prior to their acceptance and use on networks. Some larger companies in regulated industries, like banking, do code scans before use, and so do some government agencies, but they look for either known coding errors that create potential vulnerabilities, or known malware, exploits that had been seen before and even given agreed upon designations such as a number on the Common Vulnerabilities and Exposure list and the US National Vulnerabilities Database. Looking for "zero day" malware, an attack that had not been seen before, is harder.

As far as we can tell, not one corporation or government agency scanned the SolarWinds update for security and noticed that there was a file with code that was time delayed for activation two weeks after being uploaded, with instructions that the program should connect to an unknown, hard-coded server outside the target network. Such a "call" instruction could have been seen if any scan were instructed to look for something like it. If a scan did discover it, the security software should have triggered an alarm.

v. Failure of Network Detection

The initial reaction to the hack was, erroneously, that all the security software designed to detect this kind of attack had failed. This undermined our theory that it is increasingly possible to construct a defensible and resilient network. Now, however, we know that some security software might have worked. In fact, it seems so likely to have worked that it appears the malware was designed to avoid it: shortly after activating on a network, the malware looked for what security software was running and, depending on which tools it found, either turned them off or turned itself off, rather than risk being detected.

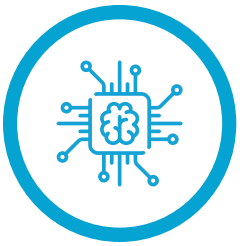
It was more important that the malware not be detected anywhere (and then reported everywhere) than the malware attempt to operate on all the networks it penetrated. The attackers likely knew in advance what security software would discover the malware running or prevent it from working properly, what security products could be silenced, and what security products needed to be avoided.

vi. Failure of National Coordinated Response

Individually, security vendors, large technology companies, and even government response teams are working diligently to collect and analyze data that could help to diagnose, mitigate, and respond to this attack. However, there is no coordinated national response that is helping to identify what networks were actually infected, to what extent, and taking action to remedy the damage. Such an atomized response will likely protract efforts to root out the infection, as well as identify deeper vulnerabilities (like "backdoors") that the attack potentially left behind.

"We know that some security software might have worked. In fact, it seems so likely to have worked that it appears the malware was designed to avoid it."

- RICHARD CLARKE



"Some commentators and practitioners have down-played the significance of the attack as "just an intelligence collection operation."

- RICHARD CLARKE

Maintaining Vigilance

Some commentators and practitioners have down-played the significance of the attack as "just an intelligence collection operation." While it certainly was a successful intelligence collection operation, I believe it was also what the military calls "preparation of the battlefield," with the hackers leaving behind backdoors that would allow them to access thousands of networks again in the future.

If there ever is a US-Russian crisis over, for instance, Poland or Estonia or Ukraine, and the Russians want to send a shot across the bow, they could cripple a great deal of our economy and our IT infrastructure by going back into these companies and wiping out critical networks. Do not relax, and do not assume the attackers were just collecting data. They were preparing the battlefield, and they succeeded.

4. Facilitated Discussion with Stephen Boyer and Richard A. Clarke

Jacob Olcott, Vice President, Communications and Government Affairs at BitSight, moderated a discussion focusing on incident response, warning signs, and key takeaways for public and private sectors. The discussion has been edited for clarity and brevity.

Q: How did CISOs and the security community react to SolarWinds?

Stephen Boyer: I've been spending a couple days a week with either CISO groups or one-on-one with companies to understand their thinking on this, and the response has certainly been an escalation to better understand their supply chain. It received attention before, but the priority is elevated. Principally, there are two questions that organizations are asking:

• First, "What is our direct and indirect exposure from the SolarWinds compromise?"
That is difficult to answer quickly and comprehensively. Assessing exposure is hard enough for companies that have a strong asset inventory, but the software could have been implemented unbeknownst to the organization. For instance, some companies reported that employees installed free versions of SolarWinds on an endpoint without IT or budgetary approval.

• Second, "What is our broader exposure through the supply chain, and what are we going to do about the next major incident?"
This is even more difficult than identifying immediate exposure. This is why I want to highlight the issue of third-party security vendors. I agree with Richard about the potential follow on risk, an attacker prepares the battlefield by going after all the security tools. How are you going to stop them the next time if they know how to get around, or subvert, or disable every one of your security tools? One of the CISOs I talked to was committed to strengthening code inspection. I think that is an interesting idea, however, doing that at scale for every update is going to be hard to do.

In some of these cases, better protections around outbound connections from software could have mitigated the risks. Unfortunately, the majority of companies did not have SolarWinds as a critical vendor, even though they had critical access to company networks. Going forward, reassessing and re-prioritizing criticality of vendors will be important.

"People say, 'well, nothing shows up in the logs.' Let me remind you that these sophisticated attackers have the capability to alter or clean the logs."

- RICHARD CLARKE

Q: Companies are definitely starting to re-think the vendor tiering process and issues of criticality. Richard, tell us about your experience with the security community and the Board level.

Richard A. Clarke: The boards that I've discussed this with have gone through something similar to the traditional "stages of grief." The first stage is shock and horror. The second stage typically sees CISOs, or more frequently CIOs, reassuring the board that the company did not run Orion, or they had some other non-compromised version of SolarWinds. Boards are told, "it's OK." However, this may be a false sense of security because, as Stephen alluded to, there is a secondary problem here. Other major vendors like Cisco, Microsoft, FireEye suffered from the attack. Did you have those on your networks? What makes you think there are not lingering risks with those vendors, or even that Orion was the only SolarWinds product that was compromised. Until we know the full extent of the attack, you cannot be sure that you are in the clear.

In defense of this people say, "well, nothing shows up in the logs." Let me remind you that these sophisticated attackers have the capability to alter or clean the logs while in the network, maintain persistence for months, and leave no evidence they were there.

Another concern on the part of boards that are a bit more sophisticated, is "consultants told us to spend all this money on these security tools. Why didn't they work? Why should we keep spending?" A partial answer that is that some of them did apparently work. Details are still emerging, but it appears that the malware sniffed the infected network to identify active security tools. If certain tools were detected, the malware aborted operations. I believe it was because the Russians knew there were tools that they could not get around.

As to Stephen's comment about companies improving code inspection, I say, "good luck." Leading vendors I've talked to claim they likely would not have caught it under current practices. Like all code inspection companies, they look for known CVEs. This was an unknown that they could not have found.

Q: Managing these vendor relationships seems like an overwhelming challenge for individual companies, as well as for establishing a collective model. What are organizations doing to identify and manage risks from vendors that may have a critical impact like SolarWinds?

Stephen Boyer: The population of vendors that could have an impact like SolarWinds is likely in the dozens. Tools like Orion are deployed in a larger enterprise, not a "mom 'n' pop" shop. However, the secondary tools that were targeted appear to have broad deployment, common management tools that organizations adopt as they scale. For instance, CrowdStrike claims a significant portion of endpoints, Microsoft provides management tools for orchestration all over. The alarming aspect of this kind of supply chain attack is how the scale cascades as organizations' data is shared across multiple vendors and outsourced providers.

Code inspection, questionnaires, or security scoring of select major vendors alone will not solve this. The ability to pass the infection to broad deployments makes this a large scale problem.

"The alarming aspect of this kind of supply chain attack is how the scale cascades as organizations' data is shared across multiple vendors and outsourced providers."

- RICHARD CLARKE

Q: This is a reason why the supply chain attack has become so popular over the past five years, the potential to attack thousands of organizations with one fell swoop. How is the risk to supply chains being addressed?

Richard A. Clarke: *People have talked about supply chain, but what have they done?*

Organizations give questionnaires to their suppliers. The suppliers "self-attest" that security is in order. Frankly, that seems worthless. Why Bother?

Companies work hard to visit vendor sites to auditing and testing, but it is unrealistic to expect all vendors to be reached or the level of testing will be detailed and effective enough to make a difference.

The solution could be more shared assessments led by third parties that are dedicated to the burden of testing these vendors. There should be an initial focus on small software companies that cannot afford the level of excellence that large corporations have the experience and funding to achieve.

Q: Is this a market failure? Could the cybersecurity community have done more as a collective to mitigate these risks?

Richard A. Clarke: *When I think about "market failure" in cybersecurity, I consider the policy history of US presidential administrations. Every administration since Clinton has indicated that the government will not impose federal regulations on industry unless there is market failure, characterized as companies demonstrating neglect or otherwise not taking it seriously. I think companies do take cybersecurity seriously. I do not think this is market failure in the traditional sense, one that that requires government regulation because companies are avoiding doing the right thing.*

I think this is an example of a lack of leadership, in both the private and public sectors. It is a lack of action to tackle the supply chain problem, not a lack of concern. The Russians found a weakness in our system and exploited it. Our mistakes point to not being coordinated, diligent, and proactive enough to go beyond paying lip service to the issue.

I would like to think a genuine cybersecurity leader inside the US government would have identified this as a national problem and would have made a specific proposal. Absent that, I would like to think that one of the industry leading tech companies would have taken leadership and proposed a solution. Unfortunately, no one was willing to say that our solutions are inadequate. To that extent, maybe it is a market failure. Maybe the government should have said to the private sector, "fix it, or we'll regulate the hell out of you." That did not happen.

Stephen Boyer: *When markets correct, it is typically because something goes wrong. In the past, we had worms and viruses that caused significant damage and the industry adapted. In this case, it highlights one of the biggest gaps that we have. Organizations are spending and creating new tools to address the gap, but it is a uniquely complex problem that will require a different approach than before. Barring some sort of coordinated market approach, it will be hard for any single vendor, even the biggest ones, to solve this particular problem for the global digital supply chain. There are some key players in the industry that will have more influence, but a coordinated response will probably require leadership in government because you have so many competing interests from the private sector.*

"I think this is an example of a lack of leadership, in both the private and public sectors. It is a lack of action to tackle the supply chain problem, not a lack of concern."

- RICHARD CLARKE

Q: Please share some of the key takeaways from the private sector and CISOs.

Stephen Boyer: *Number one is that organizations have to keep their eyes on this problem. The status quo is not working, and visibility throughout the organization should be modernized.*

However, we should not be fatalistic about the challenge. There are steps companies can take to improve their posture. Had more companies performed baseline security around SolarWinds Orion, the malware would likely not have moved past stage one. Doing the basics well is easy to understand, but it is hard to do. However, that is a better option than doing nothing.

Collectively this industry can raise the bar for their expectations and inspections of their suppliers.

Q: What is the perspective for an effective government response?

Richard A. Clarke: *I think government is taking action and we will hear about it, later. If I were still in government, first, I would make a case for regulation. I would insist on standards for software development and testing. I would insist on standards for supply chain. I would ask the private sector to create those standards, and if they did not, I would have NIST do it. An effective way to implement these standards would have the largest buyer in the world, the US government, assert that it will not buy from anyone that does not meet those standards. Along with meeting those standards is strengthening third-party inspection.*

Secondly, we have to address response capacity in the US. This incident has demonstrated response capacity is currently insufficient. The government needs to tackle the challenge for creating response capability so that critical systems can get back online after failure. We do not have the sheer number of people we need, whether from private companies or government teams, to operate within affected networks.

> "Secondly, we have to address response capacity in the US. This incident has demonstrated response capacity is currently insufficient."
>
> - RICHARD CLARKE

Finally, we need to consider international norms. I know it sounds academic, but the Russians did this knowing that they would not suffer consequences. Nothing happened to them after they unleashed NotPetya. They need to learn a different lesson, and it is not something the US alone can teach them. The Biden administration should expand their multi-lateral approach to general global issues, to include a response to bad actors in cyberspace. We need to establish an international system of cyber norms, so we have a path to respond to future problems. My model is the International Atomic Energy Agency (IAEA). The organization will be able to receive member complaints, activate an international cadre of inspectors, collect the evidence, and recommend and levy sanctions. We need that for cyber.

> "The status quo is not working, and visibility throughout the organization should be modernized. However, we should not be fatalistic about the challenge."
>
> - RICHARD CLARKE

5. Q&A and Attendee Discussion

Audience attendees were invited to ask questions and contribute to the discussion under Chatham House Rules. The summary notes below reflect key topics and a mix of areas of alignment and divergence, and they are not attributable to any individual or organization.

5.1 Changing the Status Quo

The SolarWinds attack should mark an inflection point for cybersecurity. While there is a range of behaviors across organizations, corporations are far from unconcerned or irresponsible with security. The most regulated industries also have the most sophisticated cybersecurity capabilities. It is not uncommon for security to garner 10-15% of their budgets, yet these failures keep happening. It does not make sense to double down on an approach that is not working.

Cybersecurity needs a paradigm shift, including distinct priorities for establishing effective shared assessments. There is significant overlap of responsibilities and efforts that, if coordinated, could alleviate immense burdens on individual companies. Information Sharing and Analysis Centers (ISACs) could take on the role for germinating the shared assessment model.

5.2 Establishing International Norms and Cooperation

Governments and international institutions must increase cooperation to take on cyber security challenges. If an organization is targeted by determined nation state adversaries, it is not realistic to expect an effective, prolonged defense. The time and resources at the adversary's disposal all but guarantees the targeted organization will be breached, and the damage will be severe. Industry needs support from government coordination to strengthen global order through cyber rules and norms.

Nonetheless, there are challenges with developing international cyber norms. The process takes time and action fails to maintain "the speed of relevance." The US is rebuilding relationships and capability in the new presidential administration. It should prioritize initiatives that can be rapidly achieved together, while pursuing those that the US can do alone. The concerted effort should include international non-profits, key partners, and cyber-related multilateral organizations like NATO's Communications and Information Agency (NCI) and the European Union Agency for Cybersecurity (ENISA).

5.3 Focusing Legislation

Legislative effort driven by the private sector will be an important part of the way forward. The past year has seen successful legislative efforts to improve cybersecurity. Following the Cyberspace Solarium Commission's recommendations, of approximately 50 legislative proposals, 25 have become U.S. law. The most significant was the establishment of the National Cyber Director. As a Senate confirmed position, the NCD can be the "one throat to choke" for reporting to Congress. Other efforts open for discussion include creating a "USDA for cyber" and authority for government to take down botnets.

5.4 Strengthening Public-Private Coordination

Government coordination and collaborative planning with the private sector is critical. Cybersecurity is a problem for the whole of enterprise, government, and society. Currently, the response is atomized, uncoordinated, and episodic. Expecting the market to solve the problem alone is not sufficient. There needs to be a concentration of capability and resources at the federal level, in addition to market action. A strong coalition should include aggregating power that will influence suppliers to get on board with new standards and expectations for security.

In the federal information security community, the concept of "shared services" has historically caused skepticism because efforts were characterized by top-down decisions that lacked coordination with practitioners. However, as departments start to develop these initiative, one thing is clear: If you're doing it well, others will get on board. No federal department has the resources to provide comprehensive services, like for instance, third party assessment. Information and burden sharing is critical to success. Additionally, the community needs to find a way to protect organizations if they are sharing information, particularly from liability stemming from agreements about violating licensing agreements.

5.5 Understanding Compliance vs Outcomes

The practice of security risk management would benefit from a shift from focusing on compliance to outcomes. The federal sphere should move towards risk-driven decision making to improve resource allocation and improve security. Rote compliance to federal regulations and standards can be onerous and does not necessarily promote or ensure effective cybersecurity risk management. Government agencies could benefit from an approach that manages risks according to their own unique risk profile, in accordance with approved cyber risk management standards.

5.6 Improving Supply Chain Assessment Models and Third Party Assessment

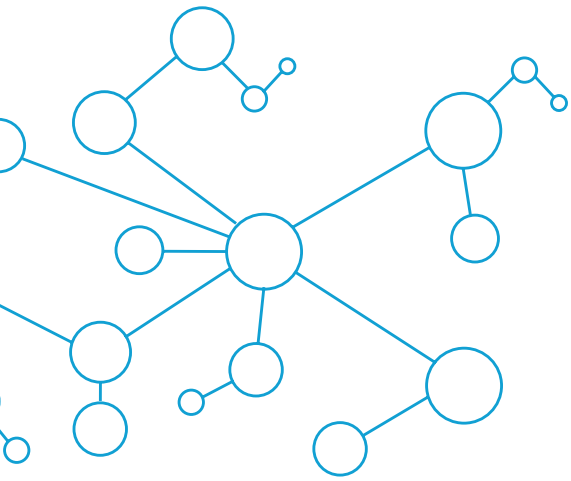
Current assessment models are insufficient. Self-attestation can be more of a myth than a reality. Some government programs, for example the Department of Defense's Cybersecurity Maturity Model Certification (CMMC), could be beneficial if applied more broadly (i.e. to commercial sectors), however there are limitations. For example, the CMMC is recognized as a good model for addressing its primary goal of protecting Controlled Unclassified Information (CUI).

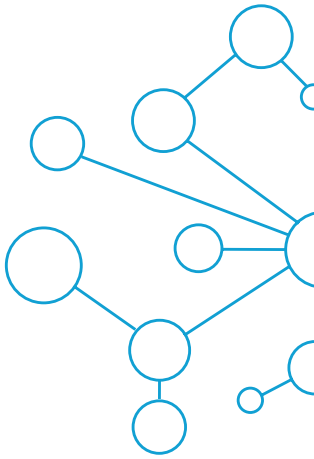
However, the scope and function of the CMMC model and other standards cannot adequately address commercial and software supply chain risks like SolarWinds and the community should not fool itself into trusting that it will be able to address the supply chain problem. The federal government does not have the expertise or resources to manage this challenge alone. Public-private cooperation is needed to develop innovative and effective models.

One proposed concept is developing a "cyber balance sheet" that outlines provisions similar to Sarbanes-Oxley Act requirements. The cyber balance sheet would provide transparent information about an organization's vulnerabilities and threats. Such a concept could provide improve transparency and disclosure to the market and incentivize investment to improve security.

6. References

1 https://www.zdnet.com/article/four-security-vendors-disclose-solarwinds-related-incidents/
2 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
3 https://www.solarium.gov/
4 https://warontherocks.com/2021/01/a-cyber-opportunity-priorities-for-the-first-national-cyber-director/





BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Fifty percent of the world's cybersecurity premiums are underwritten by BitSight customers, and 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit **www.BitSight.com**, read our blog or follow **@BitSight** on Twitter.