Neutral Introduction:

Hello everyone, before we dive into the debate, let us briefly summarize the SolarWinds cybersecurity attack, and provide the necessary context and background to fully understand this event.

SolarWinds is a company that develops software to help a variety of businesses manage their IT infrastructure, networks, and systems. However in September 2019, attackers injected malicious test code into Solarwinds' Orion network management system. This is where the attackers first started accessing SolarWinds and their activity remained undetected. And was strongly suspected by U.S. intelligence agencies such as the FBI that the attackers behind this incident have affiliations related to the Russian government. Fast forward to February 2020 the threat actor injected code into the software update files. In March, Solarwinds unknowingly released the software updates to their customers with the trojanized code, which allowed the attackers to gain unauthorized access to thousands of systems. Up until December 2020 was when SolarWinds first disclosed to the public of this supply chain attack. Infamously, the name of the malicious code planted into SolarWinds system is referred to as Sunburst, which is why this event is often referred to as the Sunburst attack.

Moreover, the Sunburst attack affected roughly 18 thousand customers, which provided the attackers remote hacking access– a backdoor– to numerous systems and networks of organizations around the world of their sensitive information and data. To name a few, the high profile customers that were affected by the breach were government agencies, such as Homeland Security, State, Commerce and Treasury, and other private companies such as Microsoft, Deloitte, Intel, etc. Crucially, the eventual discovery of the malicious code was discovered first by one of SolarWinds client-customers, FireEye which is a company that serves within cyberattack detection. Regarding the breakdown of events leading to the discovery of the Sunburst attack, with this slide it further includes a visual timeline curated by Microsoft, which they used information provided by SolarWinds, to offer a more detailed explanation of the attack's progression.

Next, the type of risk event the Solarwinds attack would appropriately be categorize in of this event would be a grey rhino –a known unknown– given Solarwinds as a brand is a major provider of IT management and monitoring software widely used by government agencies, enterprises, and other critical organizations.

as significant concerns that’s it’s impact is high in terms of the consequences and their data within risk is detrimental

due to the nature that cyberattacks and breaches are a prevalent concerns and also seen through trends in data that the cost data breaches financially situate companies over the years have increased, such as in 2021 an IBM report found that the “the average cost of a data breach was $4.24 million, which was a 10% increase from 2020” of the previous year. This highlights the high impact of growing trends in breaches that serve as the looming threat, the gray rhino, especially if the consequences are underestimated or difficult to respond to in order to prevent the damages it can cause. It fits most within the gray rhino definition-description that is related to highly probable impact trends seen approaching but what fundamentally exists is the unknown regarding how to respond appropriately.

Next, in the next two slides are the different types of Enterprise Risks that were involved in the SolarWinds attack.

[DID NOT HAVE TIME TO INCLUDE A POSSIBLE SCRIPT FOR THE 7 ENTERPRISE RISKS - read off powerpoint??]

1. Opening Statements (10 minutes)

- **Critique Team Opening Statement (5 minutes):** The team critiquing the enterprise's risk management presents their case, arguing why the losses resulting from the risk are unacceptable and providing reasons for why the risk management was poorly handled.

Today, we are here to critique the SolarWinds risk management strategy which failed to adequately address a foreseeable and significant risk, exposing 18,000 customer organizations, including U.S. federal agencies, to a massive cyber attack in which highly sensitive data was compromised. While it is impossible to reduce risk to 0, the severity of this breach brings to light the significant past SolarWinds failures in identifying, mitigating, and responding to potential and plausible vulnerabilities.

After conducting extensive research on this case, our group strongly argues that Solarwinds did not effectively handle this situation and their losses were unacceptable to their stakeholders. Among our findings, we would like to highlight the following points:

Main argument points:

-Extended timeline= It took 15 months for public disclosure since the infiltration of the threat actor and malicious code was undetected in Orion for months.

-Stakeholders involved= Over 18,000 companies rely on Solarwinds Orion infrastructure for IT management and monitoring

-Inadequate security practices= intern password case

- **Defense Team Opening Statement (5 minutes):** The defense team representing the enterprise or organization responsible for the losses presents their case, highlighting the rationale behind the actions taken and providing arguments to defend the handling of risk management.
  - They said solarwinds did the best they can to mitigate the issue, but how did they mitigate the issue when basic security measures like the password and

2. Cross-Examination (10 minutes)

- **Critique Team Cross-Examination (2.5 minutes):** The critique team asks questions to clarify or challenge the arguments presented by the defense team during their opening statement.
- **Defense Team Cross-Examination (2.5 minutes):** The defense team asks questions to clarify or challenge the arguments presented by the critique team during their opening statement.

- **Critique Team Response (2.5 minutes):** The critique team responds to the questions asked during the defense team's cross-examination, providing further explanation or defending their critique.
- **Defense Team Response (2.5 minutes):** The defense team responds to the questions asked during the critique team's cross-examination, providing further explanation or defending their position.

POSSIBLE ARGUMENTS AGAINST US:

-Companies should have monitored their own systems and not 100% rely on Solarwinds

-System managers may have trusted Solarwinds solely due to their high-profile clientele

-Investing in multiple IT services may be too costly and companies prefer to only use one resource

-There were adequate security practices in place (i.e. MFA, etc.), it was solely a one-off/human error

-Event happened during the COVID-19 pandemic – unprecedented times, and try to reason and group it up with the fact that the event is actually an unknown unknown (black swan); and that they were also going through transition in leadership.

-Reason that they took immediate action after learning about the attack and prioritized a customer first approach; and that they were going through a transition into new CEO and henceforth fixing mistakes where accountability is needed.

- Given that CEO, Sudhakar Ramakrishna, took office in January of 2021, which is weeks before December of 2020,

the SolarWinds attack exploited systemic vulnerabilities reported that were present before the CEO transition, that also indicates deeper organizational flaws unrelated to leadership changes; a new CEO does not absolve the organization of accountability for past practices.

- Security is not the responsibility of a single individual; it is a shared organizational commitment. Instead, it invites further discussion on how it can be strengthened."

3. Break (5 minutes)

- Both teams will be given 5 minutes to review and refine their arguments before presenting their arguments to the class.

4. Constructive Arguments (20 minutes)

Critique Team Constructive (10 minutes): The critique team presents their main arguments in detail, highlighting why the losses from the risk are unacceptable and providing evidence and reasoning to support their critique of the enterprise's risk management.

Main points:

- Extended timeline
    - Took 15 months for Solarwinds to publicly disclose attack, seems kinda long for an impactful attack
    - Malicious code went undetected in the Orion infrastructure
        - Solarwinds threat detection systems didn't detect it/blended in with their code
        - Consequent software updates were released and none detected its presence
- Stakeholders involved (Customers + partners)
    - Solarwinds customer base includes many high profile organizations such as the US government, making unauthorized access even more concerning/damaging.
    - Especially since the threat actor is believed to be the Russian Foreign Intelligence Service, the US government is concerned about national security.
    - Compromised systems could have provided hackers with high-value information, potentially very useful in future cyberattacks
- Inadequate security practices
    - Reports suggest SolarWinds did not adequately train employees on detection of malicious code.
    - SolarWinds use of a weak password "solarwinds123" is a critical vulnerability allowing bad actors to gain unauthorized access and potentially deploying keylogging software undetected.
        - New CEO Ramakrishna apologies for past CEO blaming the intern: saying human mistakes is where we "learn from those mistakes and get better"
    - Not having multi stage build systems to check if code is vulnerable in different environment stages

Defense Team Constructive (10 minutes): The defense team presents their main arguments in detail, explaining the rationale behind the actions taken by the enterprise or organization and providing evidence and reasoning to support their defense of the risk management.

5. Rebuttals and Closing Statements (10 minutes)

- **Critique Team Rebuttal and Closing (5 minutes):** The critique team summarizes their arguments, responds to any remaining points made by the defense team, and reinforces why the audience should agree with their critique of the enterprise's risk management.
- They said they had "best industry standards" lowkey want them to explain that

    - Well they did talk about how they have NIST but they didn’t really explain how and what, might be hard to find online but
        - I feel like these cybersecurity practices should be public info?
            -
- Court case
    - “The court held that the SEC had successfully pleaded that two of these representations were materially misleading to investors – those concerning access controls and password protections. The court explained that the SEC “plausibly allege[d]” that SolarWinds and its CISO misrepresented “the adequacy of [the company’s] access controls,” and that “[g]iven the centrality of cybersecurity to SolarWinds’ business model as a company pitching sophisticated software products to customers for whom computer security was paramount, these misrepresentations were undeniably material.”
    - Public distrust, having the claims against them still affects future stakeholder interest in a service that
        - They might talk about how their retention level is high despite the attack, but i feel like it is a case like Boeing, where people will continue to use the brand they have used for a long time even though they may have some incidents. Customers may have already invested lots of money/resources

Should we use this closing statement from Swas’ doc?

The SolarWinds hack was a significant cybersecurity incident with far-reaching consequences. While the sophistication of the attack and the shared responsibility with other companies like Microsoft should be acknowledged, SolarWinds' own security failures and delayed response cannot be ignored. The company's inadequate security practices, slow information sharing, and lack of transparency exposed its customers to significant risk and eroded trust in its products and services. This incident serves as a stark reminder of the importance of robust cybersecurity measures, proactive risk management, and transparent communication in today's interconnected world. By learning from the mistakes of SolarWinds and others, organizations can strengthen their defenses and better protect themselves against future attacks.

    - **Defense Team Rebuttal and Closing (5 minutes):** The defense team summarizes their arguments, responds to any remaining points made by the critique team, and reinforces why the audience should understand and support the actions taken by the enterprise.

6. Audience Questions (10 minutes)

- **Critique Team Audience Questions (5 minutes):** The critique team will respond to audience questions specifically challenging the arguments made by the critique team.
- **Defense Team Audience Questions (5 minutes):** The defense team will respond to audience questions specifically challenging the arguments made by the defense team.

Brief Summary of Event:

- U.S. Government Accountability Office
  - Cyberattacks started in **September 2019** when Russian Foreign Intelligence Service injected malicious test code into Orion, Solarwinds' network management suite, by breaching Solarwinds' network
  - In **February 2020**, they injected code into a software update file
  - After the software updates were released, threat actors had backdoor into customers' networks and systems
  - About 18,000 customers compromised
  - Customers that were affected most were federal government agencies and other "high-value" customers for espionage

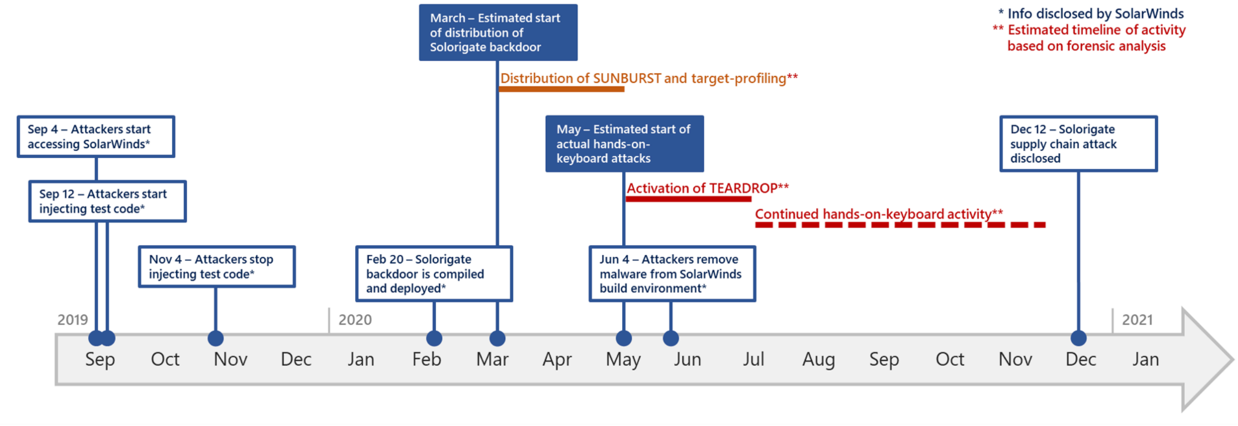
* Info disclosed by SolarWinds
** Estimated timeline of activity based on forensic analysis
March – Estimated start of distribution of Solorigate backdoor
Distribution of SUNBURST and target-profiling**
Sep 4 – Attackers start accessing SolarWinds*
Sep 12 – Attackers start injecting test code*
Nov 4 – Attackers stop injecting test code*
Feb 20 – Solorigate backdoor is compiled and deployed*
May – Estimated start of actual hands-on-keyboard attacks
Activation of TEARDROP**
Continued hands-on-keyboard activity**
Jun 4 – Attackers remove malware from SolarWinds build environment*
Dec 12 – Solorigate supply chain attack disclosed
2019
2020
2021
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan

Figure 1: Visual timeline of events (for easier viewing)

- Much earlier hack timeline (Cyberscoop)
  - Hackers were already performing reconnaissance activities as early as January 2019
  - Contrary to the original claims of September 2019
- Fortinet
  - Solarwinds attack is an example of a supply chain attack, where threat actors target a third party to get to their target (Solarwinds = third party, target = Solarwinds customers)
  - On average, attack cost companies 11% of annual revenue

- SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures (2023)
    - Research the other group might bring up: Federal Court Dismisses Bulk of SEC's Complaint Against SolarWinds in Cyberattack Case (2024)
- TechTarget
    - Grey Rhino: Known unknown because there were security rules put in place within Solarwinds' network to detect intrusion and malicious activity but attackers were able to bypass this using multiple U.S. servers
- SolarWinds': solarwinds123 password
    - SolarWinds blames intern for 'solarwinds123' password for a file server in 2019

Asset Risks

- Possibility of files and systems being damaged/destroyed

Safety Risks

- Impersonation
    - Hackers could compromise personal information and impersonate different employees in order to gain authorized access into different areas (CyberArk)

Business Risks

- Supply chain
    - Attackers were able to compromise a widely-used software update process through Orion's infrastructure to gain access to the networks of thousands of organizations around the world (Aquasec)

Financial Risks

- Fortinet
    - On average, companies lost 11% of annual revenue
    - American companies (14%), Singaporean companies at 9.1%, UK companies at 8.6%
- Bitsight (a company that calculates security ratings to shed light on an organization's security performance and measures cyber risk)
    - Insurance companies paid up to $90 million for incident response

Information Risks

- GAO
    - Gain info on high-value customers for espionage

Program/Project Risks

External Risks

Possible arguments from the defense and our responses

- Attack came out of nowhere and was highly sophisticated but we did the best we could

    - Maybe find things about notable state-sponsored attacks that occurred before this event and ask if they changed their policies to mitigate?