Deloitte.

The SolarWinds wake-up call: Why it's time to tackle concentration risks

This past week, a slew of high-level government agencies and major corporations across North America, Europe, Asia, and the Middle East were rocked by the news that their networks may have been exposed by suspected nation-state threat actors.

SolarWinds a software company with over 300, 000 customers issued a notification that potentially 18,000 customers downloaded a flagship product which may have been infected with a malicious code that gives threat actors backdoor access into their systems.

Company executives and Chief Information Security Officers (CISOs) faced with limited information on both the implications and scope of this attack yet are finding themselves under pressure —whether or not their organizations have been directly affected. Boards, customers, suppliers, and even the market are demanding immediate insight into the extent of the issue.

Pervasive and pernicious

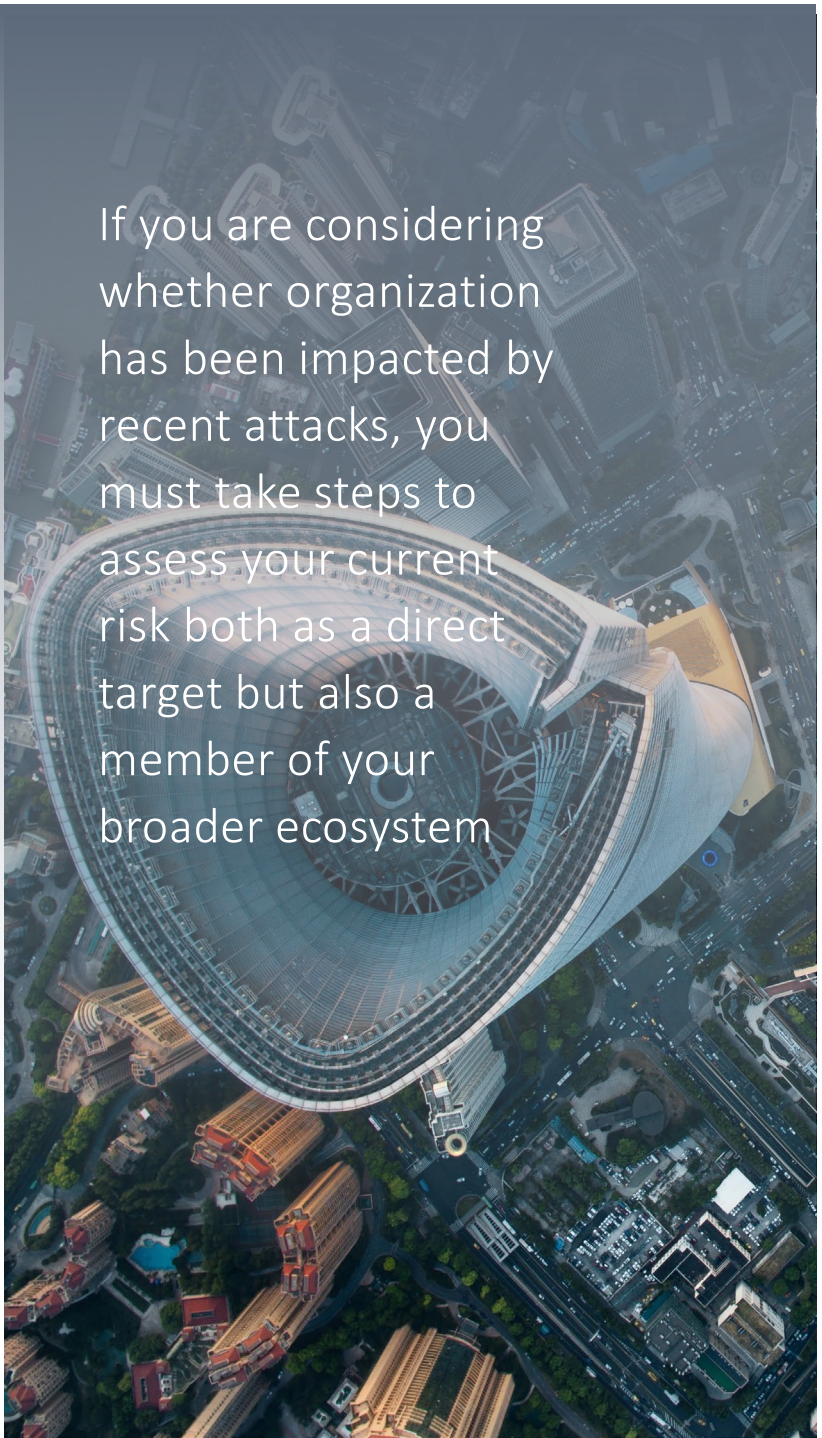
One of the reasons organizations gravitate towards best-of-breed technology solutions is because of the inherent security they ostensibly confer. Reputable endpoint detection and response (EDR) tools, cloud infrastructure solutions, and managed security service providers (MSSPs) built a trusted status within most organizations—and for good reason. These are the companies most serious about implementing unassailable security infrastructures.

Thanks to this high-level capacity, these third-party providers typically end up serving tens of thousands of customers spanning manifold industries and geographies—opening the door to concentration risk. to turn that prediction into reality.

Typically defined as the probability of loss likely to arise due to over-dependence on a single vendor, concentration risk is further exacerbated when such a vendor specializes in a specific industry. The more well-established these companies are, the more likely they are to have privileged access into networks that house extremely confidential and often classified information. They are part of the fabric and are inherently trusted. This makes them particularly tempting targets for sophisticated threat actors.

The uncomfortable truth is that these breaches happen more often than people imagine. Cybercriminals and advanced persistence threat (APT) groups consistently target even the most secure environments. Despite the higher threshold to hack these environments, the payoff is considerable: rather than gaining access to one or several backend systems, this approach can give them entry to an entire industry or geography.

During Covid times, the high volume of ransomware attacks, highly public data thefts or the concerns of remote system breaches are capturing most of the headlines. Naturally CISOs and their teams are prioritizing their resources.



No organization is immune to cyber breach

Many will identify potential concentration risks, but most will choose to deal with them later. Who would think that the global trusted provider or that industry best of bread solution would become a realistic attack vector?

Meanwhile threat actors realize the value of gaining control over the trusted providers or their solutions. Whenever they can, their work is covert and highly skilled. The return on their investment – a successful breach of an infrastructure provider – can pay back multiple times across many industries and geographies.

Understanding the consequences

When it comes to chronicling the impact of cyber breaches, statistics abound. According to research firm Cybersecurity Ventures, the global cost of cybercrime will reach $10.5 trillion by 2025—an amount that far exceeds the annual damage inflicted by natural disasters.[1]

This number hides countless repercussions within it, spanning data destruction, financial losses, and the theft of intellectual property and personally-identifiable information to business disruption, lost jobs, and often irreparable reputational damage. Yet, despite this toll, the numbers don't tell the whole story.

In fact, these attacks are most devastating when organizations can't tally their costs, simply because they don't even know they've been victimized. Some malware variants are so advanced that they can lie dormant within an organization's system for days or weeks, making them almost impervious to detection.

Once released, many of these malicious files crawl through an organization's entire network, giving attackers ongoing access into a target's systems even after the original backdoor is disabled. In many cases, organizations don't even realize they've been breached until months, and possibly years, later.

Responding intelligently

If you are considering whether organization has been impacted by recent attacks, you must take steps to assess your current risk both as a direct target but also a member of your broader ecosystem. Before you can respond to your executive sponsors, you need to determine whether you or other members of your ecosystem experienced a compromise, narrow down your view of the attack surface, and identify potential points of entry.

Although the temptation may exist to begin containment efforts immediately, it's often necessary to take a step back to first gauge the full extent of the incursion. Tipping your hand too early may cause you to lose the leverage you need to affect a complete recovery.

If your organization has a crisis response playbook, you are likely well-placed to chart out your next steps. If you don't, you will need to think through your crisis response while under pressure, likely in collaboration with the organization's law firm, insurer, and data breach coach.

It's also worth noting that even unaffected organizations are not truly unaffected. This past week has once again highlighted the fact that no organization is immune to cyber breach. It's a poignant reminder of the need to continuously strengthen your core cybersecurity hygiene to minimize the impact of concentration risk.

For some organizations, this may mean delving into your third-party liabilities and obligations. For others, it may involve categorizing your special interest vendors and assessing where you fit within the larger supplier ecosystem. For each of us, it's helpful to remember that we're all in this together. By collectively strengthening our cybersecurity postures, we can enhance not only organizational resilience, but to also raise cyber maturity across the board.

[1] Cybercrime Magazine, November 13, 2020. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," by Steve Morgan. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

If you're under pressure to minimize the impact of a current cyber incident or would like the options available to you when considering concentration risks, or simply to enhance your preparedness to weather future threats, contact Deloitte Cyber.

Authors and contacts

Amir Belkhelladi | Canada Cyber Leader
abelkhelladi@deloitte.ca

Nicola Esposito | Global Cyber Detect & Respond Leader
niesposito@deloitte.es

Loucif Kharouni | VP of Global Threat Intelligence
lkharouni@deloitte.com

Rob Masse | North America Cyber Cloud Leader
rmasse@deloitte.ca