Manus

IT- and software services have now after approximately four decades matured enough for competition to eliminate any and anybody that is not actively seeking to improve efficiency and cut costs. Long gone are the days where one organization is forced to build all its service supporting systems from scratch, simply for lack of such supply from other enterprises. In the cases where such historical outsourcing was possible, markets were usually so monopolized that some form of vertical integration, i.e the acquisition of different suppliers and or producers, was necessary in order to not get price gouged. Modern business administration strategy however dictates that mature industries should outsource all non-core stages of the supply chain in order to focus their resources and effort on their main competency or niche. The maxim being that everything that you are not the best at, can be done cheaper and better by somebody else. Thus, by specialization, you can save costs and achieve higher profits. This has been the development in IT firms for the last 15 years or so, and is a continuing trend. This is all fine when it comes to traditional industries like manufacturing, transportation and the service industry, as they are not prone to disturbances in the supply chain, and even when these disturbances occur, they can be easily remedied or fixed by delegating to different suppliers. **In the IT sector however, these disturbances can be catastrophic**, as the interdependencies between supplier and main organization does not warrant an easy change of supplier in the case of lets say, a major cyber attack. The end result being an organization incapable of functioning properly. This is exactly what happened with SolarWinds.

We can thus observe that even though outsourcing and specialization is good for performance and company profits in the IT sector, the abdication of control over several production stages introduces immense risk that could potentially undo all accumulated profits. This is exacerbated by the fact that when suppliers are for instance hacked in one way or the other, firms are left powerless to do anything about it, and are forced to be content until the supplier fixes the issue.

This is precisely what happened with the SolarWinds attack. SolarWinds being the supplier to a multitude of large corporations that have no control over SolarWinds internal cybersecurity mechanisms. When the incident was unraveled, over 18 000 customers were potentially affected, and few of them had any way of actually fixing the issue, which highlights the main problem with outsourcing within the IT industry. The main conclusion that can be drawn is that companies should engage more in developing their own infrastructure. Even as though this introduces more redundancy and less efficiency, it also results in a higher degree of control and consistency of operations.

Furthermore, as SolarWinds clients were put in danger due to a software update, it goes to show that when it comes to IT, simply purchasing a service, solution or product in general is not enough to guarantee safety. Firms must have some kind of way of defending themselves against malicious software updates. The fact that almost all clients of SolarWinds simply took the update for granted, is pretty alarming.

To this day, SolarWinds still does not know how the actors got access to their systems, which I believe says a lot about either the ability of the hackers or the inability of SolarWind, or both. A lack of understanding of their own systems, organizational and bureaucratic measures that lead to centralized decision making, among other things, could have been the culprit behind why the incident occurred. Another key indicator about the state of SolarWinds internal security mechanisms is the fact that three of their clients, independently of each other, discovered the attack before they did. Once they had notified SolarWinds management, the response was deflective and that there was in fact no real issue with the company.

Once properly aware of the intrusion however, instead of grabbing the problem by its horns, SolarWinds went ahead and hired a lawyer firm to handle the investigation. One of the first things companies tend to do after cyberattacks is to hire lawyers and put them in charge of investigations. They do this for a specific reason — it means everything they find is protected by attorney-client privilege and typically is not discoverable in court. This being yet another indicator of the centralized control structure of the company. Managements main focus is to fulfill its fiduciary obligations, and as such they deemed the safest option to be hiring outside lawyers in order to protect their assets and by extension the short-term financial well being of their owners. This however delayed the actual problem solving, which was put on freeze, until the external lawyers caught up with the developments of the attack, which presumably caused further damage to their clients. As the saying goes, justice delayed is justice denied. Allowing technicians and whoever was responsible for security to act immediately would have in hindsight stopped the bleeding earlier so to speak. It is however easy to be smart in hindsight, and how much this type of immediate action would have helped is hard to quantify.

What is surprising about the whole ordeal is that even when problems were being discovered by outsiders post-mortem, management responded by being deflective and complacent about the presented issues, such as password connected to SolarWinds accounts being shared on third party sites. This complacency has been confirmed by disgruntled ex-employees who have cited lax security standards as among the reasons they left the company. Even though SolarWinds was not very keen on cyber security expenditures, they sure were so when it came to sales and advertisement, which might be one of the key factors to why they were targeted. Considering its online marketing website. It contained an exhaustive list of clients including specific companies and government agencies that ran its Orion software. While a lot of companies do that, the SolarWinds site was very specific. Two cybersecurity analysts involved with the investigation describe it like something akin to a shopping list for adversaries. It is basically a large sign around your neck that displays the words “hack me”. This is yet another testament to what I believe is a wrongful assumption that IT firms should behave like companies in other industries. I believe that they should behave more like value transport companies for instance. That is, it is not wise to publicly state how much money each of your value transport trucks holds, less you want to be robbed. Thus, in the long term, secrecy might be desirable, especially when they cater to large enterprises and government agencies.

As high reliability organizations tend to promote decentralized decision making and a strong preference for reliability and failure free operations, SolarWInds management has displayed behavior that is the antithesis to that sort of organization. If it is any consolation to the parties involved, the new CEO at the company has stated that the main priorities of the

company is a new focus on “security by design”. One of the measures has been to publish their source code online for the entire world to see. Thus, even though now competitors can take part of their proprietary immaterial assets, effectively giving up part of their market share, this also enables outsiders to review and raise flags whenever potential security risks are detected.

Since the attack, the us government has been reviewing laws that would require companies that work with the U.S. government to meet certain software standards, and federal agencies would be required to adopt basic security practices such as encrypting data in their systems. In addition, software companies such as SolarWinds could be required to have their so-called build systems, the place where they assemble their software, air-gapped, which means they would not be connected to the Internet. If this set of laws had been in place before the attack, maybe the outcome for the affected federal agencies would have been different, as SolarWinds certainly would not have met the requirements necessary for being a government IT supplier.