Supply Chain Risk Analysis

# Abraham Cain

# July 28, 2021

Contents

[Supply Chain Risk Analysis 1](#_Toc78623844)

[Introduction 3](#_Toc78623847)

[Analysis 3](#_Toc78623848)

[Supply Chain Risk 3](#_Toc78623849)

[Due Diligence for Acquisition 6](#_Toc78623850)

[Best Practices for Managing Global Supply Chains 7](#_Toc78623851)

[Summary and Conclusions 7](#_Toc78623852)

[References 8](#_Toc78623853)

# Introduction

Cybersecurity may have been a thought in the back of a person’s mind in the early days of computers and information technology. However, those days are long passed. New threats to organizations’ information and operational security are materializing in the form of supply chain compromise. It can be seen with the SolarWinds breach, the Stuxnet worm, and the Target breach of 2013/2014 (FireEye, 2020) (Schneier, 2018) (Krebs on Security, 2014). We will analyze these incidents further in later sections, but each involved the compromise of an organization or organizations through the compromise of a trusted third party.

# Analysis

## Supply Chain Risk

After Identifying our supply chain and the companies and contractors that are links in that chain, we can look at risks to that supply chain. The publish “Identifying Cyber Supply Chain Risks” by the Australian Cyber Security Centre (2021) identifies four broad sources of risk for supply chains:

* Foreign control or interference in the supply chain
* Poor security practices of any member of the supply chain
* The lack of transparency of members of the supply chain
* Enduring access to the customer environment or systems.

When a supply chain for your hardware or software passes through another country, this can cause risk to your supply chain, especially if that country is an enemy or economic competitor. This has happened to be the case for most of the personal computers manufactured in the world. According to Bloomberg article “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies”, subcontractors for a computer manufacturer in China inserted a tiny microchip into many of the servers that they sold to American companies and government agencies. This microchip contained code that would allow attackers to access the machines remotely without the owner’s consent or awareness (Robertson, Riley, 2018).

Poor security practices of supply chain members are an area of risk for supply chains with many subparts. There are many poor security practices that may contribute to the compromise of the integrity, confidentiality, or availability of products in a supply chain. This is evident in the widely publicized SolarWinds supply chain compromise of 2020 which was briefly mentioned in the introduction. Alexys Carlton (2021) points out in her blog post “Why the SolarWinds Hack wasn’t an Intern’s Fault” that the SolarWinds breach while blamed on an intern for setting a bad password, shows that the company had room for improvement of their security policy and technical controls. She points out that there is currently software available that can be implemented to enforce password complexity policies and that an intern should not have had access to a production server that affects over 18,000 customers (Carlton, 2021).

Lack of transparency is another issue that increases the difficulty of measuring supply chain risk. Unlike risks within your own company, you may not have as much privilege to review your suppliers’ security postures. As Tucker Bailey, Edward Barriball, Arnav Dey, and Ali Sankur put it "In complex products, Tier 1 or 2 suppliers may consider their supply chains to be proprietary, limiting visibility at the purchaser or integrating-manufacturer level” (Bailey, et al, 2019). If companies could demand to probe suppliers for security weaknesses, this could pave a path for industrial espionage. All a competitor or foreign government would need to do is purchase Microsoft Windows and then they would have cause to request the source code to probe for vulnerabilities and backdoors. They could then steal the source code instead of “looking for vulnerabilities” or use vulnerabilities found to attack other governments and companies using the operating system. This creates a difficult problem as too much transparency renders the competitive advantage of a software vendor useless and too little transparency causes customers to question whether they may trust a company and creates difficulty in accurately assessing risk to their organization.

Another perspective on this is to consider the Stuxnet worm of 2010-2012. The malware was not detected by systems because it was signed by legitimate certificates which were used by computers to detect if software was safe (Schneier, 2018). Theses certificates were stolen from a certificate authority in Taiwan. This is the part that causes this attack to fall into the supply chain risk category. Users of computers had no insight into the certificate authority’s operating procedures which can degrade consumer trust in the certificate authority or enable blind trust that could still lead to compromise.

Another risk source comes in the shape of the access required/requested by members of your supply chain. For instance, Target’s payment systems were breached by attackers with credentials stolen from a heating, ventilation, and air conditioning (HVAC) contractor (Krebs, 2014). It goes without saying that an HVAC contractor should not have access to the payment card network. If there were control systems for the HVAC units that needed to be connected to the internet, they should have their own separate internet connection or they should be on a separate network at the least. Technically, I would recommend connecting them into a DMZ network, but that is beyond the scope of this paper, and we will not discuss it further here. The main point is that there are ways to limit access to networks and information for almost all software or hardware devices and we must be prepared to carefully consider where we put things and the access we grant them.

One could argue that war and natural disaster are also risk sources for disruption of supply chains. For instance, during the early stages of the COVID19 Pandemic, we saw sudden increases in the purchase of computers and home office equipment as people had to find ways to work from home during lockdowns and prohibition of gatherings. This led to shortages for a time as supply chains had to adapt to an increased demand. This kind of risk affects products in cybersecurity because employees need computers and networking equipment to maintain and create software/hardware products or cybersecurity services.

## 

## Due Diligence for Acquisition

Due diligence is one of the areas of risk management that may be hard to recognize when done right but is easily seen when done wrong. Defining due diligence in acquisition is one of the best ways to keep on track and ensure appropriate coverage of risks. It is often helpful to follow a checklist or make your own to ensure that you don’t forget to ask any questions along the way of the acquisition. It also allows you to keep track of what you have asked and provide a timeline or estimate of timeliness of your part of the acquisition. Microsoft published a great checklist for cloud acquisitions (Microsoft 2021). This isn’t surprising seeing that they are a cloud provider themselves, but it is a great resource, nonetheless. I will go over five important questions that should be asked during an acquisition for due diligence.

The first question that should be asked is “Is this company stable and will they reliably be available to meet our supply needs?”. In the cybersecurity industry, supplies can range from hardware for application hosting such as AWS or Microsoft Azure to staffing and personnel. If you depend on a supplier to give you a continuous stream of cybersecurity staff for your Security Operations Center and the flow of personnel suddenly dies, then your company may become overloaded with alerts and cases to work. The flow of employees never stops. As people grow older and more experienced, they either retire or move on to other opportunities that come along. It is important to pick your staffing firm accordingly or have a backup firm if personnel are a resource that you go through quickly which is often the case in the IT security community.

The second question you should ask is where your data may be stored or where the company is located. What foreign/competitor interests would they have that could make them subject to bribery or espionage? This would tie in with foreign control and interference risk source identified in the previous section. Microsoft specifically addresses cloud risk management when recommending companies request the geographic locations that data is stored and processed (Microsoft 2021). This will help you make an informed decision on whether the location that data is stored or processed in will incur risk of theft, destruction, or manipulation of the data.

The third question comes from Deloitte’s article “Due diligence for Mergers and Acquisitions through a cybersecurity lens” (Shukla, 2021). What is the supplier’s track record with cybersecurity? Look for any trends in their history regarding the securing of information or the lack thereof. The past doesn’t always determine the future, but it gives us a good place to start our assumptions.

Another question is brought up by Cross Country Consulting (2021) is asking yourself who your critical suppliers are. You need to be aware of risk sources to identify the risks they pose. By identifying who your suppliers are and who their critical suppliers are, you can stay on top of economic, political, and social situations that they are involved in and make informed risk-based decisions.

Once you know who your suppliers are you can look at their risks asking yourself and them what their risks are. Have you conducted or required them to conduct a risk assessment? Cross Country Consulting (2021) asks this question as well. It is an important question to ask yourself if you want to actually get proof of your assumptions of risk. As was mentioned in the Supply Chain risk section, a company may not always have transparency into their operations and vulnerabilities. However, it does not hurt to ask, and there is likely an agreement that may be come to regarding risk assessment.

## Best Practices for Managing Global Supply Chains

In their article “Addressing supply chain risks during the M&A due diligence process”, Cross Country Consulting (2021) recommends keeping an inventory of suppliers. This gives the assessor an overview of their risk sources which allows them to start evaluating different links that may have/cause issues in the supply chain.

Rob Pate (2020) makes the following recommendations in an interview with Digital Guardian’s Data Insider blog on supply chain cybersecurity:

* Conduct background checks on employees before hiring them
* Know your vendors, suppliers, and partners and verify their security practices and procedures
* Ensure only a small handful of people are able to make purchases or acquisitions and that they are run by the security department first.

Pate’s first two bullet points can be consolidated into three words: Trust, but verify. It is good to foster a relationship of trust between employees and employers and to some extent it is needed. However, when the security of your clients’ data and your company’s trade secrets are on the line, it is prudent to ask for reasonable assurance that your suppliers and partners are secure enough to meet your company’s risk appetite.

Digital Guardian also interviews Adrienne Johnson (2020) who recommends performing risk assessments on vendors and writing in protections to your contracts with them. This helps you answer the question stated in the Due Diligence section of whether you’ve conducted a risk assessment of the vendor with the bonus of making it an expectation since it is written into the contract from the start and not something that has to be renegotiated at a later date when stakeholders are asking for quick answers or you have the pressure of the media on you. Johnson (2020) also corroborates the idea of least privilege and technical controls to protect the supply chain from insider threats. These would ensure that even if the supply chain is compromised, they do not get far on your network and are restricted to only systems and information that they need to deliver whatever product or service they are delivering to you.

# Summary and Conclusions

Supply chains are vital to the success and security of our businesses no matter how big or small. Every company gets a resource of some type or another from somewhere whether it be personnel, lumber, code, or network infrastructure hardware and designs. The security of the supply chain effects both the customer and supplier and as such is the responsibility of both. If the supply chain fails, the supplier loses reputation or contracts, and the customer loses resources vital to their business or confidentiality/integrity of data/products leading to degraded consumer trust. All will either come together to protect the cybersecurity supply chain or face the consequences and risks of leaving it unguarded and open to attack.

# References

Australian Cyber Security Centre. (2021). Identifying cyber supply chain risks. <https://www.cyber.gov.au/acsc/view-all-content/publications/identifying-cyber-supply-chain-risks>

Bailey, T., Barriball, E., Dey, A., & Sankur, A. (2019, March 8). A practical approach to supply-chain risk management. McKinsey & Company. <https://www.mckinsey.com/business-functions/operations/our-insights/a-practical-approach-to-supply-chain-risk-management>

Carlton, A. (2021, March 4). Why the SolarWinds hack wasn’t an intern’s fault. Medium. <https://medium.com/digital-diplomacy/hey-executives-interns-are-never-the-root-cause-of-your-security-breach-46781f41ea1>

CrossCountry Consulting. (2021, April 27). Addressing supply chain risks during the M&A due diligence process. <https://insights.crosscountry-consulting.com/addressing-supply-chain-risks-during-the-ma-due-diligence-process>

FireEye. (2020, December 13). Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with sunburst Backdoor. <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

Johnson, A. (2020, September 25). Supply chain cybersecurity: Experts on how to mitigate third party risk. Interview by N. Lord. Digital Guardian. <https://digitalguardian.com/blog/supply-chain-cybersecurity>

Krebs, B. (2014, February 5). Target hackers broke in via HVAC company. Krebs on Security – In-depth security news and investigation. <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

Microsoft. (2021). Cloud services due diligence checklist. Retrieved July 31, 2021, from <https://www.microsoft.com/en-us/trust-center/compliance/due-diligence-checklist>

Pate, R. (2020, September 25). Supply chain cybersecurity: Experts on how to mitigate third party risk. Interview by N. Lord. Digital Guardian. <https://digitalguardian.com/blog/supply-chain-cybersecurity>

Robertson, J., & Riley, M. (2018, October 4). The big hack: How China used a tiny chip to infiltrate U.S. companies. Bloomberg Businessweek. <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

Schneier, B. (2018, February 2). Signed malware. Schneier on Security. <https://www.schneier.com/blog/archives/2018/02/signed_malware.html#:~:text=Signed%20Malware%20Stuxnet%20famously%20used%20legitimate%20digital%20certificates,malware%20is%20much%20more%20common%20than%20previously%20believed>

Shukla, G. (2021, June 15). Due diligence for mergers and acquisitions through a cybersecurity lens. Deloitte. <https://www2.deloitte.com/global/en/blog/responsible-business-blog/2021/due-diligence-for-mergers-and-acquisitions-through-a-cybersecurity-lens.html>