***Introduction***

Hello, my name is Jason Rivers, and I’m in Group 4. Our group consists of Mhaliek Ferguson, Narcisse Teyiri, Hailey Thompson, and myself. We’ve been discussing out topic over text for about a week, and our Proposal will be protecting Supply Chains from attacks. To achieve this, what we aim to do is establish a system of supply chain security audits that will assess and verify the security protocols and habits of vendors and/or businesses and offer assistance or help them reassess their security model. This topic manages to cover all of our majors (Cybersecurity, CyberOps, and Business) and addresses a huge concern that plagues parts of the IT business world today.

***The Problem at Hand***

The supply chain for business and vendors comes under constant attack every day from a world of factors, which could damage business interests, impede profits, and could lead to catastrophic failure both in the affected business, and throughout the market. Supply chains have been identified as one of the weakest links in a business’ apparatus (Cordon, 2022). Not only does a supply chain face issues with logistics, transportation, manpower, but of course security as well. These security concerns range from vulnerability of business data, logistical information, and employee information to legal risk should this information be compromised, as well as threats from inside a supply chain apparatus as well. This doesn’t just include big corporations, and businesses, but third-party vendors as well. I would personally argue that third-party vendors in a supply chain actually face the harshest threats from both cyber-threats, and physical security threats. The need for a proper auditing system to ensure they are as secure as they can be both online and off is dire, and that’s where we come in. Before we address how we can help however, let’s look at some examples of supply chain security lapses due to lack of peoper security auditing.

Two of the biggest supply chain attacks in recent memory have got to be the SolarWinds supply chain attack in 2020, and the 2017 NotPetya attack launched against Ukraine, both of which were launched in the same way, and both have been attributed to Russian state-sponsored hacking, but that’s not the issue. The issue is that in both cases, the server of software vendors for an update was compromised, and a very vicious malware was spread to tens of thousands of people who unknowingly updated their software and devices with this malware. After the update was finished, the malware would begin its work.

In the case of SolarWinds, the Orion platform was compromised by malicious code called a Remote Access Trojan, or RAT, with a backdoor being opened for hackers to access system files, business records and other configurations, and hide their actions in these compromised systems as well. The update gave them remote access to over 18000 victims, and their devices, in various businesses worldwide. Hackers were able to bypass SolarWinds security and access the server to upload the tainted update thanks to security oversights, and a lack of proper security auditing (Jena, 2023). Not only could vendor security lapses harm businesses, but they could cripple nations as well.

The next example of a vendor supply chain attack is also rather well known, and effectively crippled a modern nation until it was brought under control. NotPetya, a virus similar to the one used against SolarWinds was uploaded to a vendor server and sent out as an update to devices across Ukraine, crippling its IT infrastructure nationwide, and leading to a massive recovery effort which cost the country more than $10 billion USD before it was all said and done. These two incidents alone, though massive in scale, prove that even small IT vendors need security oversight. Now, before this proposal ends up sounding too much like a research paper, let us tell you where we come into this.

***Our Solution***

Our solution to protecting supply chains, and fixing any potential issues are to establish a 3rd party audit company to assess a company’s supply chain security, including cybersecurity, technical security, and physical protections. A unique, fair, and unbiased assessment is best for any organization; we can accurately assess the systems and protocols in place at a company, whether those protocols follow best practices, as well as how well employees of the company are versed in such practices. Employees are, unfortunately, often the weakest link in a company or organization’s security apparatus, so we like to focus on employee knowledge, and how well they follow their training. Next, we would analyze and assess the general strategy an organization has developed their supply chain around. While an efficient strategy may be useful for maximizing profits, it can sometimes clash with how secure and safe it is for customers and employees alike. Without a proper assessment, even the most efficient supply chain system can potentially collapse under its own weight following one simple intrusion. Our goal is to help assess an organization’s supply chain security and suggest changes without compromising much of its efficiency; that could be just as harmful as an attack in the long term.

As stated before, the assessment will also recommend changes to a supply chain’s security, be it IT, technical, or physical, if the need arises. Examples of this may be dangerous or insecure manufacturing or distribution sites, corruption among individual vendors, theft, easy to access-and-traverse onsite and online network computers, and many other threats. Any one of these threats, or combination of them could damage a supply chain’s infrastructure and logistics, but with oversight and auditing, we can reduce these risks to miniscule possibilities.

Finally, in addition to the audit and assessment, we will recommend risk management strategies, and recovery plans, should the worst come to pass. It’s often considered a fact at this point that half of cybersecurity focuses on preventing an attack from happening, while the other half focuses on recovery from an eventual, successful attack and we would like to adopt that mindset. There is no possible way to mitigate all risk factors, even if they’re all identified; we can only recommend changes, best practices, and recommend enforcement as needed. Reducing risk will in turn reduce the chances of an event occurring, but to reduce overall damage that could potentially be dealt, an organization needs to have at the very least, a strategy to minimize damage from a variety of harmful events and effectively recover to minimize business losses. While our recommended recovery plans, and even assessments may not be the best fit for every single organization, we can work with the organization to modify it to fit their own unique business needs.

***Our Main Barriers, and Goals***

Our main barriers will be training employees to be mindful and properly assess each organization’s potential security shortfalls, and issues. Every organization has its own unique business goals, and strategy. Our job as auditors is to work around that, assess where their security is lacking according to both best practices, and their own unique business situation, and make recommendations, feedback, and potentially draft recovery plans if necessary. We would also need to earn the organization’s trust and make sure our employees know not to discuss a company’s shortfalls outside of business audits. Selling a company’s security weaknesses to a competitor, or hacker, is not only unethical, but highly illegal, and this needs to be drilled into all of our potential employees. Another barrier is our supply chain audits will often focus on only one sector of an organization’s supply chain or vendors. While we can assess that one sector fairly well, unless we do a full in-depth audit across the entirety of a supply chain getting a full idea of their security issues would be close to impossible. The resources and time we would need to dedicate to a full-scale audit would also be astronomical depending on the organization’s size. This means that for a time, our focus will be on segmental auditing of a supply chain due to our size and available resources.

Our goals will be to successfully audit and recommend changes and improvements to an organization’s supply chain without compromising its efficiency or effectiveness. In general, this has no end goal in mind; it will be a case-by-case basis with the overall goal of improving supply chain and vendor security which will in turn protect business interests and partners, consumers who work with the business, and the employees who work for and rely on the business. We will know we’re successful when the businesses we work with for audits report lower security breaches, losses, and we receive more audit requests from other businesses as a result. Many of the specifics such as pricing model, growth planning and tracking, as well as employee requirements, and securing the legality of our work are still being ironed out, but the foundational information we have set in stone.

*I know this isn’t a research paper, but I included sources for where I got my information for the sake of transparency.*

***Works Cited:***

Cordon, C. (2022, September 6). *“a supply chain is as strong as its weakest link.”* I by IMD. https://www.imd.org/ibyimd/videos/a-supply-chain-is-as-strong-as-its-weakest-link/

Jena, B. K. (2023, September 25). *Solarwinds Attack & Details You Need To Know about it: Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack#how\_did\_the\_solarwinds\_attack\_happen