Today's Cyber Warfare: Protecting Supply Chain Integrity and Data Privacy

Organizations that aren't actively implementing robust cyber risk-mitigation and liability-reduction strategies in their supply chains could face costly operational disruptions and run the risk of falling out of compliance with laws and regulations, including privacy requirements.

In today's world, cyber guerrilla warfare occurs in every corner at any moment. That's not an overstatement. Malware, spyware, and cyber espionage lead to data compromise and data theft every day. Ransomware takes data hostage on an hourly basis. The exposure of private information belonging to individuals, for-profit companies, local and national governments, non-profits, schools, health providers, and more causes disruption and chaos. Threats to our data security and data privacy have become so "normal" that nearly everyone seems to expect that private account information, emails, intellectual property rights, and other records will eventually be pilfered, held captive, copied, laid bare, or otherwise put at risk. Data integrity and privacy are of significant concern throughout enterprises and their supply chains.

How do we protect ourselves from this cyber menace? How do we safeguard things as dear as our privacy and our data, as well as the data of our customers and contacts?

Thankfully, there are defensive measures we can take to help mitigate this risk, including some that are deep in the digital domain. One that too often receives insufficient attention and action has to do with shielding against breaches of supply chains. This is keenly important because hostile threat actors are targeting commercial and public sector supply chains for many reasons, including to gain access to data. They can violate the integrity and privacy of data by exposing information for the world to see, selling data to the highest bidder, or holding data hostage for a financial ransom.

Guidehouse

Organizations that aren't actively implementing robust cyber risk-mitigation and liability-reduction strategies for their supply chains to prevent these sorts of data and privacy abuses could face significant costs, operational disruptions, reputational damage, and other harms, as well as penalties for non-compliance with laws and regulations. A supply chain risk management program also needs to include third party vendors, and to ensure an effective data protection program, those vendors must be held to the same cybersecurity and data privacy standards as the organization.

Data and Privacy: Some Statistics Related to Supply Chains and Cyber Warfare

Companies are increasingly finding themselves or their third-party vendors to be the targets of cyber warfare. In 2021, SolarWinds, a major US network- and systems-management software provider, was infiltrated by a cyberattack believed to have originated in Russia. The breach went undetected for months and spread to many of the company's clients, including the US Department of Homeland Security and the Treasury Department. A year later, the identity-management firm Venafi released a survey revealing that 64% of businesses surveyed suspect they've been directly impacted by a nation-state-sponsored cyberattack[1]. According to the Federal Trade Commission, Americans lost more than $5.8B to fraud in 2021, a 70 percent increase from 2020[2].

The Emerging Cyber Warfare Landscape

The current cyber warfare landscape is complex and constantly evolving. Companies are not just being targeted because they offer back doors into government or business networks. Indeed, sometimes the agencies or companies targeted provide critical services or possess strategic information. A foreign nation, for example, could attack a defense contractor to steal intellectual property and design specifications. But companies are also at risk of being targeted when an attacker sows chaos, disrupts supply chains, places systems offline, or holds critical products, services, or components hostage with ransomware.

The potential of these kinds of attacks to severely impact the US should deeply concern everyone, and especially companies that own the systems and networks that are carrying out their business operations. Think of attacks where payment processing services nationwide suddenly stop working. Or where a utility is taken out for days, leaving entire states without power during severe weather.

Supply Chain Risks

Yet, despite the elevated risk, most companies aren't prepared to meet the challenge of cyber warfare. Venafi also found that 63% of companies didn't think they would even know if they were hacked by a nation-state[3]. This stems in part from the fact that the majority of organizations are uninformed about the nature of the cyber risks in their supply chain, where many breaches actually originate. But companies should pay close attention.

Those that are not proactively implementing a cyber risk-management and liability-reduction strategy that includes securing their supply chain, could face serious consequences in the future. These might include fines, sanctions, reputational damage, disruptions to supply chains, disruptions to services, loss of customers, lawsuits from customers, denials of cyber insurance claims, and orders to become compliant. Emerging data protection and privacy regulations also point toward the

What does Cyber Warfare Risk Mitigation Look Like in Supply Chains?

Companies need to better understand the existing cyber risks in their supply chain and how to mitigate them. They can do this by:

- Creating stricter service-level cybersecurity agreements with their third-party service providers.
- Conducting supply chain illumination on suppliers' supply chains.
- Researching any past cyber incidents suppliers have experienced.
- Getting cybersecurity risk scores on companies in their supply chain.
- Looking for threat actors and sanctioned entities in their supply chain.
- Exploring different suppliers via strategic sourcing.
- Implementing a robust data protection and privacy program that addresses the entire data lifecycle and ensures data is encrypted at rest and in transit and storage.

need for companies to address existing supply chain cyber risks. The time to act is now. It's critical that companies fully understand the risks and take steps to protect themselves.

Cyber Warfare and Corporate Entities

When it comes to cyber warfare, one might think defense contractors are more likely to be targeted. In actuality, threat actors and nation-states target a variety of industries. Banking, finance, healthcare, infrastructure, and technology companies are often the focus of attacks. But the exact targets vary considerably depending on the attacker's goals.

Some state actors are simply out to ransom a company's data so they can use the funds for other purposes, as North Korean state-sponsored hackers are purported to do[4]. Others are after strategic information or access to a company's customers' networks. But with everything connected to a network, there is greater potential for cyberattacks to cause chaos or tragedy. Just think of the impact an attack could have on an IoT-connected provider of pacemakers and medical dispensers. If the company is not prepared, lives could be lost as a result.

Disrupting critical public or corporate infrastructure would also have significant impacts on both nations and corporations. While one might expect state-sponsored hacking to be targeting sensitive US federal intelligence agencies, sometimes the target is a company's intellectual property. Chinese government-linked hackers, for instance, are reported to focus on industrial espionage to steal intellectual property and individuals' private data en masse[5].

Supply chains remain a point of vulnerability for many companies, even those that are otherwise on top of their cybersecurity risk management. The numbers and impact of such attacks are growing. Malicious actors can often infiltrate organizations through their supply chains due to insufficient security practices or social engineering. For example, with digital services, attacks are often hard to pinpoint since they generally piggyback on legitimate processes, like corrupted code inserted into automatic software updates. Indeed, that was how the SolarWinds attack managed to spread to the company's clients and federal agencies. A supplier's supplier might be controlled or infiltrated by a malicious actor or owned by a sanctioned state and could insert malware or harmful code into hardware. Attacks could also be targeted at supply chains to compromise a company's ability to produce critical components or products.

Without careful oversight and illumination of a company's supply chain, the risks aren't even quantifiable. Yet, research suggests there is mounting danger to companies from things like unverified or disreputable suppliers, a lack of risk assessments of third-party vendors, weak partner agreements around cybersecurity, and a lack of code transparency. These dangers must be addressed so companies can properly mitigate risk and reduce their potential liability.

The Importance of Preparation

Increasingly, organizations and state entities are paying attention to these risks and requiring companies to do so as well. On May 12, 2022, President Biden issued Executive Order 14028: Improving the Nation's Cybersecurity[6]. The order focused on things like cloud security, zero trust, and enterprise security. The order explicitly addressed the need to improve software supply chain security by developing a baseline security standard for software sold to government agencies. This will require developers to provide greater visibility into their code and make their security data publicly available. The order also established a Cyber Safety Review Board to evaluate significant cyber incidents.

Companies should be aggressively preparing to meet these additional cybersecurity and supply chain standards. Not acting now on potential threats could expose companies to future accusations of negligence, especially if a company was aware of a vulnerability and did nothing to address it. Some sectors also have industry-specific cybersecurity requirements that could result in sanctions from oversight boards when a company is the target of a successful attack that it did not take adequate precautions against. US states have also expressed a greater appetite in recent years for further regulating both cybersecurity and privacy. Now is the time for companies to be proactive.

Consequences of Supply Chain Cyberattacks

Companies that experience supply-chain-related cyberattacks could face severe consequences. Here are some of the risks:

- Fines
- Sanctions
- Reputational damage
- IP theft
- Ransomware payouts
- Disruptions to supply chains
- Disruptions to services
- Loss of customers
- Lawsuits from customers
- Denials of cyber insurance claims
- Orders to become compliant

Supply chain risk illumination work

Reviews of SBOMs

Software code reviews

Beneficial ownership evaluations

Component reviews

Potential supply chain threats

How to Mitigate Risk

It is critical for companies to illuminate their supply chains to better understand their cyber risks and limit their cyber liabilities. This process includes things like conducting supply chain risk illumination work, software code reviews, component reviews, review of software bill of materials (SBOMs), beneficial ownership evaluations, and exploring the ways a company's supply chain might be infiltrated by threat actors.

Doing this critical work will help companies better understand the threat landscape and their particular risk exposures. They can then proactively reduce their risk and liability by exploring different suppliers, implementing alternative network architectures, creating a partner-vetting protocol to reduce future risk, and strategically sourcing software and services. These actions, in concert with comprehensive cybersecurity and data protection and privacy programs, are critical to mitigating cyber risks. In many industries, preventing breaches proactively could save companies millions in fines and other consequences.

Conclusion

When it comes to cyber warfare, organizations face significant and wide-ranging risks. It is critical that companies work proactively to mitigate risk and reduce liability around potential attacks originating in their supply chains.

Guidehouse has a long track record of supporting federal and corporate partners in cybersecurity and supply chain risk-management projects. Guidehouse also has deep industry expertise in many sectors to help companies ensure they comply with all sector-specific cybersecurity requirements. Guidehouse is well-placed to help businesses build a cybersecure supply chain that limits their risk and prepares them for the brave new cyber future.

[1] Venafi. *The (Nation) State of Cyber: 64% of Businesses Suspect They've Been Targeted or Impacted by Nation-State Attacks,* 2022. https://www.venafi.com/blog/nation-state-cyber-64-businesses-suspect-theyve-been-targeted-or-impacted-nation-state-attacks

[2] New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021. https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

[3] Venafi. The (Nation) State of Cyber: 64% of Businesses Suspect They've Been Targeted or Impacted by Nation-State Attacks, 2022. https://www.venafi.com/blog/nation-state-cyber-64-businesses-suspect-theyve-been-targeted-orimpacted-nation-state-attacks.

[4] Cybersecurity and Infrastructure Security Agency. North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-187a.

[5] CNN. Chinese hackers cast a wide net for trade secrets in US, Europe and Asia, researchers say, 2022. https://www.cnn.com/2022/05/04/politics/china-hackers-economic-espionage-manufacturing/index.html.

[6] Cybersecurity and Infrastructure Security Agency. Executive Order on Improving the Nation's Cybersecurity, 2022, https://www.cisa.gov/executive-order-improving-nations-cybersecurity#:~:text=On%20May%2012%2C%20President%20Biden,economy%20and%20way%20of%20life.

Contacts

Rodney Snyder, Partner
Cybersecurity Solutions
rsnyder@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 17,000 professionals in over 55 locations globally. Guidehouse is led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

guidehouse.com/services/cybersecurity

@GHTech Solutions linkedin.com/showcase/guidehouse-technology-solutions/