Published on *The National Law Review* https://natlawreview.com

Ukraine Crisis Increases Supply Chain Cyber Risk

Article By:

Anjali C. Das

The current geopolitical climate and escalating crisis in Ukraine are amplifying concerns about the increased cyber threat to global supply chains that are already strained by the COVID-19 pandemic. This is perhaps the first time in history that the threat of cyber warfare is potentially just as devastating as the physical battle taking place on the ground. Government officials are cautioning organizations to be prepared for an increase in cyber-attacks on businesses and critical infrastructure.

Last year, cyber threats on global supply chains were in the spotlight following the unprecedented cyber-attacks on Colonial Pipeline, JBS, and SolarWinds, attacks that had far-reaching consequences for downstream businesses, customers, and individual consumers.

Background

In May 2021, Colonial Pipeline was the victim of a ransomware attack that forced the company to abruptly shut down the pipeline and suspend all operations for the first time in its history. This led to an immediate disruption in the nation's fuel supply along the Eastern Seaboard, causing shortages and spikes in the price of gas. Later that month, a ransomware attack targeted JBS, one of the largest meat producers in the world, and forced the company to temporarily shutter its U.S. facilities, which supply 23 percent of the nation's beef.

According to various sources, both attacks were perpetrated by cybercriminals (REvil and DarkSide) with ties to Russia, although White House officials stopped short of declaring these attacks to be state-sponsored. In the case of JBS, law enforcement was successful in shutting down the bad actors and recovering $2.3 million of the $4.3 million ransom paid by JBS.

In April 2021, the New York Department of Financial Services (NY DFS) issued a Report on the SolarWinds cyber-attack.[1] According to NY DFS, the SolarWinds attack was attributed to a sophisticated cyber espionage campaign by Russian Foreign Intelligence Services actors. SolarWinds saw signs of hackers about eight months earlier than the disclosed timeline and nearly two years before anyone discovered the breach.

SolarWinds is a software company with more than 320,000 customers including government, financial services and telecommunications companies. Hackers gained access to a SolarWinds

software product, known as Orion, designed to monitor an organization's network. Hackers inserted malicious code into Orion that was then installed on the systems of SolarWinds's customers. This enabled the hackers to gain access to customers' internal networks and information stored on these systems. NY DFS characterized the SolarWinds incident as a "wake-up call" for all organizations – not just the financial services industry – that highlights the "existential threat" and "vulnerability of supply chain attacks."

Response

On January 11, 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and National Security Agency (NSA) issued a joint Cybersecurity Advisory warning organizations of the increased risk presented by cyber threats.[2] In particular, the Advisory provides an overview of commonly observed tactics and techniques used by Russian state-sponsored cyber operations and guidance on how to mitigate cyber risk posed by these and other threats. According to the Advisory, Russian-backed advanced persistent threat (APT) actors have demonstrated increasingly sophisticated capabilities designed to compromise third-party infrastructure and third-party software, in addition to developing and deploying custom malware that can gain access to computing environments without detection for long periods of time.

The Ukraine Factor

Since the escalation of the Ukraine conflict, Ukrainian officials have lauded the efforts of the "IT Army of Ukraine" comprising 400,000 volunteers that are targeting the Russian government, taking down its banking websites, attacking its military systems and providing intelligence. This is perhaps the first time in history that a government has publicly recognized and recruited a cyber-espionage "army" to assist its defensive military operations. Meanwhile, a gang of cybercriminals known as "Conti" have publicly supported Russia in cyber warfare. In a recent report by the U.S. Department of Health & Human Services (HHS), the agency noted that Conti has historically targeted U.S. health care organizations with ransomware attacks that both encrypt systems and steal information.[3]

U.S. Legislative Effort Awaits House Approval

In recognition of the growing risk of cyber-attacks on U.S. critical infrastructure, supply chains and businesses, the Senate recently passed a bill known as the Strengthening American Cybersecurity Act. The Act, which has yet to pass the House, includes provisions that would require critical infrastructure organizations[4] to report "substantial" cyber-attacks to CISA within 72 hours. Moreover, organizations that make ransom payments to cybercriminals would be required to report this fact to CISA within as little as 24 hours. The Act is designed to encourage (and mandate) public-private sector communication and cooperation regarding cyber threats that could have devastating consequences for the country.

All of these recent developments highlight the need for all organizations across all industry sectors to recognize that cyber threats pose significant risks and costs including supply chain disruption, economic costs, reputational harm and safety concerns. As noted by NY DFS in its SolarWinds Report, organizations should adopt a "Zero Trust" approach and prepare for breaches in the supply chain.

Prepare for the Worst

All organizations should take steps to mitigate cyber risk in part by focusing on critical vendors and third-party service providers. In fact, a number of existing and soon-to-be enacted cybersecurity laws and regulations legally require organizations to assess, manage and mitigate third-party cyber risk.

For instance, NY DFS Cybersecurity Regulations, 23 NYCRR 500,11, require licensed organizations to implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to or held by third-party service providers. The organizations' policies and procedures should address:

- The identification and risk assessment of third-party service providers
- The minimum cybersecurity practices that these providers must satisfy
- Due diligence processes used by an organization to evaluate the adequacy of a provider's cybersecurity practices
- Periodic assessments of providers based on the risk they present to the organization.

In the event of a cyber-attack, the January 11, 2022, joint Cybersecurity Advisory by CISA, FBI, and NSA recommends that organizations take the following steps:

- Containment. Immediately isolate affected systems.
- Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
- Conduct an investigation. Collect and review relevant logs, data and artifacts to analyze the nature and scope of the threat actor activity within the environment.
- Remediation. Consider soliciting support from a specialized cybersecurity firm to ensure that any bad actor is eradicated from the network and avoid residual issues that could result in follow-on exploit attempts.
- Report incidents to applicable regulators and law enforcement.

---

[1] *See* NY DFS Report on the SolarWinds Cyber Espionage Attack and Institutions' Response (April 2021) found here.

[2] *See* Alert (AA22-011A), "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure found here.

[3] *See* HHS Report 202203011700, "The Russia-Ukraine Cyber Conflict and Potential Threats to the U.S. Health Sector" (March 1, 2022) found here.

4 Critical infrastructure industries include chemicals, communications, critical manufacturing, dams, defense industrial bases, emergency services, energy, financial services, food and agriculture, government, health care, information technology, nuclear reactors and transportation, among others.

National Law Review, Volume XII, Number 70