



PROTECTING CRITICAL SUPPLY CHAINS

Building a Resilient Ecosystem





OVERVIEW

Public and private organizations must defend themselves from evolving—and increasingly sophisticated—cyber supply chain attacks. Foreign adversaries and non-state actors conduct campaigns that target supply chains—either directly or through proxy groups—to advance their global ambitions. These threat actors position themselves throughout the supply chain, fully aware that organizations trust and depend on this critical, complex, diverse, and distributed ecosystem. While the global supply chain saves money and accelerates innovation, it also exposes a multitude of vulnerabilities. All organizations must understand that their relationships with suppliers, vendors, customers, and users are increasingly abused by foreign adversaries to:



access protected networks and data;



exploit network components and vulnerabilities, move across trust boundaries within networks, and extend dwell time within a network;



conceal their actions for plausible deniability; and



delay or limit defenders' response, especially in a crisis or conflict.

Foreign adversaries' military and economic strategies have evolved to include the use of sophisticated tactics, techniques, and procedures (TTPs). Organizations can help mitigate these actions by enhancing foundational security practices, including applying techniques from law enforcement and cybersecurity advisories. These steps can help identify potential threats and reduce risks

to their most trusted supply chain relationships. Careful evaluation of these cyber tactics enables organizations to avoid costly mistakes. Organizations should not assume a threat actor's apparent restraint indicates a lack of intent or capability. Today's threat actors align their planned actions in proportion to the perceived near-term cost and reward.

The People's Republic of China (PRC) is especially adept at abusing trusted supply chain relationships to achieve a desired end state. As FBI Director Christopher Wray has recently noted:

Today and literally every day, they're [PRC] actively attacking our economic security, engaging in wholesale theft of our innovation and our personal and corporate data. Nor is cyber the only PRC threat we face. The PRC cyber threat is made vastly more dangerous by the way they knit cyber into a whole-of-government campaign against us. They recruit human sources to target our businesses, using insiders to steal the same kinds of innovation and data that their hackers are targeting while also engaging in corporate deception. Hiding Beijing's hand in transactions, joint ventures, and investments to do the same. And they don't just hit our security and economy, they target our freedoms.¹

This quote demonstrates the strategic campaign the PRC employs through multiple supply chain threat vectors to achieve their desired effects. For example, the PRC will leverage foreign direct investment, overseas acquisitions, legal technology imports, foreign research and development (R&D) centers, joint ventures, research and academic partnerships, talent recruitment, cyber espionage, and theft of intellectual property to gain access to foreign technologies. Further, the Chinese People's Liberation Army's (PLA) modern warfare theory includes positioning themselves on opposing networks as a method to paralyze, sabotage, and destroy an enemy's cyber and non-cyber assets on demand. Blended supply chain attack campaigns like these mark an evolution in foreign adversaries' capabilities.



CYBER SUPPLY CHAINS ARE THE MOST EXPLOITED VECTOR

In recent years, nation-state cyber attackers have used “Living-off-the-Land” (LOTL) techniques, such as hiding malware on an organization’s trusted third-party software and firmware applications (tools) in order to conduct attacks, often avoiding detection for a prolonged period. These techniques allow cyber threat actors to appear in logs as “normal” network traffic to sustain initial access and evade detection. Because these applications are trusted by the organization, threat actors can remain in an organization’s network for prolonged periods, creating a foothold that preserves access for future activity. Nation-state cyber actors may also exploit other vulnerabilities—including zero-days, unpatched software defects, or phishing campaigns—to gain initial access to networks or data.

Recent examples of nation-state cyber campaigns include:



Since 2022, PRC actors dubbed “Volt Typhoon” have engaged in a campaign of cyber activity against U.S. critical infrastructure. Cyber threat actors from the PLA used LOTL techniques to compromise Small Office/Home Office (SOHO) devices, and establish persistent access on critical infrastructure networks located in the U.S. and Guam.



In March 2024, according to open-source information, the Republic of Korea’s National Intelligence Service (NIS) disclosed a North Korean campaign to acquire semiconductor product design drawings through LOTL techniques. To circumvent U.S. sanctions and potentially advance their own semiconductor sector, North Korea actors compromised two South Korean semiconductor companies’ networks.



In April 2024, CISA issued Emergency Directive 24-02 in response to a recent campaign by Russian state-sponsored cyber actor Midnight Blizzard—the Russian Foreign Intelligence Service—targeting Microsoft corporate email accounts, and potentially accessing correspondence with Federal Civilian Executive Branch (FCEB) agencies. Midnight Blizzard used information initially exfiltrated from Microsoft corporate email systems, including authentication details shared between Microsoft customers and Microsoft by email, to gain—or attempt to gain—additional access to Microsoft customer systems.²



In May 2024, the FBI released a Public Industry Notification (PIN) that highlights cybercriminals—tracked publicly as STORM-0539—targeting national retail corporations with phishing and smishing campaigns. The actors intended goal is to gain unauthorized access to employee accounts and corporate systems to target the gift card department and create fraudulent gift cards. In one instance, a corporation detected STORM-0539’s fraudulent gift card activity in their system, and instituted changes to prevent the creation of fraudulent gift cards. STORM-0539 actors continued their smishing attacks and regained access to corporate systems. Then, the actors pivoted tactics to locating unredeemed gift cards, and changed the associated email addresses to ones controlled by STORM-0539 actors in order to redeem the gift cards.

“PRC operations discovered by the U.S. private sector probably were intended to pre-position cyber attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia. If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.”

- Annual Threat Assessment of the U.S. Intelligence Community (2024)



Protecting Critical Supply Chains: Building a Resilient Ecosystem

The cyber campaigns outlined above highlight the evolving tactics of these nation state actors. Initial access to an organization's cyber network is not typically the end goal. With positioning and access, foreign adversaries can escalate their actions to co-opt or coerce organizations at will.

Foreign adversaries breach, or otherwise leverage, organizations that have access to intended targets through a trusted third-party relationship, which is often an existing or necessary business, corporate, or institutional relationship. Because trust has already been established, organizations may not protect or scrutinize the network or data access granted. In the cyber domain, this can occur through multiple methods, including compromised IT, cloud services, users, and managed service providers. Foreign adversaries prefer the cyber domain, as this vector is relative low risk and high reward. By understanding these risks and the broader geopolitical

context and implications for their critical supply chains, organizations can work collaboratively with stakeholders to build a resilient ecosystem. (See Resources & Tools | CISA and Enduring Security Framework (ESF))^{9&10}

Specifically, Chinese cyber actors, including a group known as 'Volt Typhoon,' are burrowing deep into our critical infrastructure to be ready to launch destructive cyber-attacks in the event of a major crisis or conflict with the United States. This is a world where a major conflict halfway around the globe might well endanger the American people here at home through the disruption of our gas pipelines; the pollution of our water facilities; the severing of our telecommunications; the crippling of our transportation systems—all designed to incite chaos and panic across our country and deter our ability to marshal military might and citizen will.

-CISA Director Jen Easterly³

Foreign adversaries abuse trusted supply chain relationships to advance campaigns and achieve effects.



The cyber supply chain is most likely the initial threat vector, but other supply chain relationships can be abused in concert or separately.

INTEGRATED RISK MANAGEMENT: ADDRESSING DYNAMIC EXPOSURE TO RISK

The cyber domain is dynamic and can instantly change, creating risk for an organization. Accordingly, organizations should integrate cybersecurity supply chain risk management (C-SCRM) into enterprise risk management (ERM) program activities. ERM programs help organization leaders establish an acceptable risk level and set the security conditions needed to maintain this risk level. In addition, cyber supply chain ecosystems are complex, and the relationship interactions throughout the supply chain lifecycle are influenced by technologies, laws, policies, procedures, and practices. Managing this risk exposure

is a shared responsibility among different organization stakeholders. Understanding supply chain dependencies is vital to reducing the impact of supply chain attacks stemming from a trusted relationship. Such attacks shift, circumvent, or subvert an organization's risk tolerance. To address these threats, organizations must collaborate, communicate, and coordinate with stakeholders to reduce risk. While not exhaustive, the following categories of supply chain stakeholders should be reviewed to understand the dynamics affecting an organization's cyber supply chain.

THIRD PARTY RELATIONSHIPS

Well-defined and managed third-party relationships are essential to supply chain resilience. The harm or compromise from a third-party relationship with suppliers, their supply chains, and their supplied products or services regularly result in significant supply chain incidents. These incidents materialize when a threat actor successfully exploits a vulnerability tied to a system, product, service, or the supply chain ecosystem. Organizations should establish processes to identify, measure, monitor, and control the risk associated with third parties. As reliance on third parties increases, it's essential to establish a continuously monitored enterprise-wide program that:

1. verifies third parties who maintain an effective security culture and have their own SCRM program; and
2. establishes protocols to assess third parties.
(See NIST 800-161r1) ¹

INSIDER RISKS

Insider risks are also exploited when nation-state actors augment their cyber operations with non-traditional methods to advance their interests. Employees, contractors, sub-contractors, and vendors that have been granted access to facilities, systems, and networks may wittingly—or unwittingly—do harm to the organization's supply chain ecosystem. For example, trusted insiders may conspire to commit economic espionage to steal sensitive intellectual property. Efforts by threat actors to bypass multifactor authentication (MFA) are rising, including increases in social engineering attempts.

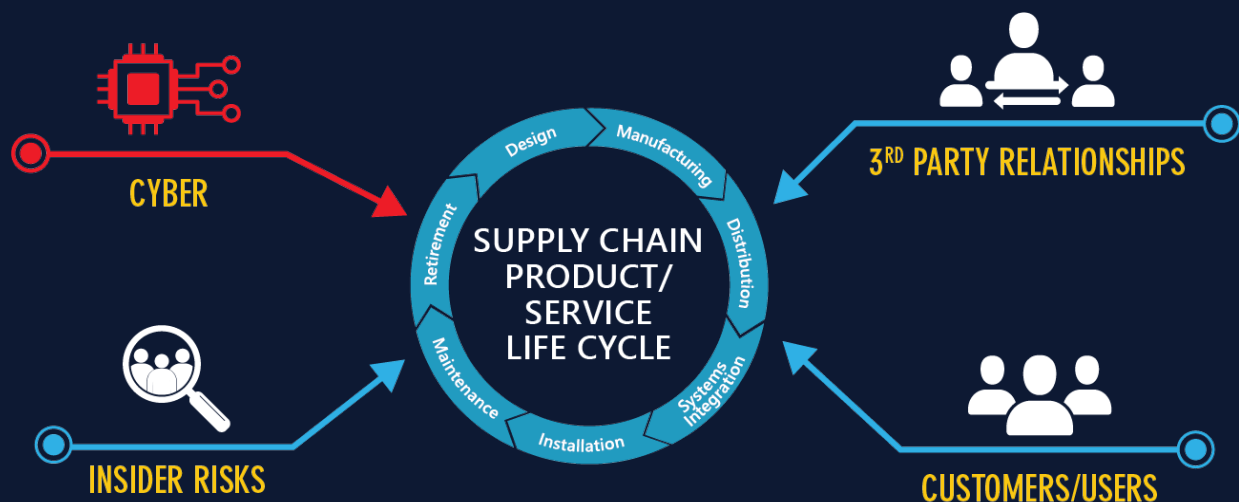
“Organizations can no longer protect themselves by simply securing their own infrastructures since their electronic perimeter is no longer meaningful; threat actors intentionally target the suppliers of more cyber-mature organizations to take advantage of the weakest link.”

— NIST IR 8276

Because authorized access is abused for an unauthorized purpose, these attacks are more difficult to detect and counter if a business is not prepared. (See CDSE Insider Threat toolkit) ⁶

CUSTOMERS AND USERS

For certain sectors, including telecommunications, energy, and finance, customers and users can be a vector for supply chain risks. In those sectors, customer-facing corporate assets can be exposed to heightened risk. For example, organizations may implement MFA for all users and for all services, including email, file sharing, and financial account access. MFA is an essential practice to reduce the threat of cyber threat actors using compromised credentials to conduct malicious activity on networks. However, not all forms of MFA are equally secure, resulting in the potential for compromise through phishing or push bombing attacks. Thus, organizations must understand that their customers' use of MFA may itself be used as a threat vector to access an organization's protected systems. (See CISA Alert on MFA) ¹¹ Organizations should take care to identify external user or customer connections that require access to critical internal processes. Identifying these interdependencies will address the risks from user vectors, reducing the risk of critical failures.





TAKEAWAY

Cyber supply chain challenges are intensifying with profound implications for security and resilience. Foreign adversaries, criminal organizations, and hacktivists are seeking information vital to our national security and economic competitiveness. Organizations must remain engaged to develop the capabilities to protect their ecosystems from multiple supply chain threats. Effective C-SCRM requires active collaboration, communication, and action with stakeholders to improve organizational supply chain security and resilience.

Enhancing supply chain cybersecurity is not the only method to build supply chain resilience. Organizations should use all available security disciplines (e.g., acquisition, personnel, logistics, facilities) to enhance their supply chain security and remove opportunities for exploitation. In addition, organizations should train their employees about the importance of cyber supply chain security and how their organizational role is part of the C-SCRM approach. Such training should address the processes and procedures for reporting cybersecurity incidents associated with all supply chain relationships. At a minimum, employees with supply chain responsibilities, including program officials, security officials (e.g., the

Chief Information Officer, the Chief Information Security Officer), and acquisition officials (e.g., contracting officers, contracting officer's representatives, project managers), should receive C-SCRM training as part of their performance measures (See NIST NICE Framework)⁵ By incorporating C-SCRM activities into existing enterprise risk management programs, organizations can take additional steps to address cyber supply chain risks.

These steps can include:

- Identify critical supply chain relationships—suppliers, vendors, industry relationships, service providers, customers, and employees.
- Understand the vulnerabilities that each relationship brings to the organization.
- Identify potential risks to these critical relationships—what consequences could occur if the trusted relationship is broken, unreliable, or exploited?
- Develop an integrated supply chain security strategy to mitigate the potential risks, address these consequences, and adjust the supply chain relationship accordingly.

“Businesses need to prepare for and expect an attack and test and prepare for and exercise their critical systems so that they can continue to operate through a disruption and recover rapidly to provide services to the American people.

“Every critical infrastructure entity should establish a relationship with their local CISA team and take advantage of our free services, including vulnerability scanning, to ensure they can identify and prevent the vulnerabilities that the Chinese cyber actors are using. Every critical infrastructure entity should use these services and CISA cybersecurity performance goals, as well as the advisories that we’ve published with NSA and FBI and international partners, to do the necessary investments in cyber hygiene to ensure that they can protect their networks, including throughout their supply chains.”

- CISA Director Jen Easterly



REPORTING AN INCIDENT

To report an intrusion and request resources for incident response or technical assistance, contact the FBI through a local field office, or the FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937)

REFERENCES

For additional information, please see the references, frameworks, and guidance below.

REFERENCES:

1. [Opening Statement by FBI Director Christopher Wray before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, January 31, 2024](#)
2. [ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System](#)
3. [Opening Statement by CISA Director Jen Easterly before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party, January 31, 2024](#)
4. [U.S. and International Cybersecurity Authorities Joint Cybersecurity Advisory \(CSA\) on Volt Typhoon](#)
5. [PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure](#)
6. [People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection](#)
7. [CISA Directs Federal Agencies to Immediately Mitigate Significant Risk from Russian State-Sponsored Cyber Threat](#)
8. [DoD Annual Report on Military and Security Developments Involving the PRC](#)
9. ["Foreign Country of Concern," as defined by Executive Order 14017](#)

FRAMEWORKS AND GUIDANCE:

1. [NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#)
2. [NIST CSF 2.0: Cybersecurity Supply Chain Risk Management \(C-SCRM\)](#)
3. [NISTIR 8179: Criticality Analysis Process Model](#)
4. [NIST SP 800-61R2: Computer Security Incident Handling Guide](#)
5. [NIST Special Publication 800-181, revision 1: Workforce Framework for Cybersecurity \(NICE Framework\)](#)
6. [Center for Development of Security Excellence: Insider Threat Toolkit](#)
7. [NISTIR 8276: Key Practices in C-SCRM: Observations from Industry](#)
8. [Navigating NIST's CSF 2.0 Quick Start Guides | NIST](#)
9. [National Security Agency Enduring Security Framework \(ESF\)](#)
10. [CISA Cybersecurity Resources & Tools | CISA](#)
11. [CISA Alert on Multifactor Authentication \(MFA\)](#)



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

For more information on supply chain security, please visit ncsc.gov