LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

APRIL 2023

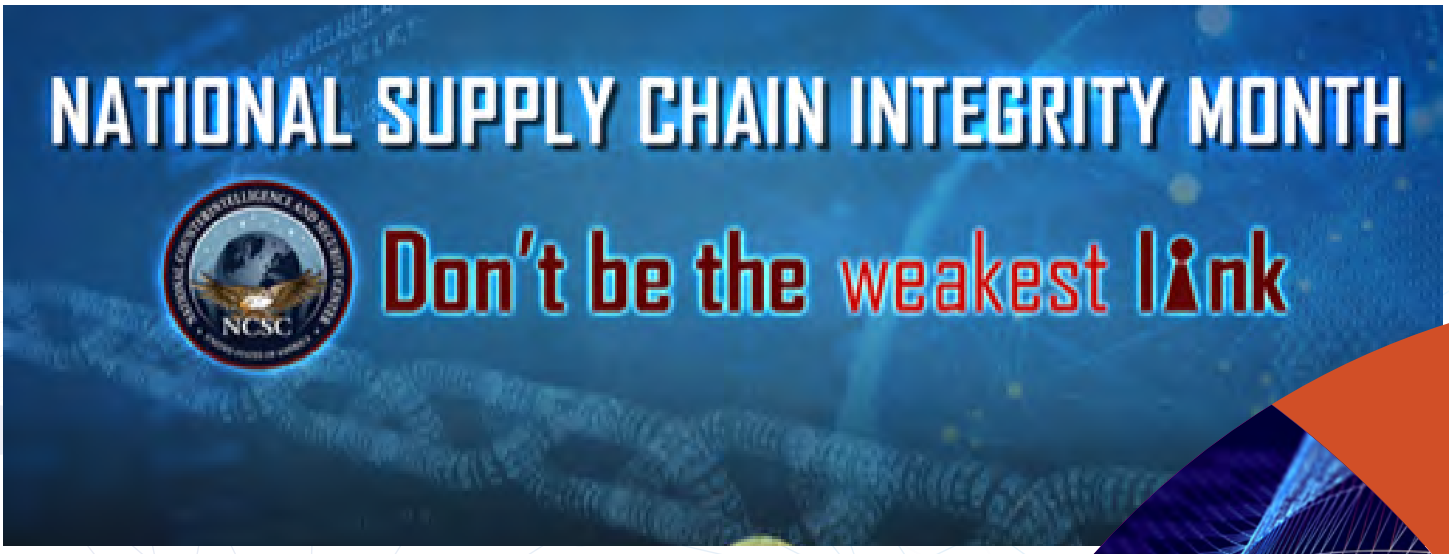
NATIONAL SUPPLY CHAIN INTEGRITY MONTH

The Defense Counterintelligence and Security Agency (DCSA) has designated April as National Supply Chain Integrity Month. Our complex network of global supply chains has become a cornerstone of our current way of life, with goods and resources constantly moving across land, sea, and air. We may take this system for granted but that doesn't change the reality; any disruption could have far-reaching consequences at home or abroad. From malicious cyber-attacks to EMPs and from space weather events to catastrophic derailments or aviation accidents, our system can be impacted from any number of malicious or unintentional actions.

According to The Office of the Director of National Intelligence, reducing the threats to key U.S. supply chains was one of the five pillars of the National Counter intelligence Strategy of the U.S. for 2020-2022.

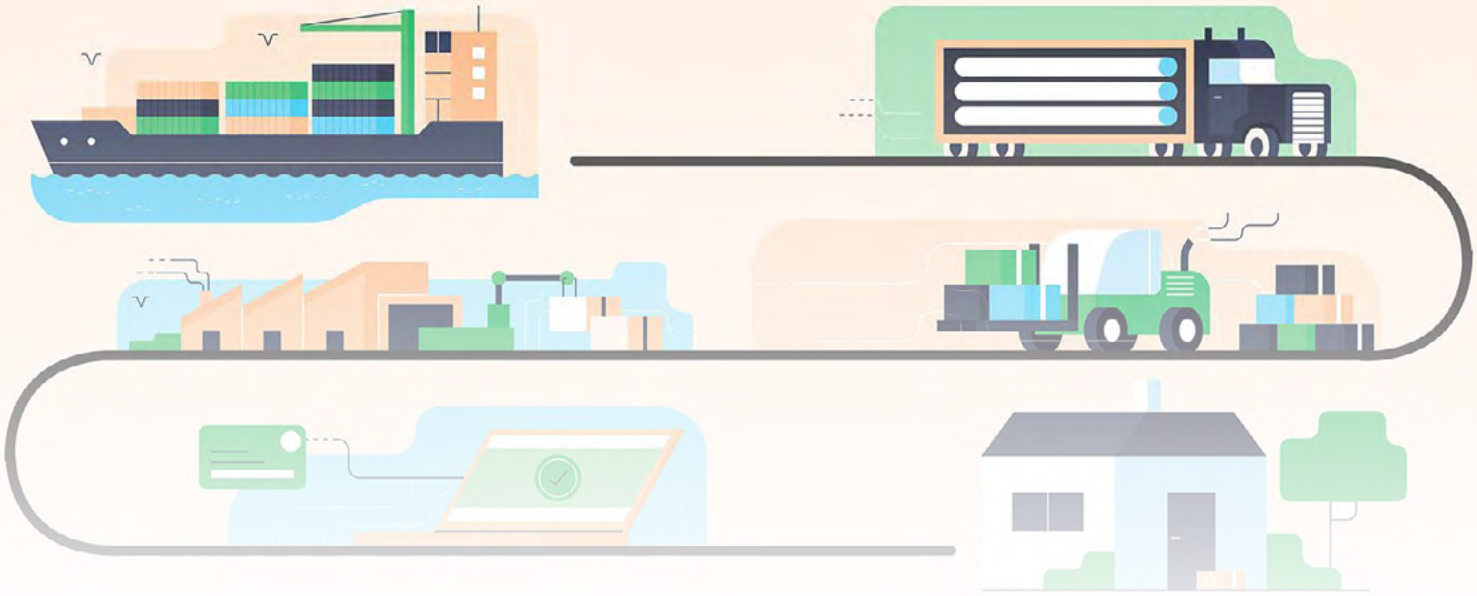
The strategic objective for supply chain security is to: "Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. Government, the Defense Industrial Base, and the private sector."

You can read more about how the government is working to meet this objective at: **https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf**



LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com



CYBERSECURITY AND THE SUPPLY CHAIN

We often think of supply chains as physical handoffs of goods from one place to another. There are countless cyber touchpoints along the chain that could cause the system to be disrupted or fail.

These digital connections include the analytics tools that manage where products are in the delivery process, authentication tools that confirm delivery to the correct people and places, and the signals that turn on and off systems like oil pipelines.

All of these connections are vulnerable to cybersecurity threats, including disruption of services, unauthorized access to data, and potential damage to physical assets. Unfortunately, these risks are especially severe during times like now when businesses have already had to cope with challenges from the COVID-19 pandemic.

The Cybersecurity and Infrastructure Security Agency (CISA) reminds us that safeguarding your business against supply chain threats means fully understanding the systems impacting your immediate needs as well as those of third-party vendors, service providers, and customers. Proactively assessing any potential risks in these extended supply chains can ultimately mean the difference between protecting or compromising valuable corporate knowledge.

CISA recommends these steps are in place to build an effective Supply Chain Risk Management (SCRM) system.

Identify the people: Build a team of representatives from various roles and functions of the company. Ensure personnel at all levels are well-trained in the security procedures of their role or function.

Manage the security and compliance: Document the set of policies and procedures that address security, integrity, resilience, and quality.

Assess the components: Build a list of ICT components (e.g., hardware, software, and services) that your organization procures to enable your business. Know which internal systems are relied upon for critical information or functions, and which systems have remote access capability that must be protected to prevent unauthorized access.

Know the supply chain and suppliers: Identify your suppliers and, when possible, the suppliers' sources.

Verify assurance of third-parties: Verify that your suppliers maintain an adequate security culture and SCRM program to appropriately address the risks that concern your organization.

Evaluate your SCRM program: Determine the frequency with which to review your SCRM program, incorporate feedback, and make changes to your risk management program. This may also include auditing suppliers against practices and protocols established by your organization.

To keep supply chains functioning optimally, cybersecurity is necessary to protect them from physical and digital threats.

Read the full list of CISA'S SCRUM recommendations here: **https://www.cisa.gov/ict-supply-chain-program-basics**

IT SUPPLY CHAIN RISKS

Anyone who uses a computer may not think that supply chain risks would affect them or require them to modify their normal computer use and online behavior. Here are two examples that highlight that there are indeed risks users may face:

Example #1: Malicious Links

At times users will receive emails or Web Browser pop-ups telling them they need to install updates, or they "have been infected with a virus" and "click here to install or run" that are NOT legitimate. Users need to be aware of this and use great care when running updates or malware scans/removal tools. They should NEVER run these when received in an email or Browser pop-up. They should use the built-in Microsoft, Dell, HP, etc. tools in MS Windows and/or the Anti-Malware tools they purchased/installed on their computer.

Clicking on malicious links can allow hackers to access your corporate and personal information.

Example #2:

Users should also be slow to use and (if possible) often should uninstall many "add-on" apps provided by their computer manufacturer. This example comes courtesy of the National Counterintelligence and Security Center:

"In 2014 Lenovo, one of the world's largest personal computer retailers began pre-installing Superfish software into its products. Superfish allowed consumers to 'shop for deals' on the web. However, it also allowed attackers access to a person's internet traffic and browser history by intentionally 'poking a hole' into the browser security, allowing anyone on the Wi-Fi network to easily hijack the computer browser. Robert Graham, a cybersecurity expert from Errata Security, tested the Superfish vulnerability, and found it incredibly easy to attack. He was able to intercept the encrypted Superfish communications all while 'hanging out near them at a café Wi-Fi hotspot' without the victims aware the attack was taking place. In February 2015, the Department of Homeland Security (DHS) urged Lenovo consumers to uninstall Superfish and the connected Superfish certificates because the computers were 'vulnerable to serious cyberattacks, including interception of passwords and sensitive data being transmitted through browsers'."

These types of risks are often something that end-users have no control over, but everyone should be cautious and where possible and avoid or delete "helpful" apps.

At LIS, our IT team handles all anti-malware, Windows, and other patch installations on the company supplied laptops. End users should not need to perform any themselves. If prompted to install patches or remove viruses, users should contact LIS IT Support. For personal computers, they should follow the recommendations above to be as careful as possible.

The Superfish example is courtesy of The Office of The Director of National Intelligence (pages 6 & 7):
https://www.dni.gov/files/NCSC/documents/supplychain/ict-supply-chain-risk-2022-5BE169B1-.pdf