Cyber-Supply Chain Risk Management

July 21st, 2022
Mark Keelan - Director Compliance Practice
Agenda

- ISACA House Keeping
- Cyber Supply Chain Risk Management
  - Supply Chain State
  - NISTIR 8276
  - Government Response
  - Examples – Cyber Supply Chain Incident
  - Best Practices
  - Live Example

- Questions and Wrap Up
ISACA House Keeping

- Meeting is being recorded and will be shared on ISACA website
- CPE Certificate of Attendance
  - On-premises attendees: please make sure we checked you with the Eventbrite app
  - Online attendees: please make sure to complete the registration form we will share in the chat about half-way through the meeting, or you can self-submit your CPE (i.e. take screenshots to submit as proof of attendance)
- August Meeting: Andy Kim
  - Understanding CMMC 2.0
- Job Opportunities updated on the website
- Any community events, news, employment opportunities, etc. others would like to share in Chime or in-person

- If you have any questions and/or would like additional information, please email the chapter at isacasandiego@gmail.com or visit us online at https://isaca-sd.org
The World's Supply Chain is at RISK

Data Processing is one of the Top Risks!

A PERFECT STORM

1. Globalization
2. Economic Growth
3. Outsourcing

These trends have resulted in a world where organizations no longer fully control—and often do NOT HAVE FULL VISIBILITY into—the supply ecosystems of the products that they produce or the services that they deliver. And without sufficient control, organizations struggle to manage risks stemming from their supply chains and the products and services traversing them.

Source - NISTIR 8276
https://csrc.nist.gov/publications/detail/nistir/8276/final
Feb. 2021
COVID-19 and shattered supply chains

Download the report ➔ Get free insights via email ➔
Record Number of Ships off CA Coast

Why a record number of container ships are backed up off the coast of California

With a dearth of places to anchor, some of the giant vessels are just drifting.

BY STACIE BROWN DEAN SEP 12, 2021 5:00 PM PDT

2021 Container Rates Surge 333% From One Year Ago

Bloomberg
Total Views: 520K
July 15, 2021
Shipping Rates are off the Charts!

Container shipping rates between U.S. and China exceed $20,000, hitting a record

PUBLISHED THU, AUG 5 2021 8:34 AM EDT | UPDATED THU, AUG 5 2021 8:35 AM EDT

KEY POINTS
- Container shipping rates from China to the United States have scaled fresh highs above $20,000 per 40-foot box.
China – US Transit Times Coming Down
China – US Rates Coming Down

Asia – N. America West Coast rates fell more than 30% in May to $10,762/FEU and East Coast prices fell 20% to $13,796/FEU.

Both remain more than 35% higher than a year ago, but have returned to levels not seen since last summer.

Likewise, conditions at LA/Long Beach ports have improved over the last two months.
Supply Chain Improving

The supply chain crisis is getting better — and it could make a lot of things cheaper soon

Juliana Kaplan and Madison Hoff  Jul 11, 2022, 11:48 AM

Back in October, it took more than 110 days for goods to make their way from Asia to the U.S. That has now fallen to 95 days. While 15 days may not seem that dramatic, it's a rate not seen since mid-2021.

How Big is the Problem?

Transportation & Logistics › Water Transport

Container shipping - statistics & facts

Published by Martin Placek, Sep 23, 2021

Maritime shipping is the backbone of world trade; it is estimated that some 80 percent of all goods are carried by sea. In terms of value, global maritime container trade is estimated to account for around 60 percent of all seaborne trade, which was valued at around 14 trillion U.S. dollars in 2019. While the number of goods carried by containers increased from around 102 million metric tons in 1980 to about 1.83 billion metric tons in 2017, vessels have likewise increased their capacity. Between 1980 and 2020, the deadweight tonnage of container ships has grown from about 11 million metric tons to around 275 million metric tons. With a total capacity of over four million TEUs*, Danish shipping line APM-Maersk is currently the largest container-shipping company globally, followed by MSC, COSCO, CMA CGM, and Hapag-Lloyd.
Russia, DHS said, has a "range of offensive cyber tools that it could employ against US networks," and the attacks could range from a low level denial of service attack, to "destructive" attacks targeting critical infrastructure.

DHS says Russia "continues to target" and gain access to critical infrastructure in the United States, but Russia does not limit itself to conducting cyber operations just in the U.S.
The Colonial Pipeline Hack Is a New Extreme for Ransomware

An attack has crippled the company’s operations—and cut off a large portion of the East Coast’s fuel supply—in an ominous development for critical infrastructure.

Other Large Public Examples:

JBS USA paid an $11 million ransom in response to a cyberattack that led to the shutdown of its entire US beef processing operation.

NotPetya:
World’s First $10 Billion Malware in 2017

Target Retailer
Attack came from HVAC provider 2014
The intersection of cyberattacks and supply chains creates a wicked new form of risk—and the stakes are as much about national security as they are economics.
Biden Administration Executive Order

Executive Order on America’s Supply Chains

FEBRUARY 24, 2021 • PRESIDENTIAL ACTIONS
Key Practices in Cyber Supply Chain Risk Management:
Observations from Industry

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

https://csrc.nist.gov/publications/detail/nistir/8276/final
Feb. 2021
Key Practices for C-SCRM

• 1. Integrate C-SCRM Across the Organization
• 2. Establish a Formal C-SCRM Program
• 3. Know and Manage Critical Suppliers
• 4. Understand the Organization’s Supply Chain
• 5. Closely Collaborate with Key Suppliers
• 6. Include Key Suppliers in Resilience and Improvement Activities
• 7. Assess and Monitor Throughout the Supplier Relationship
• 8. Plan for the Full Life Cycle
### Appendix C—Recommendations Mapped to Key Government and Industry Resources

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, ERM, business units, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Integrate cybersecurity considerations into system and product life cycles</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clearly define roles and responsibilities for security aspects of specific</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
2 Key Requirements for Simplifying Cyber Supply Chain Risk Management

• **MEASURABLE & ACTIONABLE**
• Designed for Ease of Use
• Deployable
  • Anywhere
  • Anyone
• Uses Industry Standards Only
  • NIST Cybersecurity Framework
  • CMMI
CMMC – 3rd Party Cyber Risk Assessment
Capability Maturity Model - “Quantitative”

**Maturity Level 5**
- **Optimizing**
  - **Stable and flexible.** Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.

**Maturity Level 4**
- **Quantitatively Managed**
  - **Measured and controlled.** Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.

**Maturity Level 3**
- **Defined**
  - **Proactive, rather than reactive.** Organization-wide standards provide guidance across projects, programs, and portfolios.

**Maturity Level 2**
- **Managed**
  - **Managed on the project level.** Projects are planned, performed, measured, and controlled.

**Maturity Level 1**
- **Initial**
  - **Unpredictable and reactive.** Work gets completed but is often delayed and over budget.
CMMC – 3rd Party Cyber Risk Assessment

# NIST Cybersecurity Framework – “Qualitative”

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| ID.AM-1: Physical devices and systems within the organization are inventoried | ID.AM: Asset Management | - CIS CSC 1  
- COBIT 5 BA109.01, BA109.02  
- ISA 62443-2-1:2009 4.2.3.4  
- ISA 62443-3:2013 SR 7.8  
- ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
- NIST SP 800-53 Rev. 4 CM-8, PM-5 |
| ID.AM-2: Software platforms and applications within the organization are inventoried | - CIS CSC 2  
- COBIT 5 BA109.01, BA109.02, BA109.05  
- ISA 62443-2-1:2009 4.2.3.4  
- ISA 62443-3:2013 SR 7.8  
- NIST SP 800-53 Rev. 4 CM-8, PM-5 |
| ID.AM-3: Organizational communication and data flows are mapped | - CIS CSC 12  
- COBIT 5 DSS05.02  
- ISA 62443-2-1:2009 4.2.3.4  
- ISO/IEC 27001:2013 A.13.2.1, A.13.2.2  
- NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 |
| ID.AM-4: External information systems are catalogued | - CIS CSC 12  
- COBIT 5 APO02.02, APO10.04, DSS01.02  
- ISO/IEC 27001:2013 A.11.2.6  
- NIST SP 800-53 Rev. 4 AC-20, SA-9 |

**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.
NIST CSF Framework

- Qualitative – NIST CSF
- Risk Focused
- Described in words
- Results
  - Narrative
  - Relative

CMMI

- Quantitative - CMMI
- Value Focused
- Described in numbers
- Results
  - Numeric Score
  - Normalized
Clean & Straight Forward Cybersecurity Assessment

### NIST Cybersecurity

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

**Instructions** Feedback

Progress on Assessment-2021-Oct-29 @ 15:48

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management 1 of 130</td>
<td>Identity Management, Authentication and Access Control 0 of 393</td>
<td>Anomalies and Events 0 of 171</td>
<td>Response Planning 0 of 44</td>
<td>Recovery Planning 0 of 13</td>
</tr>
<tr>
<td>Business Environment 0 of 149</td>
<td>Awareness and Training 0 of 93</td>
<td>Security Continuous Monitoring 0 of 201</td>
<td>Communications 0 of 108</td>
<td>Improvements 0 of 16</td>
</tr>
<tr>
<td>Governance 0 of 97</td>
<td>Data Security 0 of 256</td>
<td>Detection Processes 0 of 174</td>
<td>Analysis 0 of 103</td>
<td>Communications 0 of 174</td>
</tr>
<tr>
<td>Risk Assessment 0 of 186</td>
<td>Information Protection Processes and Procedures 0 of 392</td>
<td>Maintenance 0 of 32</td>
<td>Mitigation 0 of 84</td>
<td></td>
</tr>
<tr>
<td>Risk Management Strategy 0 of 151</td>
<td>Protective Technology 0 of 163</td>
<td>Improvements 0 of 38</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Supply Chain Risk Management 0 of 137

<table>
<thead>
<tr>
<th>Identify</th>
<th>Asset Management</th>
<th>Physical devices and systems within the organization are inventoried</th>
<th>Question # 2</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Initial</td>
<td></td>
<td>Are inventories manual (e.g., spreadsheets)?</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

| | In Progress | No |
Assessment: Measurement & Reporting

Interactive reports are available
CMMI Not Limited to NIST C-SCRM Assessments

- NIST Privacy Framework v1.0
- NIST CSF v1.1
- NIST 800-53
- ISO 27701
- ISO 27001 v2013
- US HIPAA
- EMEA EU GDPR
- PCI DSS v3.2
- SOC 2

Guided on-line maturity assessments make it easy to survey your organization

Quantitative measurement of privacy value supports ROI for Investment in Privacy
Privacy and Cybersecurity Assessments

Welcome to the future of privacy and cybersecurity assessments. While individual certifications are important, the world of privacy and cybersecurity lacked a qualitative and quantitative “industry standardized organizational assessment.” Not anymore! This solution combines the best of the best to provide qualitative and quantitative privacy maturity assessments using the NIST Privacy or Cyber Security Framework with the Capability Maturity Model Integration (CMMI).

New NIST Privacy Assessment

The NIST Privacy Framework is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals’ privacy.

New NIST Cybersecurity Assessment

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

New PIPEDA v2019.6 Assessment

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law for private sector organizations in Canada. The purpose of the law is to govern the collection, use, and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

New ISO27001 Assessment

MOST COST-EFFICIENT PATH TO MINIMIZE CYBER RISK ACROSS YOUR SUPPLY CHAIN
Supplier Community Portal

MAKES IT EASY TO ASSESS YOUR SUPPLY CHAIN RISK ACROSS COMPLEX GLOBAL SUPPLY CHAINS

• Dedicated Supplier Community Cloud Environment
  • Client Branded
  • Multi-Brand / Multi-Region
  • Single Tenant
  • Customizable
  • Upgradable

• Automated Supplier On Boarding
  • Supplier receives e-mail with link to join community
  • Multi-brand e-mail templates
  • Self-registers on the portal
  • Establishes Secure Channel of Communication with the Supplier

• Supplier Risk Assessment Portal
  • Allows user to easily complete cybersecurity assessments
  • Supports multi-users per Supplier to answer 1 assessment
  • Supports synch of common answers across multiple frameworks
Supplier Community Management

GET YOUR SUPPLIERS TO PAY FOR COST OF COMPLIANCE

Supplier On-Boarding

Compliance Campaign Events

Supplier Funded Compliance
Creative Program Funding

Let Your Suppliers Pay For Compliance?

• Customer Funded Model
• Supplier Funded Model
  • Have your supplier network fund your assessment program
  • Have suppliers sign up for the network
Objectives & Outcomes

LIFECYCLE OF CONTINUOUS IMPROVEMENT

OBJECTIVES

OUTCOMES
Why Does this Matter?

• Shutdown your company
  • Indirectly – by disrupting your supply chain
  • Directly – using your supply chain as an attack vector

• You need to Report Readiness
  • Executive Management – Business Risk
  • 10K – Shareholders if you are public

• Lost Growth and Customers

• National Security
  • Scary Scenarios
    • Loss of Food on Shelves
    • Disable water and power
    • No Gas for your car
    • Cripple National Defense
NIST Cybersecurity Supplier Chain Risk Assessment
Contacts at UST

Mark Keelan
mark.keelan@ust.com
Director – Compliance Practice

Austin Gould
austin.gould@ust.com
Marketing
-Question-
Copyright and confidentiality notice

Copyright © 2021 by UST Global Inc. All rights reserved.

This document is protected under the copyright laws of United States, India, and other countries as an unpublished work and contains information that shall not be reproduced, published, used in the preparation of derivative works, and/or distributed, in whole or in part, by the recipient for any purpose other than to evaluate this document. Further, all information contained herein is proprietary and confidential to UST Global Inc and may not be disclosed to any third party. Exceptions to this notice are permitted only with the express, written permission of UST Global Inc.

UST® is a registered service mark of UST Global Inc.