Resources to Help SMEs Manage Cybersecurity Risks When Doing Business in the Transatlantic Marketplace

June 26, 2024

This webinar is being recorded
• Opening Remarks
• About NIST
• NIST International Engagement
• NIST Small Business Cybersecurity Resources
  • Small Business Cybersecurity Corner
  • CSF 2.0 Small business Quick Start Guide
  • Supply Chain Risk Management Quick Start Guide
• Overview of NIST Manufacturing Extension Partnership (MEP) ExporTech Program
• Audience Q&A
Opening Remarks

David De Falco
Deputy Assistant Secretary for Europe and Eurasia. Global Markets, International Trade Administration, United States Department of Commerce

This webinar supports the efforts of the U.S.-EU Trade and Technology Council (TTC) Working Group 9 to improve SME access to and use of digital tools. For more information about the TTC, please visit: https://www.trade.gov/useuttc
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life
The Applied Cybersecurity Division implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities.

https://www.nist.gov/itl/applied-cybersecurity
NIST International Engagement on Cybersecurity and Privacy Standards
The cross-border nature of our economies makes it critical that NIST considers the global context when it conducts research, determines priorities, and conceptualizes approaches.

As a result of widespread international use, there are now multiple translations and adaptations of NIST cybersecurity and privacy resources.

NIST encourages international participation at all stages in the development and evolution of its cybersecurity and privacy programs and resources.

Learn About Our Global Impact: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources
The CSF and other NIST cybersecurity and privacy resources have benefitted from international expertise and are rooted in international standards.

The CSF is currently used by government and industry in several countries and regions. Version 1.1 is translated into thirteen languages and Version 2.0 is currently translated into two languages.

International engagement remains a focus for CSF 2.0.

Work with interagency partners, including the State Department and International Trade Administration (ITA), to share information on NIST cybersecurity and privacy resources to international government partners.

Work closely with industry on international engagements, including meetings, webinars, and side events during large international conferences.

Translations and adaptations of NIST resources are highlighted on the NIST International Cybersecurity and Privacy Resource Site: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources
Standards Activities in ISO

• NIST has contributed to the following documents in ISO that leverage the CSF:
  ➢ ISO Technical Specification 27110, “Cybersecurity Framework Guidelines,” which specifies guidance for developing a cybersecurity framework that aligns with the functions of the CSF
  ➢ ISO Technical Reference 27103, “Cybersecurity and ISO and IEC Standards,” which provides guidance on how to leverage existing ISO standards in a cybersecurity framework and maps to the CSF

• NIST is currently contributing as an editor on ISO 27028, a proposed international standard for guidance for attributes for the recently revised ISO 27002 standard

Learn About Our Global Impact: https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources
NIST Small Business Cybersecurity Resources

www.nist.gov/itl/smallbusinesscyber
NIST Small Business Cybersecurity Resources

SMALL BUSINESS CYBERSECURITY CORNER

Cybersecurity Basics
NIST Cybersecurity Framework
Events
Guidance by Sector
Guidance by Topic
Training
Videos
Get Engaged
Cybersecurity @ NIST

CONNECT WITH US

www.nist.gov/itl/smallbusinesscyber
Guidance by Topic

SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics
- NIST Cybersecurity Framework
- Events
- Guidance by Sector
- Guidance by Topic
- Training
- Videos
- Get Engaged
- Cybersecurity @ NIST

CONNECT WITH US

SPOTLIGHT

- Videos
- Cybersecurity Framework
- Case Studies

- All-Purpose Guides
- Phishing
- Choosing A Service Provider
- Privacy
- Cloud Security
- Protecting Against Scams
- Cybersecurity Insurance
- Ransomware
- Government Contractor Requirements
- Responding to a Cyber Incident
- Developing Secure Products
- Securing Data and Devices
- Employee Awareness
- Securing Network Connections
- Multi-Factor Authentication
- Telework

www.nist.gov/itl/smallbusinesscyber
NIST Cybersecurity Framework

Voluntary guidance that helps organizations—regardless of size, sector, or maturity—better understand, assess, prioritize, and communicate their cybersecurity efforts.

*not a one-size-fits-all approach to managing cybersecurity risks.

CSF Core

The nucleus of the CSF. A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks.

Functions>Categories>Subcategories

CSF Organizational Profiles

A mechanism for describing an organization’s current and/or target cybersecurity posture in terms of the CSF Core’s outcomes.

CSF Tiers

Characterize the rigor of an organization’s cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

https://www.nist.gov/cyberframework
NIST CSF 2.0 Small Business Quick Start Guide as an On-Ramp to the CSF 2.0 Journey

View full CSF 2.0 SMB QSG: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
Together, these 6 Functions provide a comprehensive view for managing cybersecurity risk.

https://www.nist.gov/cyberframework
The Govern Function helps you establish and monitor your business’s cybersecurity risk management strategy, expectations, and policy.

**Actions to Consider**

**Understand**
- Understand how cybersecurity risks can disrupt achievement of your business’s mission. (GV.OC-01)
- Understand your legal, regulatory, and contractual cybersecurity requirements. (GV.OC-03)
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. (GV.RR-02)

**Assess**
- Assess the potential impact of a total or partial loss of critical business assets and operations. (GV.OC-04)
- Assess whether cybersecurity insurance is appropriate for your business. (GV.RM-04)
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. (GV.SC-06)

**Prioritize**
- Prioritize managing cybersecurity risks alongside other business risks. (GV.RM-03)

**Communicate**
- Communicate leadership’s support of a risk-aware, ethical, and continually improving culture. (GV.RR-01)
- Communicate, enforce, and maintain policies for managing cybersecurity risks. (GV.PO-01)

**Getting Started with Cybersecurity Governance**

You can use these tables to begin thinking about your cybersecurity governance strategy.

### Setting Organizational Context

**Our business mission statement:**

<table>
<thead>
<tr>
<th>Documenting Cybersecurity Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>List your legal requirements:</td>
</tr>
<tr>
<td>List your regulatory requirements:</td>
</tr>
<tr>
<td>List your contractual requirements:</td>
</tr>
</tbody>
</table>

### Technical Deep Dive: Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

**Questions to Consider**

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

### Related Resources

- Securing Small and Medium-Sized Supply Chains Resource Handbook
- Choosing A Vendor/Service Provider

View all NIST CSF 2.0 Resources Here
A Few Notes on the Govern Function

- The Big Picture

- Provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions.

- Encompasses how organizations make and carry out informed decisions on cybersecurity strategy.

- Emphasizes that cybersecurity is a major source of enterprise risk that business leaders should consider alongside other business risks.

- Emphasis on supply chain risk management.
CSF 2.0 Cybersecurity Supply Chain risk Management (C-SCRM) Quick Start Guide
CSF 2.0 C-SCRM Quick Start Guide
https://www.nist.gov/quick-start-guides

NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)
A QUICK START GUIDE

HOW TO USE THE CSF TO ESTABLISH AND OPERATE A C-SCRM CAPABILITY

Establishing a C-SCRM Capability
The CSF has a Category within its Govern Function dedicated to C-SCRM: the Cybersecurity Supply Chain Risk Management (GV.SC) Category. GV.SC contains the key outcomes that every organization should achieve through its C-SCRM capability. Additionally, many of the subcategories within the remainder of the CSF can be used to identify and communicate C-SCRM-related requirements internally for organizations and for their vendors.

Perform these activities to establish your organization’s C-SCRM capability:
Activity 1: Create a C-SCRM strategy, objectives, policies, and processes. [GV.SC-01]
Activity 2: Identify your organization’s technology suppliers and determine how critical each one is to your organization. [GV.SC-04]
Activity 3: Establish C-SCRM roles and requirements and communicate them within and outside your organization. This includes identifying C-SCRM roles and responsibilities [GV.SC-02] and C-SCRM requirements [GV.SC-05].

It is also important to coordinate and harmonize activities between your C-SCRM capability and other internal capabilities. Here are a few examples:

- Integrate C-SCRM into cybersecurity and enterprise risk management, risk assessment, and improvement processes, and monitor the performance of C-SCRM practices throughout the technology lifecycle. [GV.SC-03, GV.SC-09] See the Enterprise Risk Management Quick-Start Guide for more information on C-SCRM integration.
- Include your relevant suppliers in cybersecurity incident planning, response, and recovery activities. [GV.SC-08] See NIST’s Computer Security Incident Handling Guide for more information on key practices for cybersecurity incidents.

Checklist of actions for Activity 1: Create a C-SCRM strategy, objectives, policies, and processes.
- Establish a C-SCRM strategy that lays out the objectives of the capability.
- Develop a C-SCRM plan (with milestones) and C-SCRM policies and procedures that guide implementation and improvement of the plan and the capability; socialize those policies and procedures with organizational stakeholders.
- Develop and implement C-SCRM processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders.
- Establish a cross-organizational mechanism that ensures alignment between functions that contribute to C-SCRM management, such as cybersecurity, IT, legal, human resources, engineering, etc.

Checklist of actions for Activity 2: Identify your organization’s technology suppliers and determine how critical each one is to your organization.
- Develop criteria for supplier criticality based on, for example, the importance of the supplier’s products or services to the organization’s business, sensitivity of data processed or stored by the supplier, and degree of access to the organization’s systems.
- Prioritize suppliers into criticality levels based on the criteria. See NIST IR 8179, Criticality Analysis Process Model: Prioritizing Systems and Components for more information on a structured method for prioritization.
- Keep a record of all suppliers, prioritized based on the criticality criteria.
New to C-SCRM?

Here are some NIST resources that can help you get up to speed on the basics of C-SCRM and support you in establishing and operating your C-SCRM capability:

• **CSF 2.0 C-SCRM Quick Start Guide**
  [https://www.nist.gov/quick-start-guides](https://www.nist.gov/quick-start-guides)

• **Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (NIST IR 8276)**

• **Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Revision 1)**
  [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf)

• **The Software and Supply Chain Assurance Forum**

• **NIST’s C-SCRM Program**
Additional CSF 2.0 Resources

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework
<table>
<thead>
<tr>
<th>GOVERN (G)</th>
<th>Category</th>
<th>Subcategory</th>
<th>Implementation Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (I)</td>
<td>Function</td>
<td>Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) 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.</td>
<td></td>
</tr>
</tbody>
</table>
|           |          | Asset Management (ID.AM): Inventories of hardware managed by the organization are maintained | Ext: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices  
Ex:2 Constantly monitor networks to detect new hardware and automatically update inventories |
|           |          | Asset Management (ID.AM): Inventories of software, services, and systems managed by the organization are maintained | Ext: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source custom applications, API services, and cloud-based applications and services  
Ex:2 Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes  
Ex:3 Maintain an inventory of the organization’s systems |
|           |          | Asset Management (ID.AM): Representations of the organization’s authorized network communication and internal and external network data flows are maintained | Ext: Maintain baselines of communication and data flows within the organization’s wired and wireless networks  
Ex:2 Maintain baselines of communication and data flows between the organization and third parties  
Ex:3 Maintain baselines of communication and data flows for the organization’s Infrastructure-as-a-Service (IaaS) usage  
Ex:4 Maintain documentation of expected network ports, protocols, and services |
|           |          | Asset Management (ID.AM): Inventories of services provided by suppliers are maintained | Ext: Inventory all external services used by the organization, including third-party Infrastructure-as-a-Service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings: APIs; and other externally hosted services |
ExporTech – Accelerating sales growth in global markets for small and medium-sized manufacturers

https://www.nist.gov/mep/mep-national-network
A unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

Our mission is to strengthen and empower U.S. manufacturers.
MEP National Network

Centers located in all 50 states and Puerto Rico.

Public-private partnership with local flexibility.

Federal funds, state investments, and private sector fees cover services.

Market driven program that creates high value for manufacturers.

Leverage partners to maximize service offerings.

Transfer technology and expertise to manufacturers.
Business Solution Examples
ExporTech is a structured process that helps exporters expand sales in global markets

| PLAN                  | Develop strategic export growth plan through workshops, planning tools, and individual coaching  
                          | Receive plan feedback from experienced international business leaders |
|-----------------------|--------------------------------------------------------------------------------------------------|
| EDUCATE               | Learn from wide range of experts – with opportunity for individualized consultation              |
| CONNECT               | Companies meet experts that become part of their network                                          
                          | Learn about programs, services, and grants that many exporters are unaware of                      
                          | Learn from peer companies – and hold each other accountable                                        |
| IMPLEMENT             | Execute plan, and connect to resources that can help you go-to-market (e.g. partner search and matchmaking, STEP grants, tradeshows) 
                          | Achieve higher ROI on business development – guided by plan                                         |
ExporTech Program Partners

**Exporters**

**Local Partners** (differ by region)
- District Export Councils
- State trade offices/organizations
- FedEx
- Universities, colleges
- SBDCs, SBA offices
- World Trade Centers
- Private consultants
- State and federal department of agriculture
- Other economic development organizations
- City governments

**MEP National Network**
- Delivery
- Selling, marketing
- Program management

**U.S. Commercial Service**
- Delivery
- Selling, marketing
- Program management
Principles/Philosophy of ExporTech

• Aimed at leadership
• Each company develops strategic international growth plan, receives feedback for go-to-market strategy
• Customized to participants
• Highly interactive – breakouts, one-on-ones, speed dating
ExporTech Unique Elements

- Development of export plan with feedback in final session
- Breakout groups working on elevator pitch
- Coaching in between sessions
- Connection to export ecosystem – expand network
- Significant involvement of experienced exporting company executives (plan feedback, panel discussions, breakout consultations)
ExporTech National Program History and Impacts

Program Summary (6/20/24)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># Programs Completed</td>
<td>275</td>
</tr>
<tr>
<td>(since inception in 2007)</td>
<td></td>
</tr>
<tr>
<td># States</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>(and PR)</td>
</tr>
<tr>
<td># Participating Companies</td>
<td>1,380</td>
</tr>
</tbody>
</table>

Client Impact

- Average sales increase/retention of $469,000
- Average cost savings of $93,000
- Average 6 new jobs per company
- Total program impact to date: >$600 million sales increase/retention
Success Story

Hydronalix Grows Export Markets Fivefold in Five Years

• Manufactures robotic water rescue systems and small unmanned watercraft in Green Valley, Arizona.

• First responders and military use: water rescue, bridge inspection, scientific research and law enforcement on oceans, lakes, and rivers.

• *The Challenge:* selling into export markets but no defined strategy/process.

• ExporTech partners helped company develop an export plan - how to structure and negotiate payment terms to ensure up-front payment.

• Executed export plan through international trade shows and trade mission initiatives led by the AZSTEP program - met with potential sales channel partners, end-users and buyers.

“I think the success of the program is because it’s been repeatable and sustainable. It takes a lot of continuous effort to grow our global customer base. In our case, ExporTech provided that critical push. In 2016, before we started ExporTech, I think we were selling in 11 or 12 countries. Now we have distributors in 33 countries, and we sell our products in 50 countries. The program has had a big impact on our business.”

Hydronalix CEO
Connect with Us

Visit Our Blog
www.nist.gov/blogs/manufacturing-innovation-blog

Visit Our Website
www.nist.gov/mep
www.nist.gov/exportech

Contact Us:
Brian.Lagas@nist.gov
301-975-5043
<table>
<thead>
<tr>
<th>Quick Links</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSF 2.0 Website: <a href="https://www.nist.gov/cyberframework">https://www.nist.gov/cyberframework</a></td>
<td><a href="mailto:cyberframework@nist.gov">cyberframework@nist.gov</a></td>
</tr>
<tr>
<td>CSF 2.0 FAQs: <a href="https://www.nist.gov/faqs">https://www.nist.gov/faqs</a></td>
<td></td>
</tr>
<tr>
<td>CSF 2.0 Small Business Quick Start Guide:</td>
<td><a href="mailto:smallbizsecurity@nist.gov">smallbizsecurity@nist.gov</a></td>
</tr>
<tr>
<td>NIST Small Business Cybersecurity Corner:</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.nist.gov/itl/smallbusinesscyber">https://www.nist.gov/itl/smallbusinesscyber</a></td>
<td></td>
</tr>
<tr>
<td>CSF 2.0 C-SCRM Quick Start Guide: <a href="https://nvlpubs.nist.gov/nistpubs/">https://nvlpubs.nist.gov/nistpubs/</a></td>
<td><a href="mailto:scrm-nist@nist.gov">scrm-nist@nist.gov</a></td>
</tr>
<tr>
<td>SpecialPublications/NIST.SP.1305.ipd.pdf</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity and Privacy Reference Tool (CPRT):</td>
<td><a href="mailto:cprt@nist.gov">cprt@nist.gov</a></td>
</tr>
<tr>
<td><a href="https://csrc.nist.gov/Projects/cprt">https://csrc.nist.gov/Projects/cprt</a></td>
<td></td>
</tr>
<tr>
<td>NIST International Cybersecurity and Privacy Resources:</td>
<td><a href="mailto:intl-cyber-privacy@nist.gov">intl-cyber-privacy@nist.gov</a></td>
</tr>
<tr>
<td><a href="https://www.nist.gov/cybersecurity/international-cybersecurity-and-">https://www.nist.gov/cybersecurity/international-cybersecurity-and-</a></td>
<td></td>
</tr>
<tr>
<td>privacy-resources</td>
<td></td>
</tr>
<tr>
<td>Computer Security Resource Center: <a href="https://csrc.nist.gov/publications">https://csrc.nist.gov/publications</a></td>
<td><a href="mailto:csrp-inquiry@nist.gov">csrp-inquiry@nist.gov</a></td>
</tr>
<tr>
<td>EXPORTECH <a href="https://www.nist.gov/exportech">https://www.nist.gov/exportech</a></td>
<td><a href="mailto:Brian.Lagas@nist.gov">Brian.Lagas@nist.gov</a></td>
</tr>
</tbody>
</table>
Questions?