RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PDSC-T09**

The Missing Supply Chain Link: A Safe Harbor for Risk Information Sharing

Edna Conway

Vice President, Security & Risk Officer, Azure
Microsoft
@edna_conway

Ari Schwartz

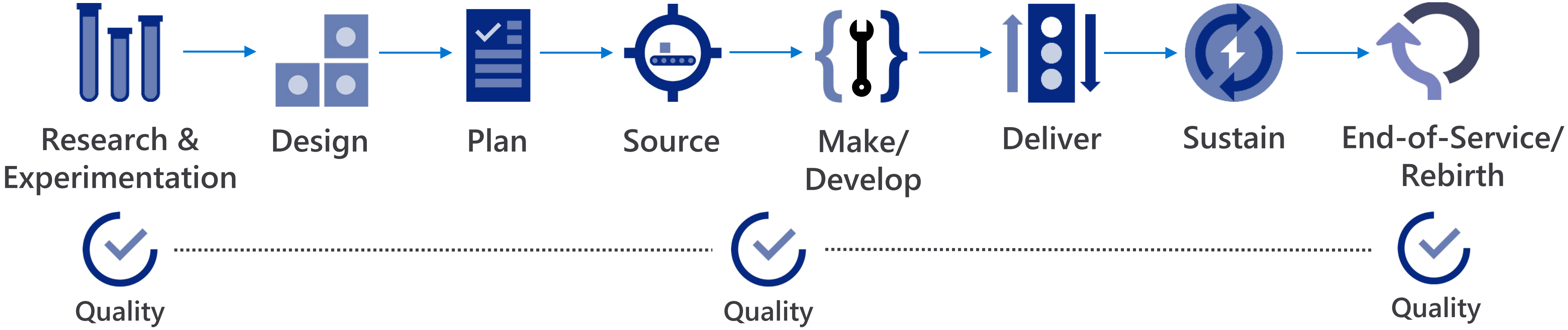
Managing Director for Cybersecurity Services
Venable LLP
Coordinator, Cybersecurity Coalition
@cybercoalition

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Supply Chain Risk: A Lifecycle Challenge



Hardware + Systems + Software + Firmware + Silicon

Supply Chain: A Critical Source of Risk

Over 12 years an average of

74%

security incidents linked to 3rd parties over the last 13 years

2010-2022 Verizon Data Breach Investigation Report

In 2021

91%

had an incident linked to a 3rd party

2022 Cyber Risk Alliance
3rd Party Risk in The Era of Zero Trust

In the prior 12 months

97%

suffered negative impact from a 3rd party's breach

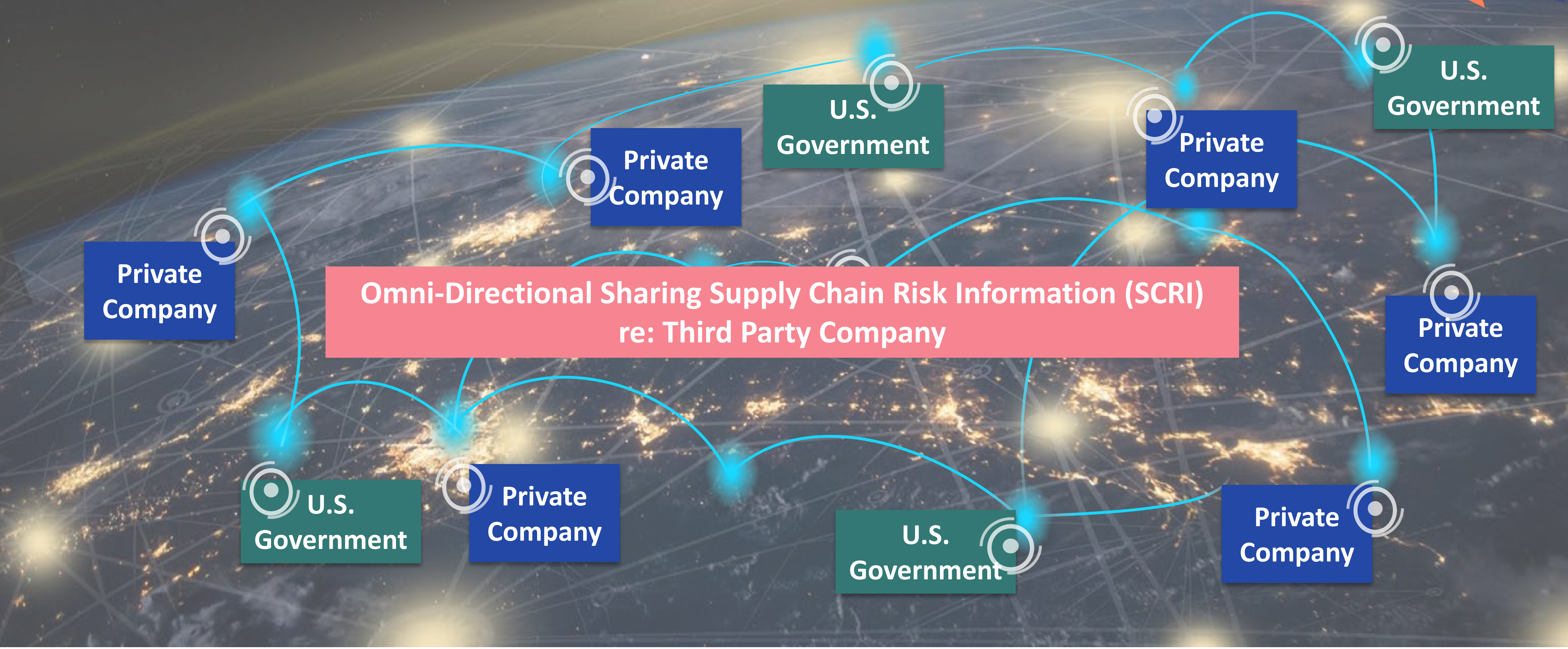
2021 BlueVoyant Managing Cyber Risk Across the Extended Vendor Ecosystem

The Depth of Hidden SC Risk

77% of enterprises have limited third party visibility*

*2020 BlueVoyant Global Insights: Supply Chain Cyber Risk

Information Sharing: Exposing Hidden SC Risk



Omni-Directional Sharing Supply Chain Risk Information (SCRI) re: Third Party Company

Today’s SC Risk Information Sharing Models

Law: Cybersecurity & Information Sharing Act of 2015 (CISA 2015):

- Some private sector liability protection for sharing certain “cyber threat” information

Public-Private Forums:

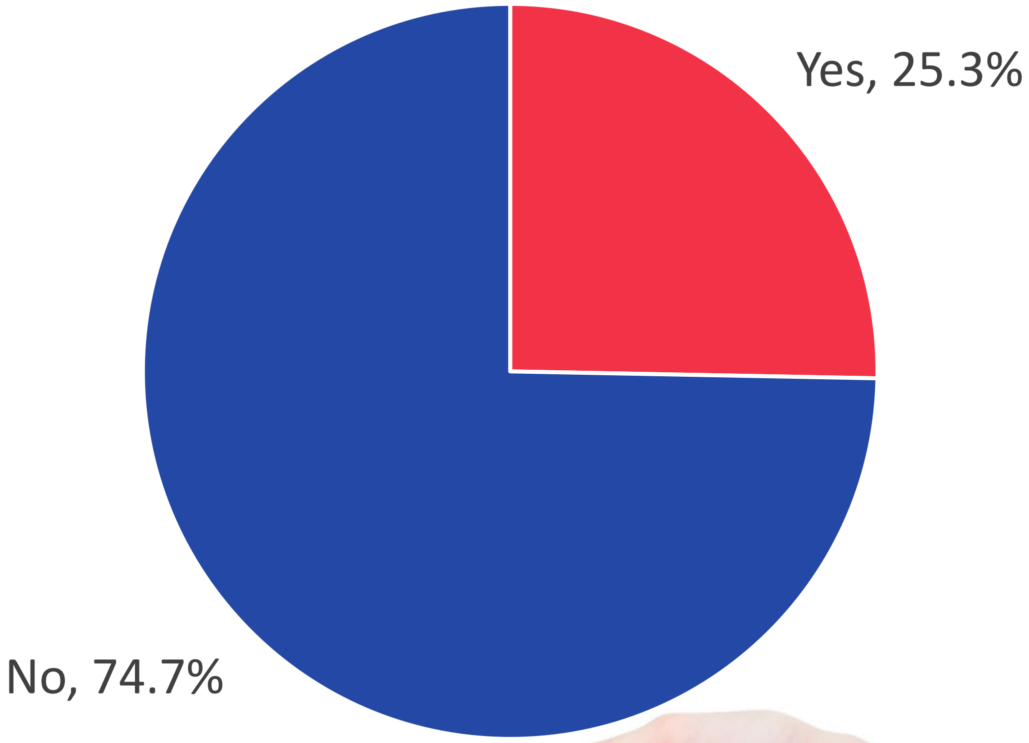
- ISACs, ISAOs, DHS Sector Coordinating Councils, Homeland Security Information Network, FBI Infragard, State Fusion Centers; Federal Acquisition Security Council (“Voluntary Information Submission)

US DHS Cybersecurity & Infrastructure Security Agency

- Threat Information Sharing Framework
- National Cybersecurity and Communications Integration Center (NCCIC)
- Automated Indicator Sharing (AIS)
- Cyber Information Sharing and Collaboration Program (CISCP)

Information Sharing: Kind of...But Not Really

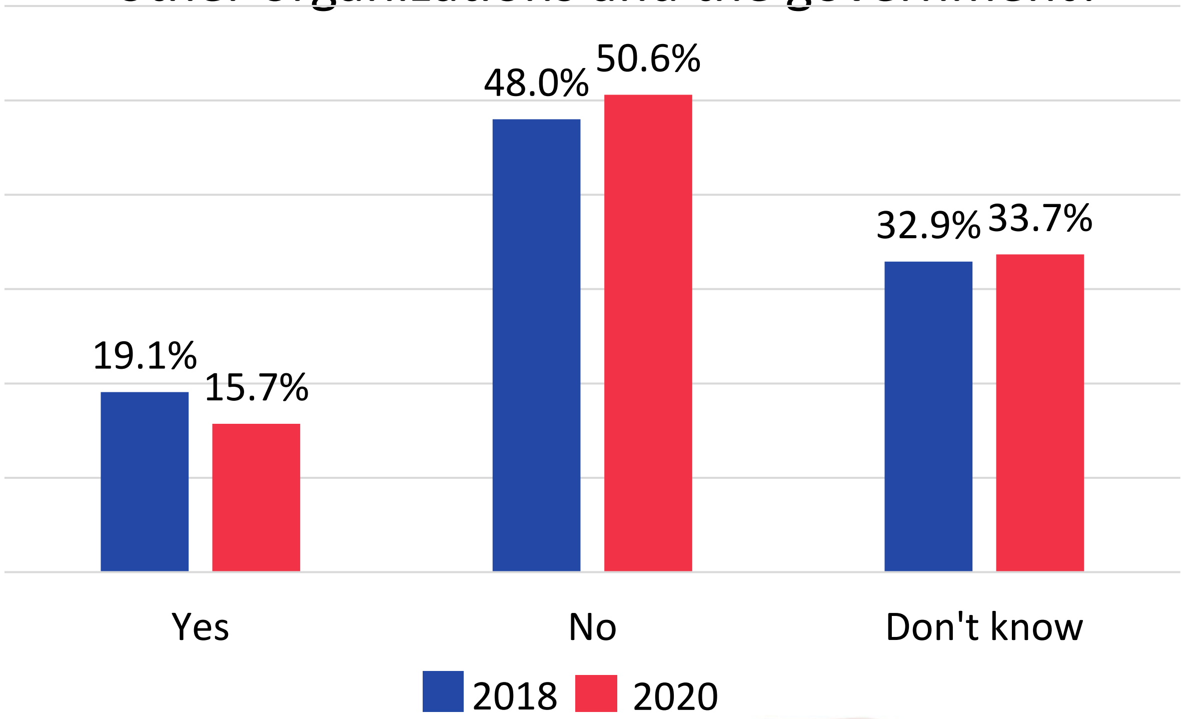
Does your organization have internal processes to utilize existing information sharing statutes and programs, such as the Cybersecurity Information Sharing Act of 2015 (CISA 2015)?



ASSOCIATION OF CORPORATE COUNSEL 2020 SURVEY DATA

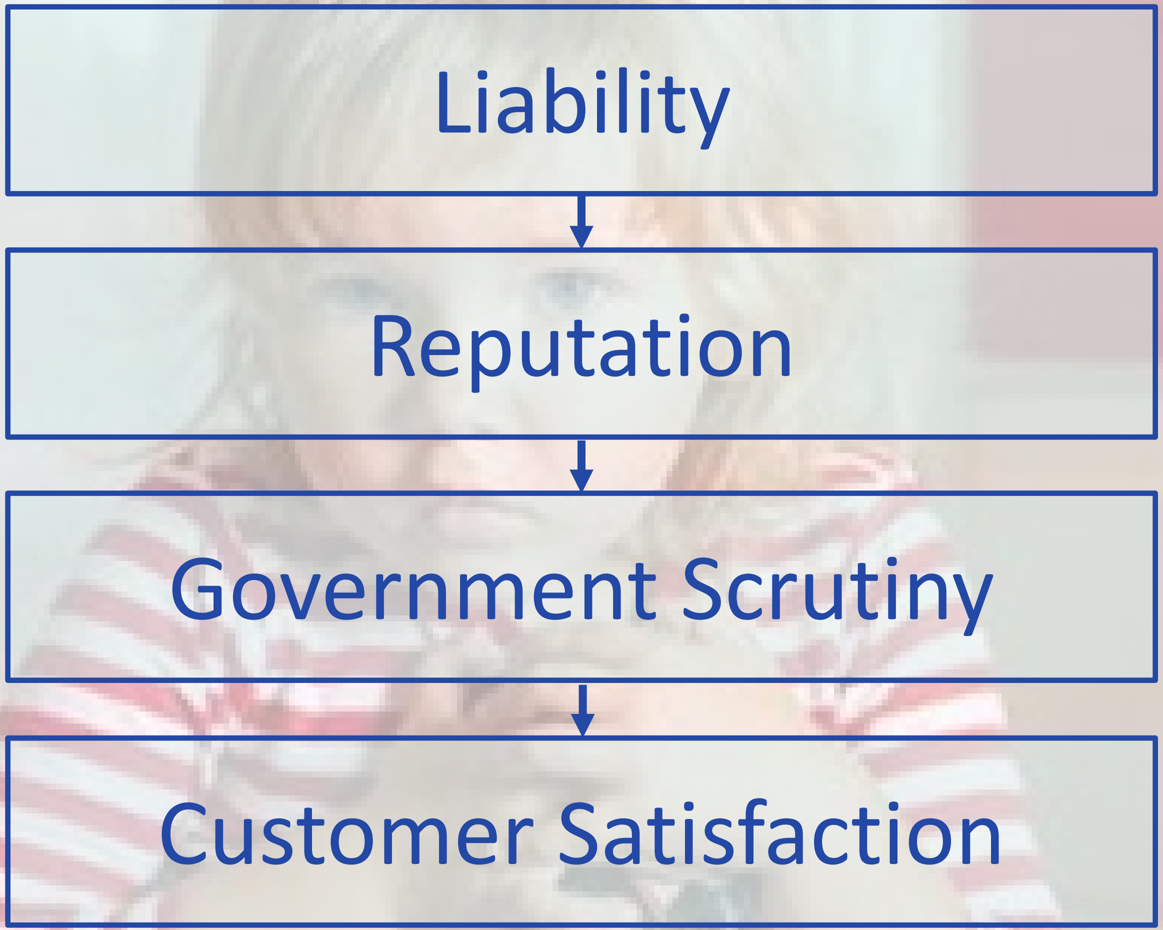
Information Sharing: Kind of…But Not Really

Does your organization participate in an information sharing and analysis organization to share cybersecurity threat information with other organizations and the government?



ASSOCIATION OF CORPORATE COUNSEL 2020 SURVEY DATA

Why Are Companies Reluctant to Share?



Liability

Reputation

Government Scrutiny

Customer Satisfaction

Growing Supply Chain Risk Efforts in U.S. Government

DHS Cybersecurity and Infrastructure Security Agency (CISA) - Information Communications Technology Supply Chain Risk Management Task Force

U.S. Department of Homeland Security

- Protectin rity Th ication Chain Th C 19-
- Supply Ch Ruler ocket 1
- Final Desig or Huawe any (PS D 19-351)
- Final Designation Proceeding for ZTE Corporation (PS Docket No. 19-352)
- Communications Security, Reliability, and Interoperability Council (CSRIC)

U.S. Depart nse

- NSA – Out Services SAT) To now avail p and (formerly Outso (RMC
- Cybersecu ertifica
- National De n Act (ND eral Acqu Regulation (FA ementation
- Alliance for Telecommunications Industry Solutions (ATIS)/DOD 5G SCRM

Department of Energy

- Supply Chain Risk Management Plan
- Cyber Testing for Resilient Industrial Control Systems (CyTRICS) Program

Executive Office of the President of the U.S.

tion and Communications

Assessment of Services Sector System ouncil (FASC)

tive Or he Uni
of Ma edera
al_Str he Un
tive Ord ening A s
cutive Order ing the Nati y

NIST

- NISTIR 8276
- TIR 8286
- 0-161 Re
- ationa of Excellence (NCCoE) – C Assurance
- -53A R

epartm ce

- ureau of Industr y (BIS) – Entities List, De Minimis Regulation
- Bureau of Industry and SecuriExport Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List
- National Telecommunications and Information Administration (NTIA) Software Bill of Materials (SBOM)

DHS ICT Supply Chain Risk Management Task Force

Key Work Groups

- Small and Medium-sized Businesses (SMB)
- Criteria for Qualified Bidder List Inclusion
- Framework of Threats Across the ICT SC
- Evaluation Criteria for Vendor SCRM Posture
- Lessons From Recent Software SC Attacks
- Covid-19 Risk Study

Information Sharing Framework:

Create common framework for omni-directional sharing of SCRM threat information

Information Sharing Work Group - Year 1

Mapping Exercise: Mapped Information available to SC Threats

Conclusion: Highest value information = exchange of supplier-specific risk creating information

Information Source Analysis

Conclusion: Suspect supplier information discovery—Earlier by industry, later by government

Impediment Analysis

Conclusion: Sharing is hampered by legal concerns, namely the prospect of facing a private cause of action, most likely brought by the supplier about whom the concerns were raised

Information Sharing Work Group - Year 2

Identify the Legal Impediments to Increased Information Sharing of SC Risk

- **Categories of Claims**
  - Tortious Interference with Existing Contract
  - Tortious Interference with Prospective Contract, Business Relationship or Business Advantage
  - Defamation
  - Business or Commercial Disparagement
  - Fraudulent Misrepresentation
  - Breach of Contract
  - Misappropriation of Trade Secrets
- **Mapping of key considerations** for litigation risk for each Category of Claim
- **Potential approaches to ↑ beneficial sharing while ↓ litigation risk:**
  - Education/outreach promoting > sharing of SCR information + liability risk reducing precautions
  - Ask for the relevant information through an existing government body
  - Longer-term changes in law

The Elephant in the Room: Naming Risk Actors

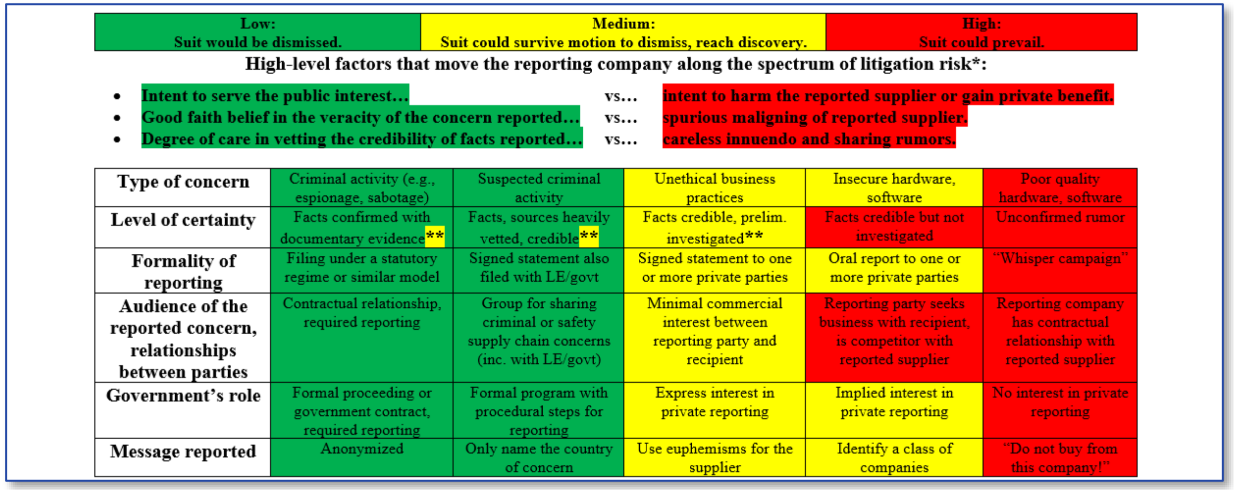
- ↑ Sharing the Most Valuable Information - Risky SC Actors/Activity
- ↓ Liability for Identifying Risky SC Actors/Activity

High-level factors that move the reporting company along the spectrum of litigation risk:

Intent to serve the public interest	vs.	intent to harm the reported supplier or gain private benefit
Good faith belief in the veracity of the concern reported	vs.	spurious maligning of reported supplier
Degree of care in vetting the credibility of facts reported	vs.	careless innuendo and sharing rumors

Conclusion:

Private Litigation Risk Spectrum



Low: Suit would be dismissed.	Medium: Suit could survive motion to dismiss, reach discovery.	High: Suit could prevail.

High-level factors that move the reporting company along the spectrum of litigation risk*:

- **Intent to serve the public interest…** vs… **intent to harm the reported supplier or gain private benefit.**
- **Good faith belief in the veracity of the concern reported…** vs… **spurious maligning of reported supplier.**
- **Degree of care in vetting the credibility of facts reported…** vs… **careless innuendo and sharing rumors.**

Type of concern	Criminal activity (e.g., espionage, sabotage)	Suspected criminal activity	Unethical business practices	Insecure hardware, software	Poor quality hardware, software
Level of certainty	Facts confirmed with documentary evidence**	Facts, sources heavily vetted, credible**	Facts credible, prelim. investigated**	Facts credible but not investigated	Unconfirmed rumor
Formality of reporting	Filing under a statutory regime or similar model	Signed statement also filed with LE/govt	Signed statement to one or more private parties	Oral report to one or more private parties	"Whisper campaign"
Audience of the reported concern, relationships between parties	Contractual relationship, required reporting	Group for sharing criminal or safety supply chain concerns (inc. with LE/govt)	Minimal commercial interest between reporting party and recipient	Reporting party seeks business with recipient, is competitor with reported supplier	Reporting company has contractual relationship with reported supplier
Government's role	Formal proceeding or government contract, required reporting	Formal program with procedural steps for reporting	Express interest in private reporting	Implied interest in private reporting	No interest in private reporting
Message reported	Anonymized	Only name the country of concern	Use euphemisms for the supplier	Identify a class of companies	"Do not buy from this company!"

Private Litigation Risk Spectrum

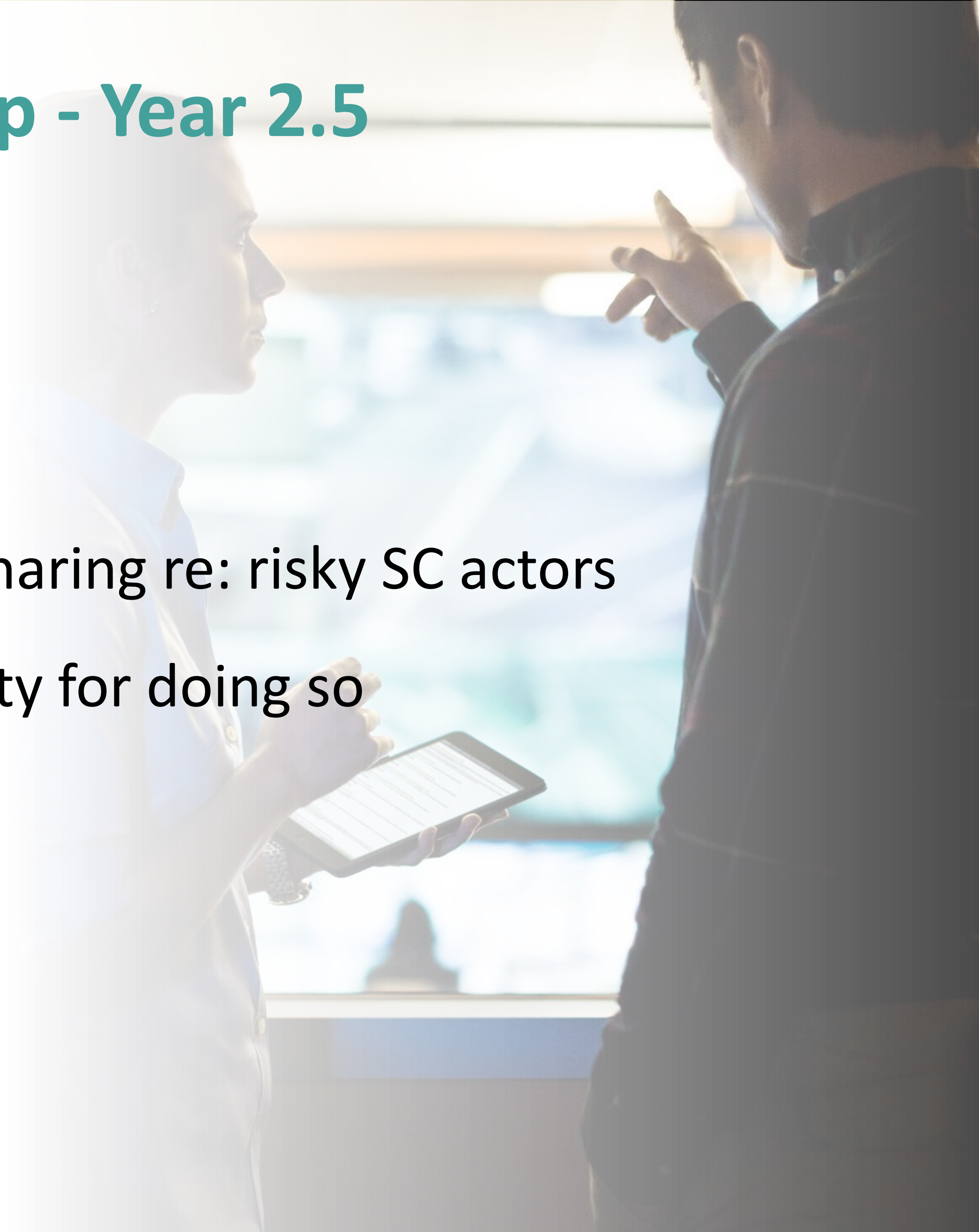
Type of concern	🟦 Criminal activity (e.g., espionage, sabotage)	🟦 Suspected criminal activity	🟨 Unethical business practices	🟨 Insecure hardware, software	🟥 Poor quality hardware, software
Level of certainty	🟦 Facts confirmed with documentary evidence	🟦 Facts, sources heavily vetted, credible	🟨 Facts credible, prelim. investigated	🟥 Facts credible but not investigated	🟥 Unconfirmed rumor
Formality of reporting	🟦 Filing under a statutory regime or similar model	🟦 Signed statement also filed with LE/govt	🟨 Signed statement to one or more private parties	🟨 Oral report to one or more private parties	🟥 "Whisper campaign"
Audience of the reported concern, relationships between parties	🟦 Contractual relationship, required reporting	🟦 Group for sharing criminal or safety supply chain concerns (inc. with LE/govt)	🟨 Minimal commercial interest between reporting party and recipient	🟥 Reporting party seeks business with recipient, is competitor with reported supplier	🟥 Reporting company has contractual relationship with reported supplier
Government's role	🟦 Formal proceeding or government contract, required reporting	🟦 Formal program with procedural steps for reporting	🟨 Express interest in private reporting	🟨 Implied interest in private reporting	🟥 No interest in private reporting
Message reported	🟦 Anonymized	🟦 Only name the country of concern	🟨 Use euphemisms for the supplier	🟨 Identify a class of companies	🟥 "Do not buy from this company!"

🟦 **Low:**
Suit would be dismissed

🟨 **Medium:**
Suit could survive motion to dismiss, reach discovery

🟥 **High:**
Suit could prevail

Information Sharing Work Group - Year 2.5



Final Goal

Identify Paths to:

- Ensure omni-directional information sharing re: risky SC actors
- Protect sharing enterprises from liability for doing so

Information Sharing: How to Do It Right!

Amend CISA 2015 to include:

- supply chain risk as a Cyber Threat Indicator
- a definition of supply chain risk that includes data & information
- preemption over conflicting state/federal laws
- exemption from possible antitrust violation
- segregation + exclusion of information extraneous to Supply Chain Risk

Apply

Public-Private Engagement

- ✓ Influence to enhance information sharing legislation
- ✓ Participate in industry associations or coalitions e.g.:
  - U.S. Chamber of Commerce
  - Information Technology Industry Council
  - USTelecom
- ✓ Take advantage of NGO Information Sharing Forums (ISACs, ISAOs etc.)

Enterprise Action

- ✓ Share your SC Security controls with your supplier ecosystem
- ✓ Adapt your controls to meet new demands and communicate changes with your supplier ecosystem
- ✓ Follow Information Sharing guidance in NIST 800-161 Rev. 1 (2nd draft) §3.2
- ✓ Meet CIS Critical Security Controls V8 IG1-3 Control 17.2

Thank you!

Cybersecurity Coalition

Microsoft