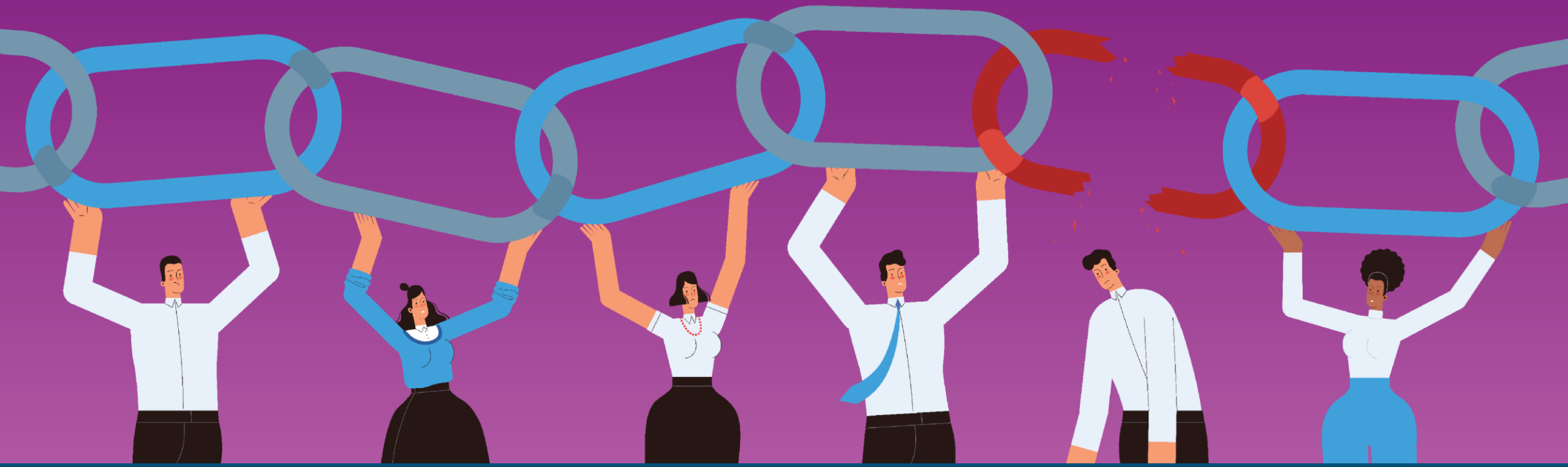
All together now

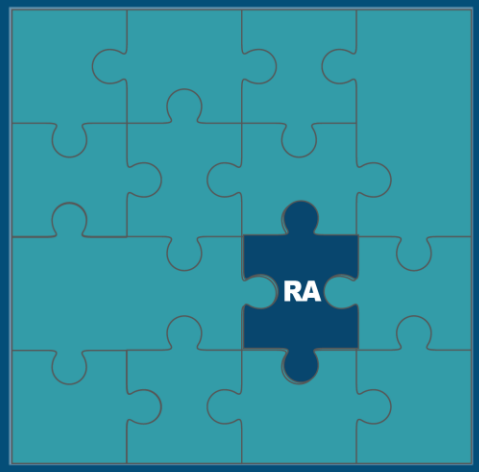
Exploiting the supply chain



NeoSystems & EXIGER | DECEMBER 12, 2024

CMMC #4: All Together Now

Exploiting the Supply Chain



Contractors comply with FAR, DFARS, and NIST because the Federal Government says they must.

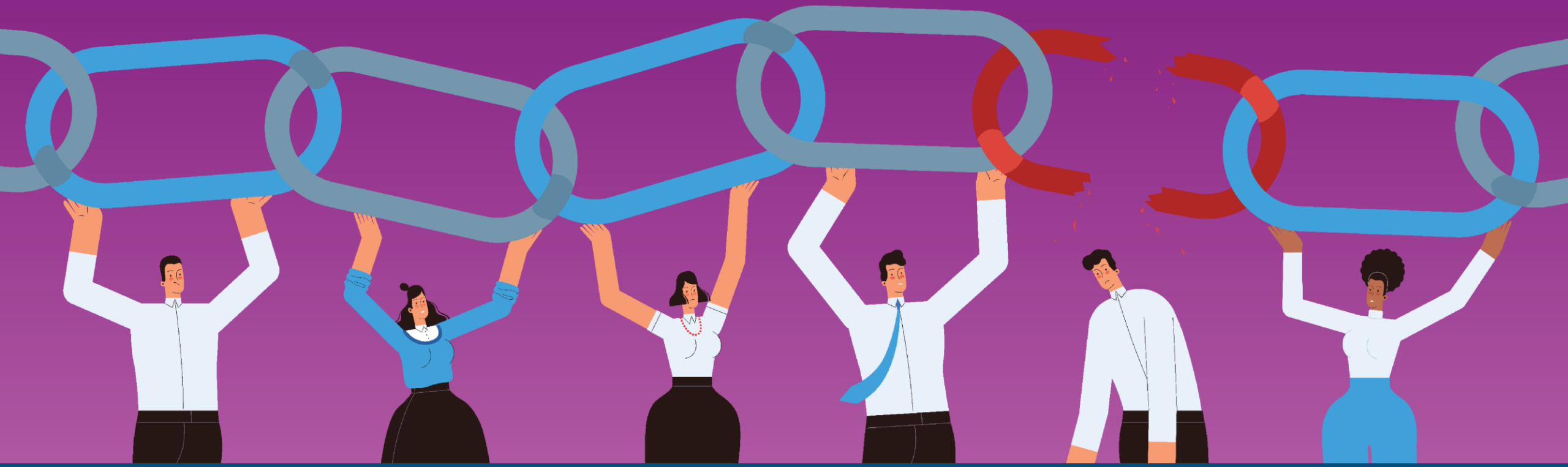
But to be effective, cybersecurity must align with the actual threats. In this series, we will explain the linkage between threats and the cybersecurity measures that counter those threats.

These webinars should help you make better choices about cybersecurity and reduce the likelihood that you will become a victim.

EPISODE 1	EPISODE 2	EPISODE 3	EPISODE 4	EPISODE 5	EPISODE 6	EPISODE 7	EPISODE 8
Shut the Front Door	Loose Lips Sink Ships	The K.I.S.S. Principle	All Together Now	Thinking Critically About Security	Rip the Band-Aid Off	Hiding in the Shadows	Working Hard or Hardly Working
How unauthorized access happens	*The role of user behavior in cyber attacks*	*How complexity & connectivity increase the probability and impact of a cyber incident*	*Exploiting the supply chain*	*You've already been hacked, or at least should act like it*	*Old security only leaks when it rains*	*How threats exploit the unprepared*	*How threat can tell the difference between real security versus fake security*

All together now

Exploiting the supply chain



NeoSystems & EXIGER | DECEMBER 12, 2024

Our Speakers

Stuart Itkin
NeoSystems

Ed Bassett
NeoSystems

Katie Arrington
Exiger

JC Herz
Exiger

Agenda

EPISODE 4:
All Together Now: Exploiting the Supply Chain

- Why supply chain risk is important to understand and manage
- What supply chains are we talking about
- How attacks on your supplier becomes an attacks on you
- How bad actors uncover and exploit vulnerabilities
- Consequences
- Case Studies: A large enterprise and a SMB
- Reducing supply chain risk
- Related NIST 800-171 control families
  - Risk Management

Supply Chain Risk

Cyber security breaches that occurred in the supply chain have negatively impacted **97%** of firms in the past 12 months.

-- BlueVoyant

77% of companies lack the data and knowledge to fully understand their supply chain risks

-- William Towers Watson

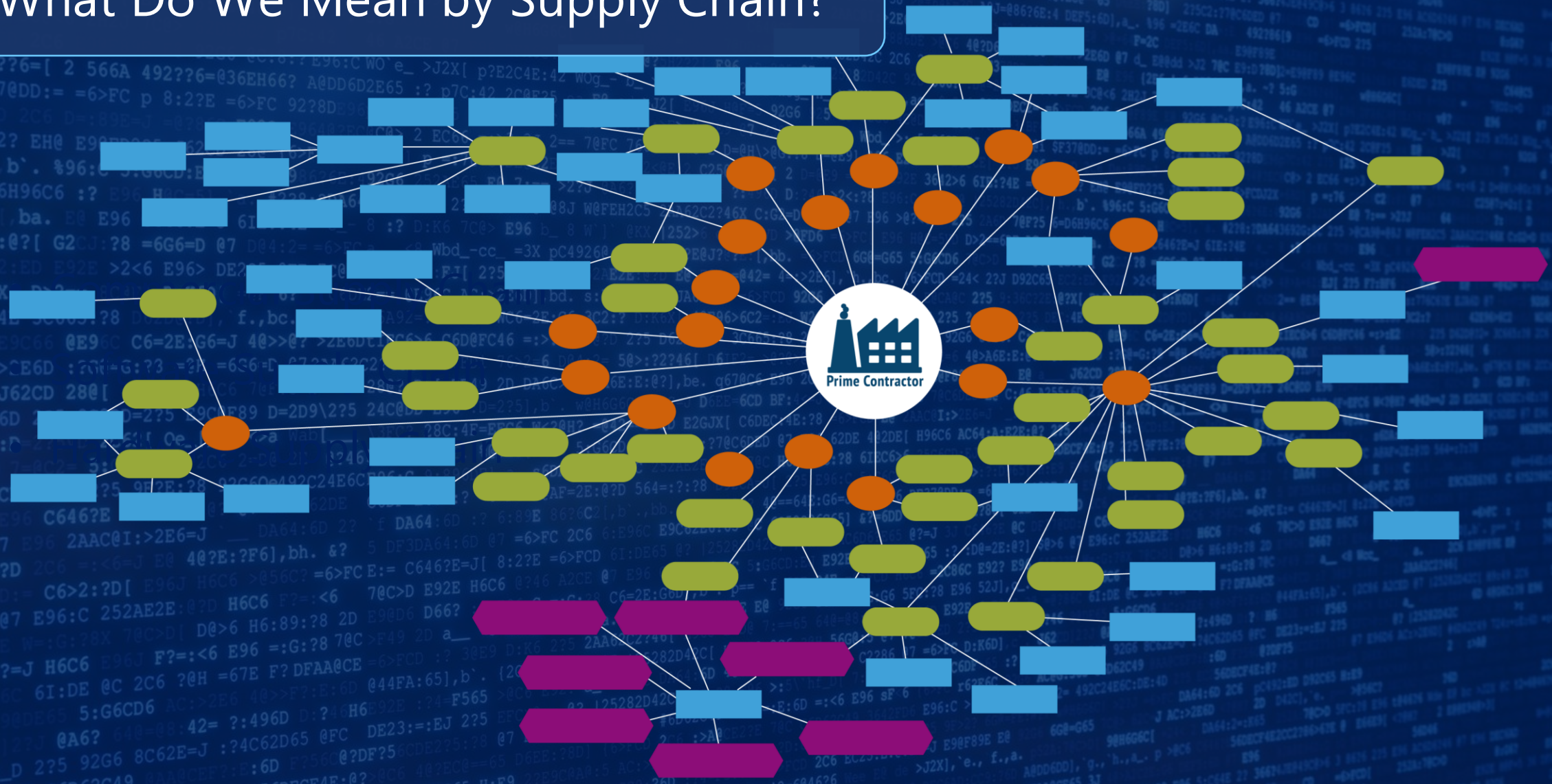
Supply chain attacks have increased by **78%** over the past year.

-- Symantec

88% of companies rate cyber risk as having a medium or high impact on their supply chain--

William Towers Watson

What Do We Mean by Supply Chain?

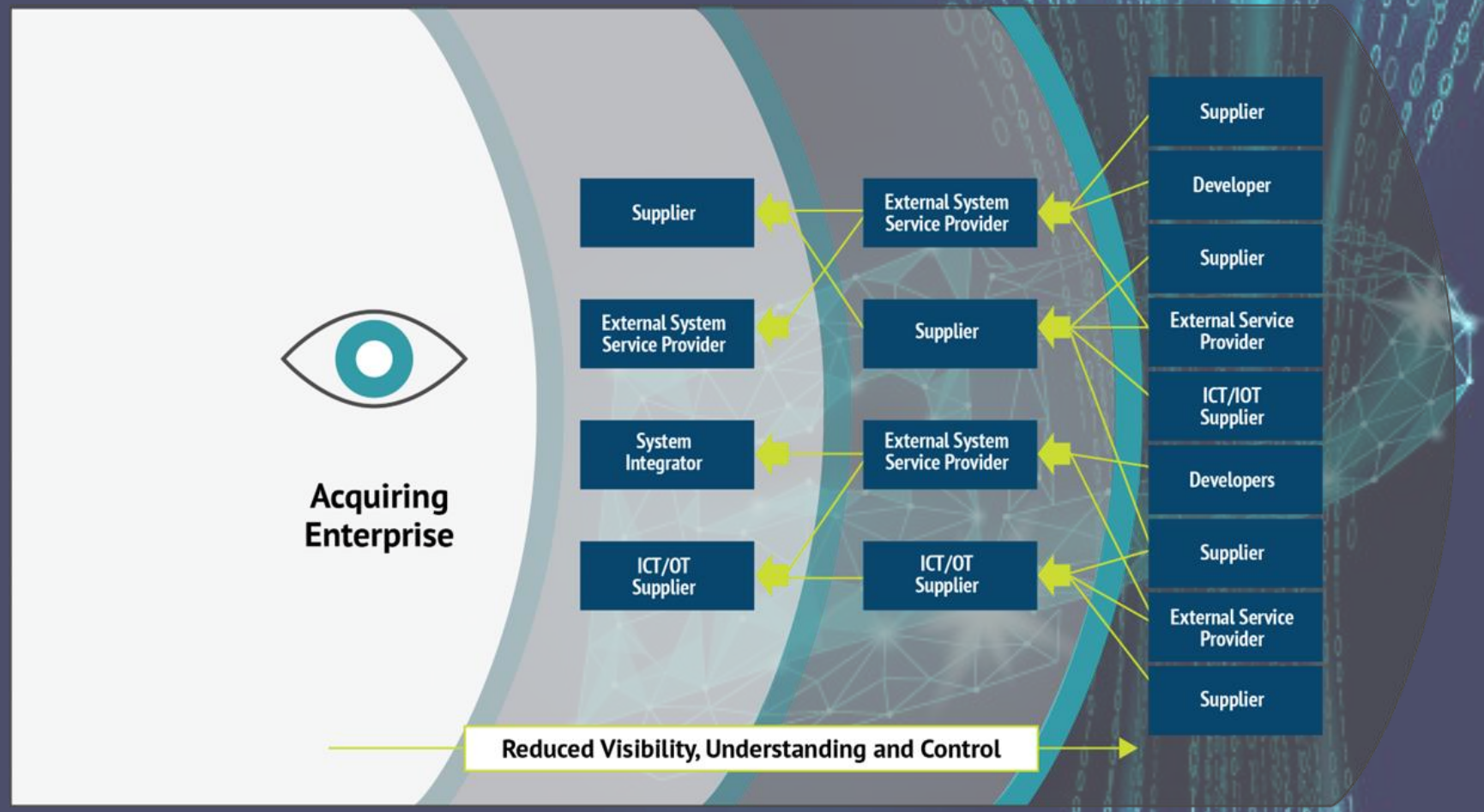


supply chain risk

noun sə'plaɪ tʃeɪn rɪsk | sə'plaɪ tʃeɪn rɪsk

the potential for disruptions or failures within a supply chain that can affect the flow of goods and services from suppliers to customers. These risks can arise from various sources, including natural disasters, cyber attacks, geopolitical issues, financial instability, and operational inefficiencies.

Risk With the Commercial Supply Chain



Hardware and Software Supply Chain Risk

The Bad Actor's Playbook

1. Gather information from public sources
2. Look for an open door
3. Trick someone into letting you in
4. Be sneaky – avoid detection
5. Establish a way to get back in whenever you want
6. Poke around looking for things of value ('living off the land')
7. Escalate privileges until you have the crown jewels

Case Study

- Massive worldwide impact
- Global economic impact exceeding $10 billion (Gartner)
- Spurred global reassessment of software supply chain security
- Unpatched systems remain vulnerable

Case Study

VISSERPRECISION™

- An attack of a small supplier can have a big impact
- Visser Precision shut down to investigate and remediate breach
- Lockheed Martin missile antenna schematic among stolen data
- Disrupted production at Northrup Grumman


Managing Supply Chain Risk

Government Playbook

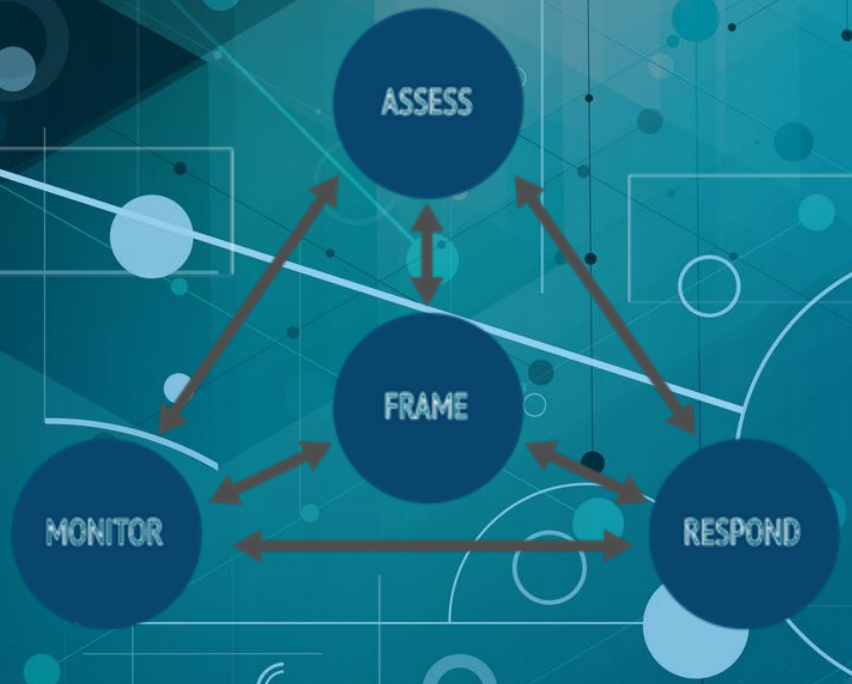
Requirements to address complexity and connectivity:

- Risk Management

Risk Assessment

Risk Assessment

- Frame Risk
- Assess Risk
- Respond to Risk
- Monitor Risk

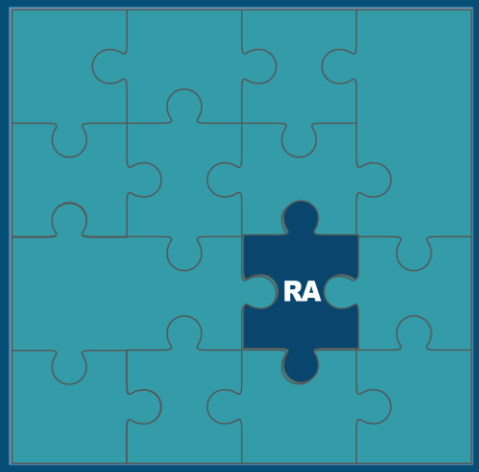


Takeaway Summary

1. Supply chains are complex and multi-tiered and include commercial, software, and electronics supply chains
2. Supply chain risk is multi-dimensional: cybersecurity, operational, financial, environmental, geopolitical, supplier
3. Disruption at any point affects the flow of goods, services, and information affecting others in the supply chain
4. Mitigate risk through regular assessments, robust risk management enhanced cybersecurity, and diversification

CMMC #4: All Together Now

Exploiting the Supply Chain



Contractors comply with FAR, DFARS, and NIST because the Federal Government says they must.

But to be effective, cybersecurity must align with the actual threats. In this series, we will explain the linkage between threats and the cybersecurity measures that counter those threats.

These webinars should help you make better choices about cybersecurity and reduce the likelihood that you will become a victim.

EPISODE 1	EPISODE 2	EPISODE 3	EPISODE 4	EPISODE 5	EPISODE 6	EPISODE 7	EPISODE 8
Shut the Front Door	Loose Lips Sink Ships	The K.I.S.S. Principle	All Together Now	Thinking Critically About Security	Rip the Band-Aid Off	Hiding in the Shadows	Working Hard or Hardly Working
How unauthorized access happens	*The role of user behavior in cyber attacks*	*How complexity & connectivity increase the probability and impact of a cyber incident*	*Exploiting the supply chain*	*You've already been hacked, or at least should act like it*	*Old security only leaks when it rains*	*How threats exploit the unprepared*	*How threat can tell the difference between real security versus fake security*

Questions?

Thank you.

Feel free to contact us:

stuart.itkin@neosystemscorp.com

ed.bassett@neosystemscorp.com

karrington@exiger.com

jcherz@exiger.com

www.neosystemscorp.com