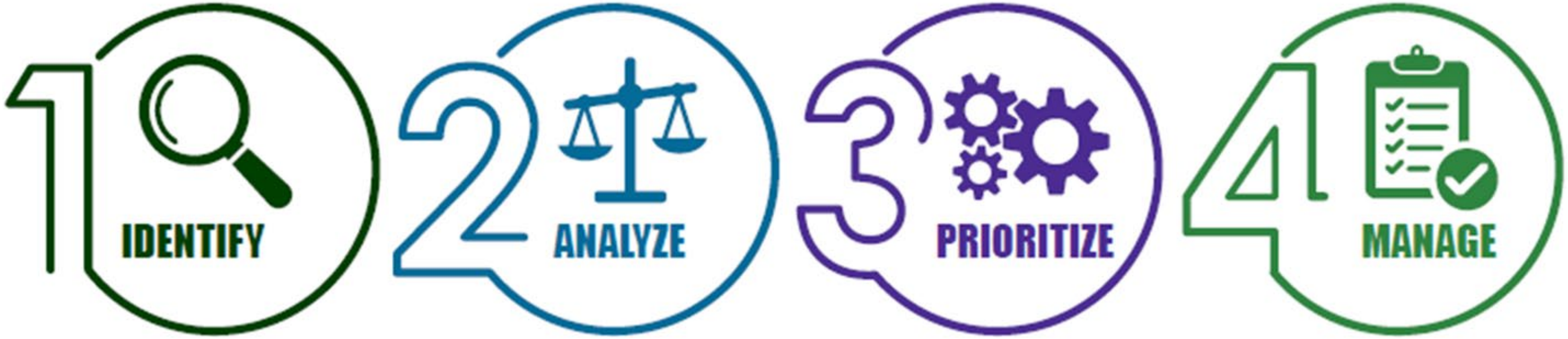
3RD ANNUAL NATIONAL

CYBERSECURITY SUMMIT

CISA Strategic Risk Management Process



Identify

- Publish National Critical Functions
- Convene public and private stakeholder groups connected by functions
- Identify and validate scenarios of concern

Analyze

- Engage with stakeholders to conduct risk analysis
- Assess risk from interdependencies and concentrated dependence on technology

Prioritize

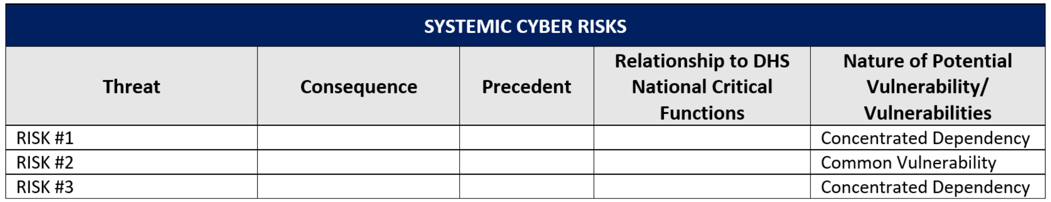
- Use risk and scenario analysis to build a Risk Register
- Consider risk and readiness for action to prioritize plans

Manage

- Convene teams to develop collaborative strategies
- Coordinate risk management and implementation plans

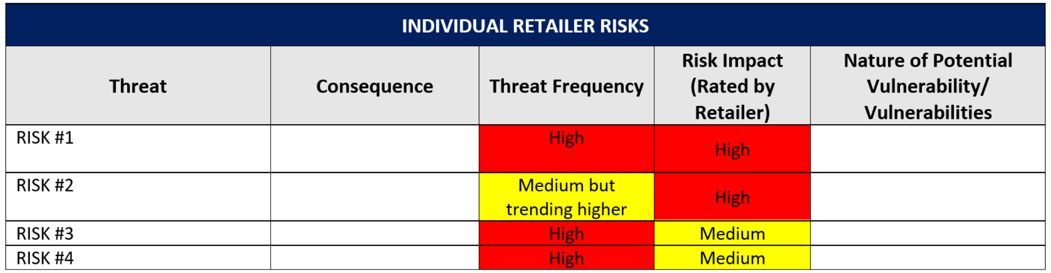
National Retail Federation (NRF) Cyber Risk Register

- Retail industry supports 1 in 4 American jobs; critical part of US economy as demonstrated during COVID-19 pandemic this year
- NRF has developed retail-focused risk register over past 18 months, working with input from retail CISOs and other members of NRF’s IT Security Council
- Includes both systemic and sector-specific individual risks relevant to retail companies – see illustrative version of framework (details removed) at right
- Current version of risk register addresses 8 systemic risks and 11 individual risks



SYSTEMIC CYBER RISKS

Threat	Consequence	Precedent	Relationship to DHS National Critical Functions	Nature of Potential Vulnerability/ Vulnerabilities
RISK #1				Concentrated Dependency
RISK #2				Common Vulnerability
RISK #3				Concentrated Dependency



INDIVIDUAL RETAILER RISKS

Threat	Consequence	Threat Frequency	Risk Impact (Rated by Retailer)	Nature of Potential Vulnerability/ Vulnerabilities
RISK #1		High	High	
RISK #2		Medium but trending higher	High	
RISK #3		High	Medium	
RISK #4		High	Medium	

Objectives for Risk Register:

- Inform decision-making and risk management by retail CISOs and other senior executives
- Provide government partners with priority intelligence requirements for sector
- Inform NRF’s own activities related to threat intelligence sharing, member education, exercises, etc.
- Align with other risk management frameworks