ncta

NCSL
NATIONAL CONFERENCE OF STATE LEGISLATURES

Cable Industry Leadership in Cybersecurity

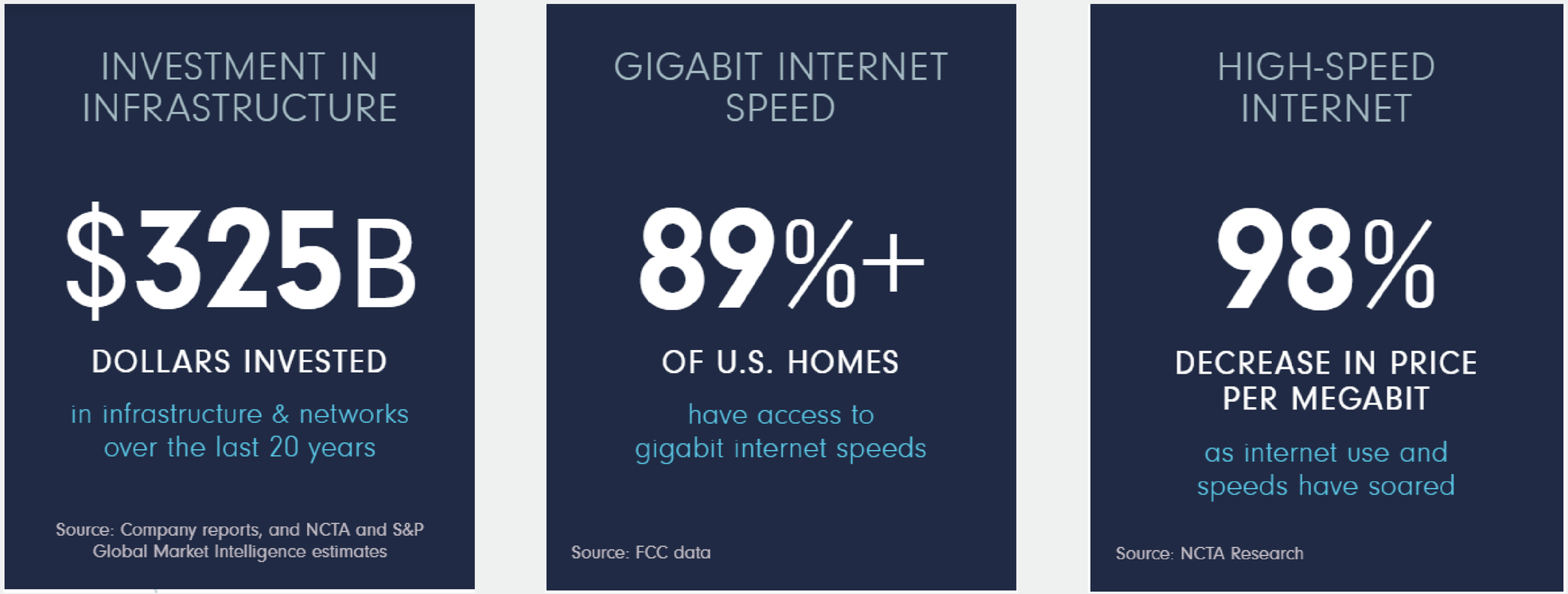
Robert Cantu

VP, Cybersecurity and Broadband Technology

MAY 17, 2024

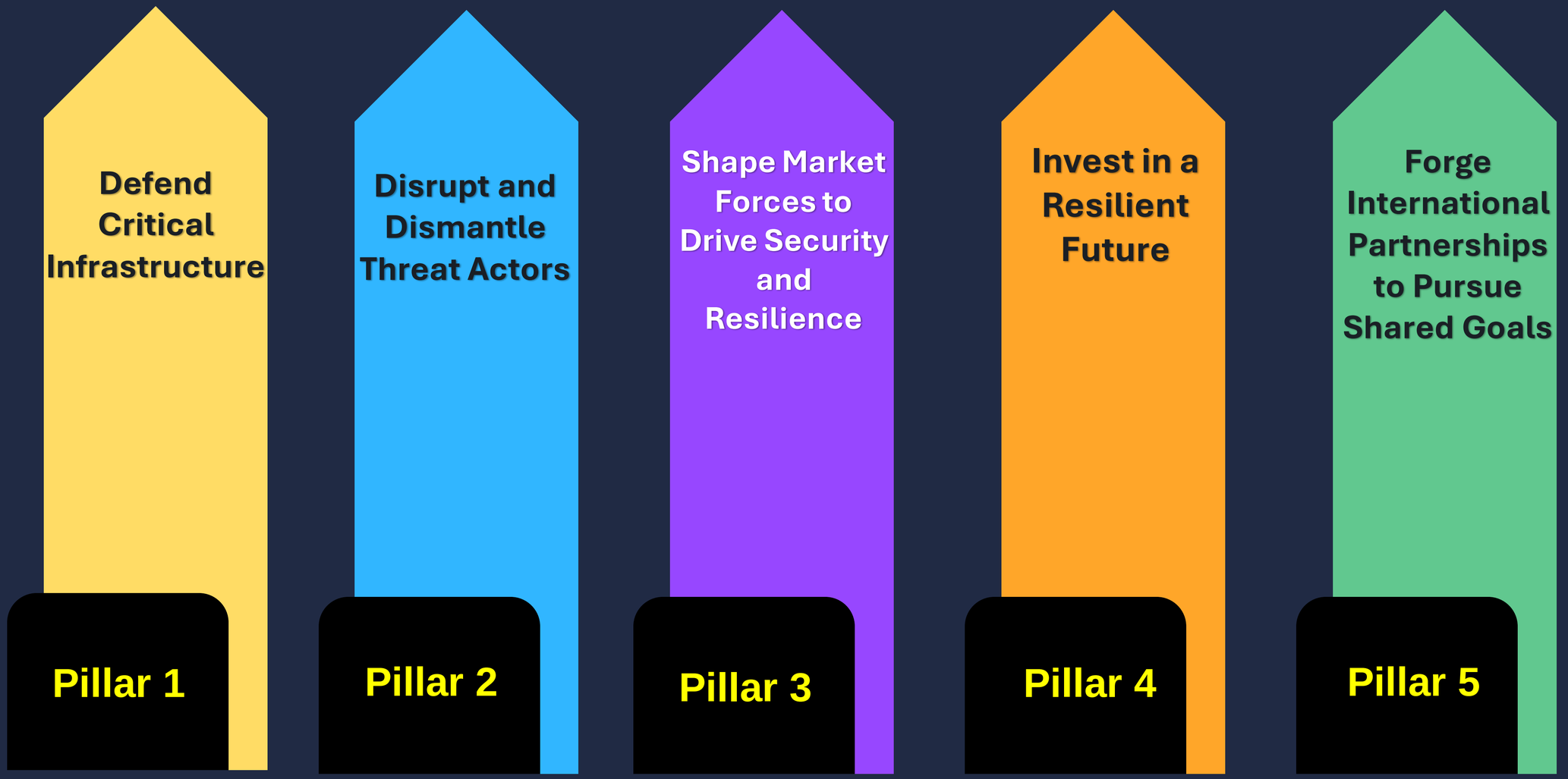
QUEBEC, QC

Cable ISP’s Leadership in Cybersecurity



- The Cable Industry remains the leading provider of broadband services in the US
- The Cable Industry Connects and Supports Critical Infrastructure
- In 2024, there are approximately 20 connected devices per household

National Cybersecurity Strategy Implementation Plan



Strategy and Plan Released in 2023
Updated in May 2024

National Security Memorandum - 22

Strategic Cybersecurity Policy

- Emphasis on enhancing digital infrastructure protection using Public-Private partnership

Supply Chain Resilience

- Prioritizing critical industries and technology supply chains.

Critical Infrastructure Defense

- Reinforced safeguards for energy, finance, healthcare, and communications.
- Implementation of rapid response protocols to incidents.

Information Sharing and Collaboration

- Improved information exchange between federal and state entities.
- Development of secure platforms for sensitive data sharing.

Workforce Development and Preparedness

- Support for state and local cybersecurity education initiatives, such as cybersecurity training.

International Partnerships

- Coordination with allies for a unified global cybersecurity stance, reinforced with joint incident response efforts

NIST Cybersecurity Framework 2.0 Overview

Version 1 released 10 years ago

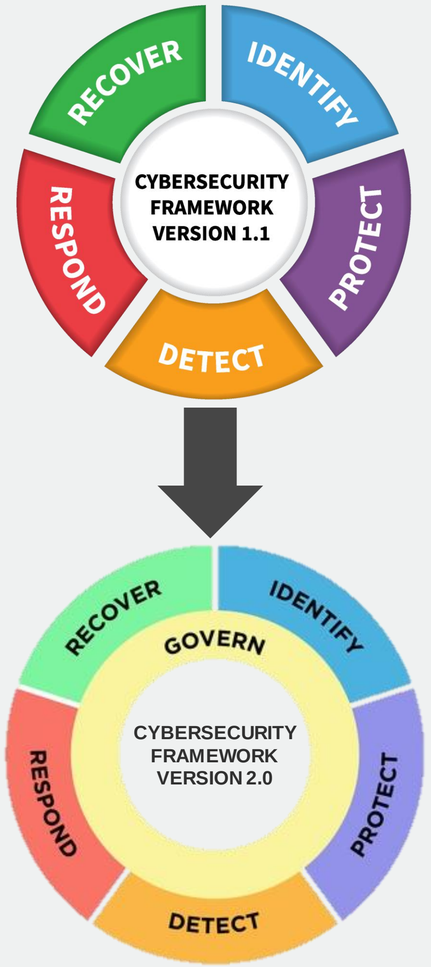
- Voluntary and focused on helping critical infrastructure to identify & assess their risks and develop processes to detect & respond

Version 1.1 released in 2018

- Updates focused on self assessments, supply chain risk mgmt, and vulnerability disclosure process.

Version 2 released in late Feb 2024

- Still voluntary, for every company, expanded risk assessment and supply chain vulnerabilities. Added sixth core function: Govern
- Equates Cyber risk with Legal, Financial and Business risks

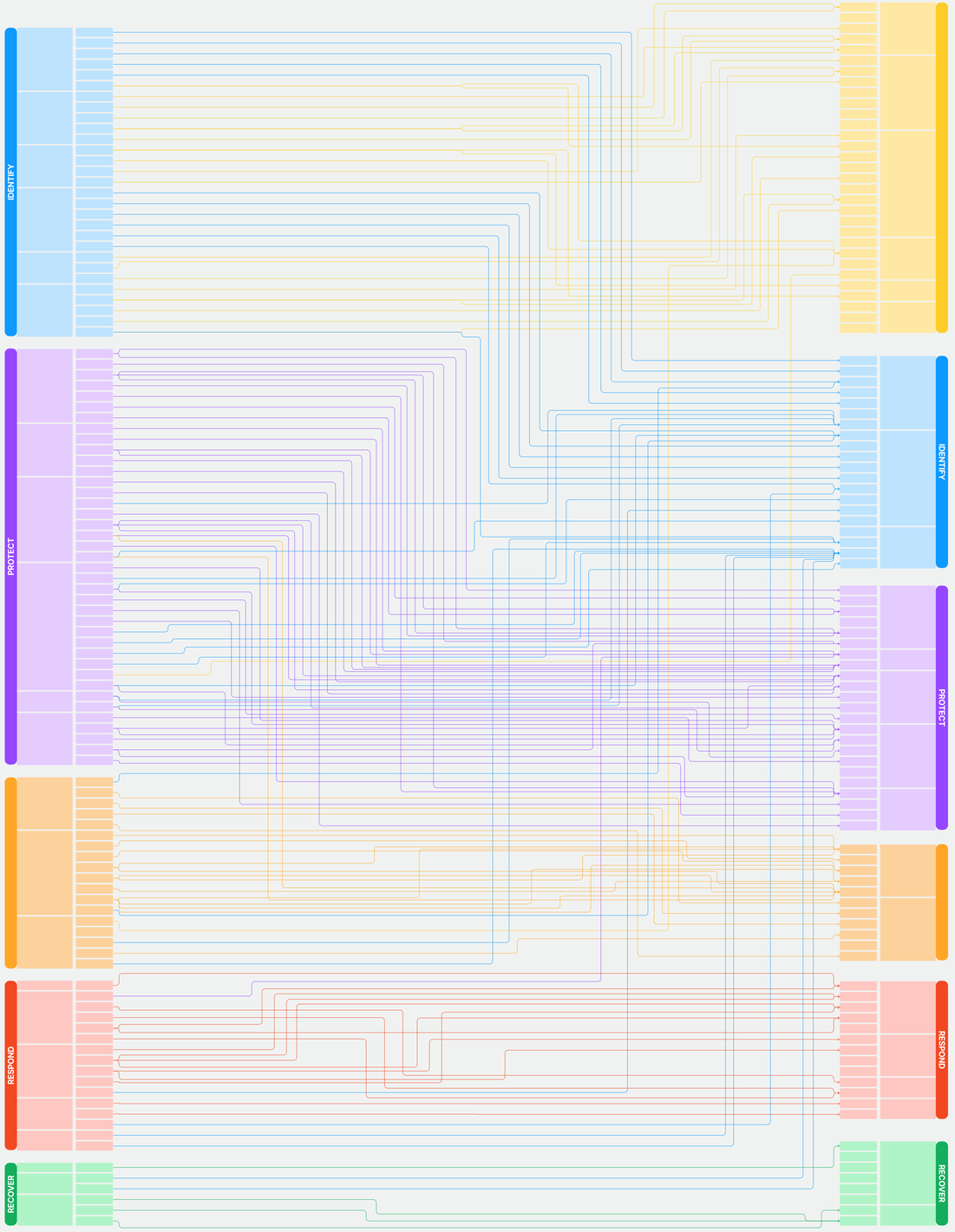


Comparison of CSF 1.1 to 2.0

New Governance Function largely comprised of existing Categories and Subcategories

14 Categories are new to Governance

- Organizational Context (stakeholders)
- Risk Management Strategy (priorities, constraints, risk tolerance and assumptions)
- Oversight is all new (Outcome of the organizational risk management strategy is communicated, evaluated and adjusted)



NCTA & Members Support CSF 2.0

- Cloud, IoT and the emergence of AI have changed industry since CSF was first released
- Integration with newer risk management and privacy framework guidance documents from NIST and the EU
- Under CEA, NIST is the “voluntary, consensus-based, industry-led” facilitator, without placing additional regulatory requirements on businesses
- C- SCRM – Agrees on the level (Category) and the integration of “GV.SC” in the Governance Function to be at the right level that bolsters the protection of first party organization.
- Via the CSF Profile – advocated for CableLabs Internet Routing Security Profile, which is a benchmark and a tool for risk-based guidance to address ISP and Autonomous Systems network routing risks.

NIST
National Institute of Standards and Technology

ncta
THE INTERNET & TELEVISION ASSOCIATION

CSF 2.0
Profiles

Facilitates Discussion & Prioritization

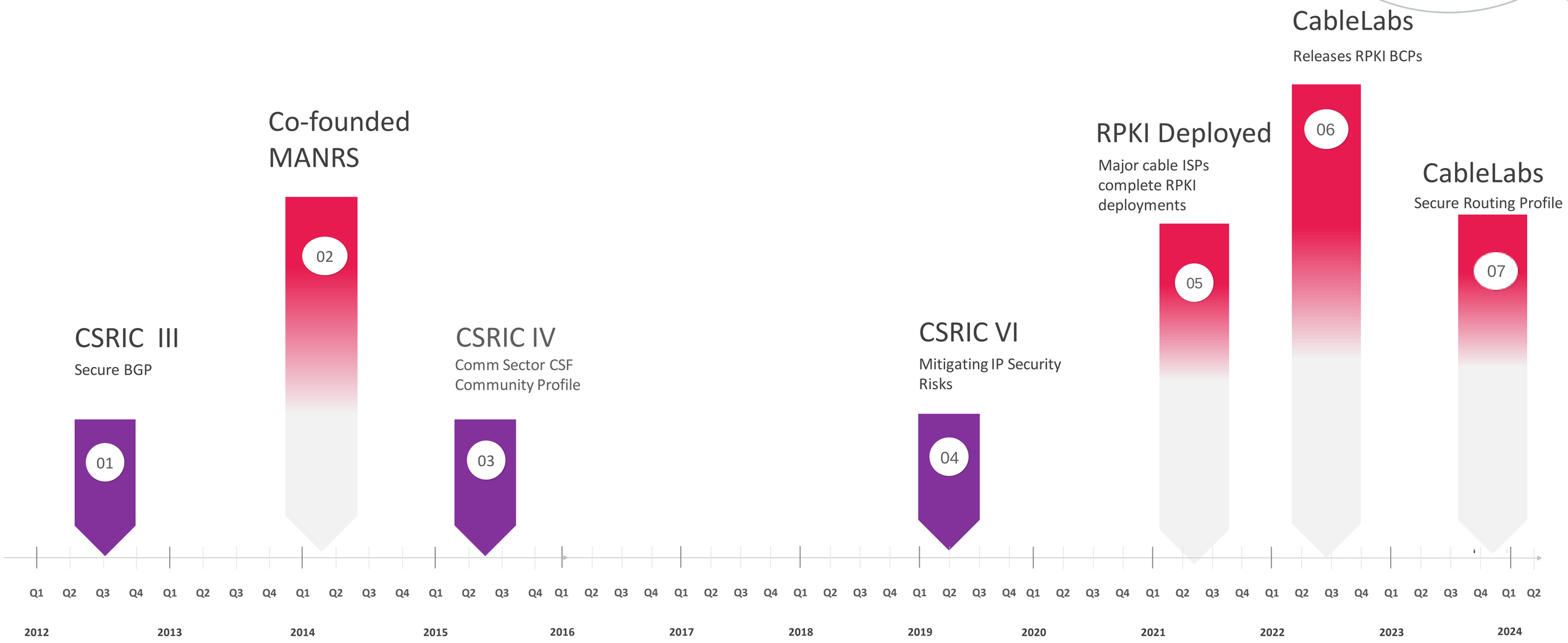
- Risk Management
- Cost Efficiency
- Regulatory Compliance
- Continuous Improvement

Flexible Scope

- Customizability
- Scalability
- Integration

Can Be Used for Strategic Planning,
Gap Analysis and Resource Allocation

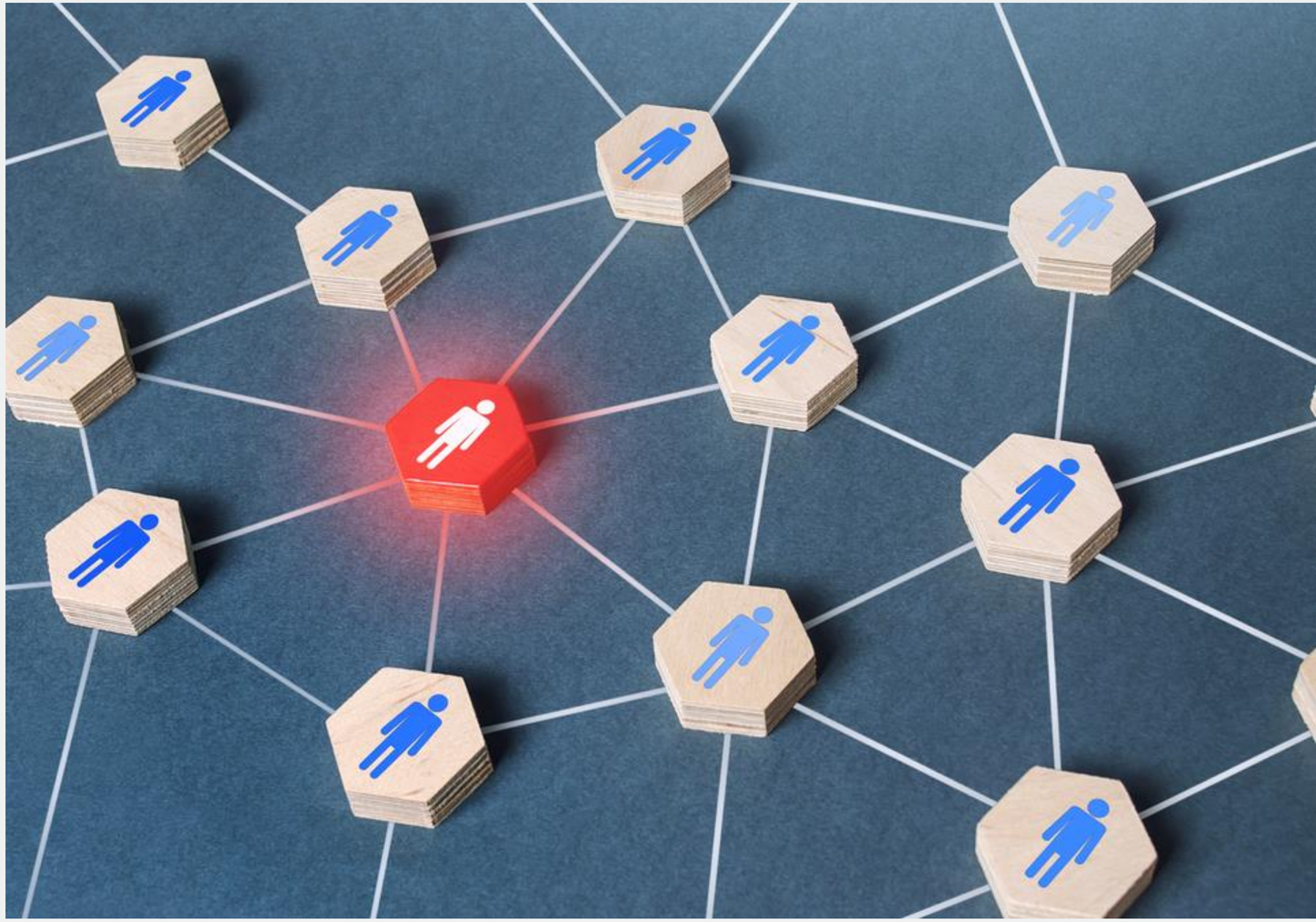
Cable’s History in Routing Security



Enhancing Cybersecurity Through NIST CSF and Secure Internet Routing

The Cable Sector uses the Cybersecurity Framework to plan, secure, defend and respond to any incursion on their networks.

The Secure Routing Profile uses and complements the Cybersecurity Framework. It enforces trusted routes with authentication and verification.



Questions?

Robert Cantu, VP Cybersecurity and Broadband Technology
rcantu@ncta.com

ROBERT CANTU, VP CYBERSECURITY AND BROADBAND TECHNOLOGY
RCANTU@NCTA.COM