TEXAS RE

Secure Tomorrow Toolkit

Devin Kitchens
Manager, CIP Compliance Monitoring

March 1, 2024

Secure Tomorrow Series Toolkit - Overview

What is it?

Free Knowledge Base

- Identify Emerging Risks
- Develop Risk Mitigation Strategies
- Long-Term Planning

Scenario Workshop

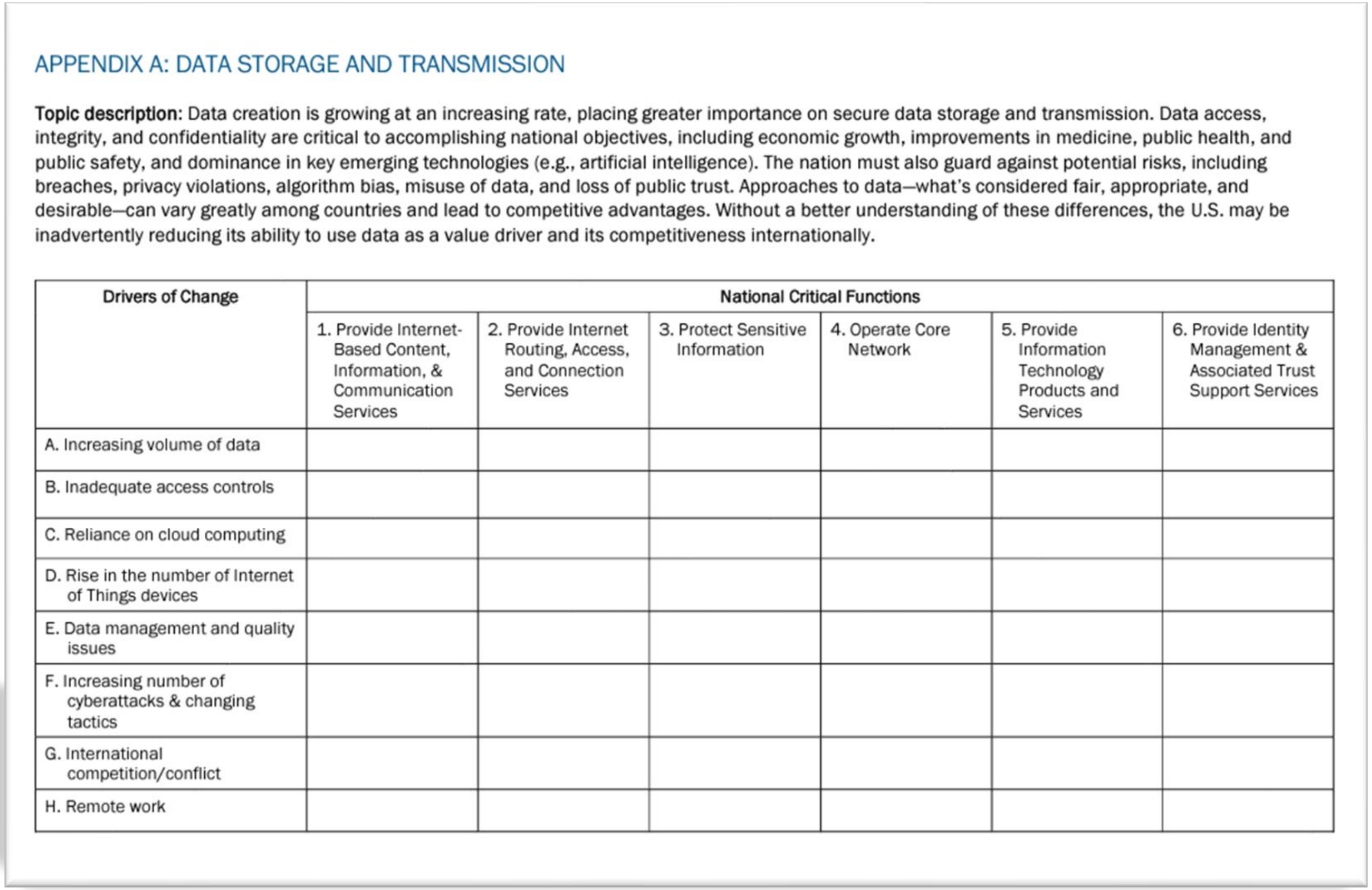
Scenario Workshop Content

- Synopses
- Facilitator Guides
- Road maps

Matrix Games

Data Privacy, Storage, and Transmission

Cross-Impacts Session

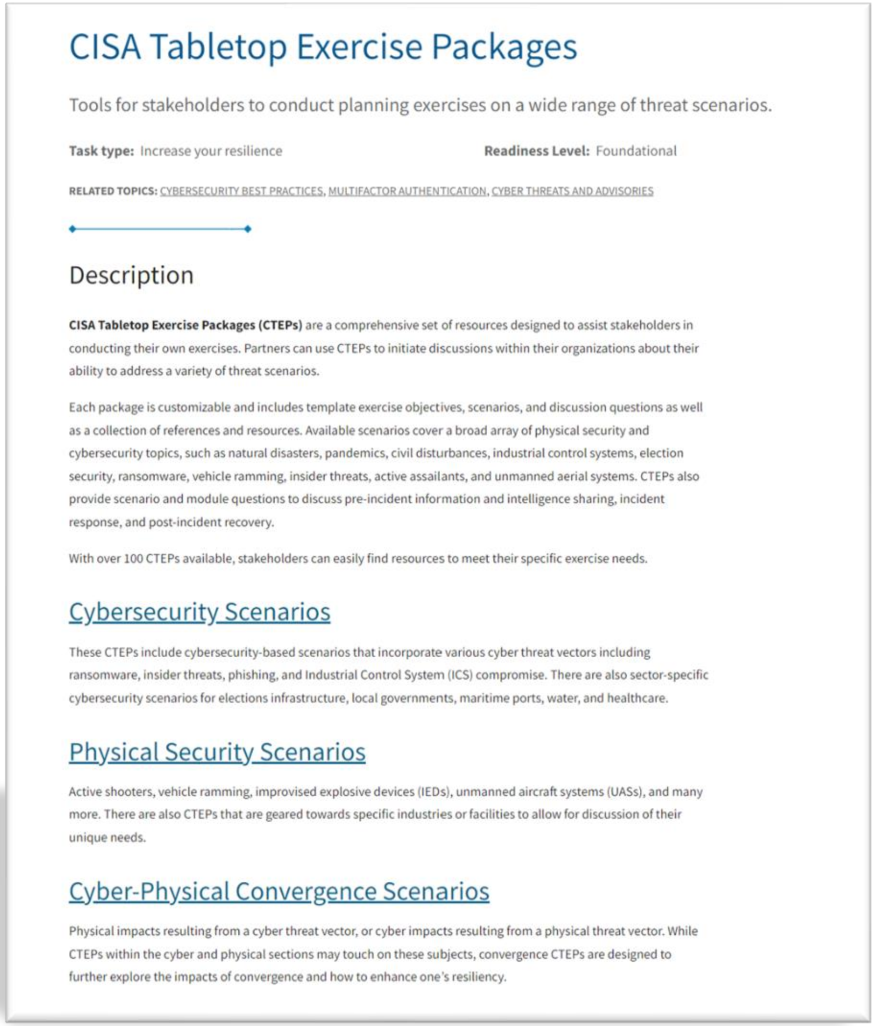


APPENDIX A: DATA STORAGE AND TRANSMISSION

Topic description: Data creation is growing at an increasing rate, placing greater importance on secure data storage and transmission. Data access, integrity, and confidentiality are critical to accomplishing national objectives, including economic growth, improvements in medicine, public health, and public safety, and dominance in key emerging technologies (e.g., artificial intelligence). The nation must also guard against potential risks, including breaches, privacy violations, algorithm bias, misuse of data, and loss of public trust. Approaches to data—what's considered fair, appropriate, and desirable—can vary greatly among countries and lead to competitive advantages. Without a better understanding of these differences, the U.S. may be inadvertently reducing its ability to use data as a value driver and its competitiveness internationally.

Drivers of Change	National Critical Functions					
	1. Provide Internet-Based Content, Information, & Communication Services	2. Provide Internet Routing, Access, and Connection Services	3. Protect Sensitive Information	4. Operate Core Network	5. Provide Information Technology Products and Services	6. Provide Identity Management & Associated Trust Support Services
A. Increasing volume of data						
B. Inadequate access controls						
C. Reliance on cloud computing						
D. Rise in the number of Internet of Things devices						
E. Data management and quality issues						
F. Increasing number of cyberattacks & changing tactics						
G. International competition/conflict						
H. Remote work						

Other CISA Resources



CISA Tabletop Exercise Packages

Tools for stakeholders to conduct planning exercises on a wide range of threat scenarios.

Task type: Increase your resilience

Readiness Level: Foundational

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, MULTIFACTOR AUTHENTICATION, CYBER THREATS AND ADVISORIES

Description

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources. Available scenarios cover a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems. CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response, and post-incident recovery.

With over 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs.

Cybersecurity Scenarios

These CTEPs include cybersecurity-based scenarios that incorporate various cyber threat vectors including ransomware, insider threats, phishing, and Industrial Control System (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.

Physical Security Scenarios

Active shooters, vehicle ramming, improvised explosive devices (IEDs), unmanned aircraft systems (UASs), and many more. There are also CTEPs that are geared towards specific industries or facilities to allow for discussion of their unique needs.

Cyber-Physical Convergence Scenarios

Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector. While CTEPs within the cyber and physical sections may touch on these subjects, convergence CTEPs are designed to further explore the impacts of convergence and how to enhance one's resiliency.

Questions?

TEXAS RE

Ensuring electric reliability for Texans