CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

Building Resilience for Critical Infrastructure

October 11, 2024

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established a Building Resilience for Critical Infrastructure (BR) subcommittee (hereinafter referred to as the "subcommittee") to enhance national resiliency.

In January 2024, the BR subcommittee was tasked with providing recommendations for full Committee deliberation and vote to help CISA prioritize and align cybersecurity and resilience efforts for the greatest impact, in the context of threats posed by the People's Republic of China. The subcommittee tasking document also included the following tasking questions to guide the subcommittee's work:

1. Taking the PRC's goals and targets into account, how should CISA best align its cybersecurity and resilience efforts for the greatest impact?
2. What key metrics would help determine how resilience is increased?

Findings

Through regular meetings, the subcommittee captured the following key takeaways:

- With limited exception, critical infrastructure and government agencies have not prepared for a contested environment as a result of nation-state conflict.
- "Living off the land" challenges traditional methods of threat detection; risk mitigation solutions are as important as threat intelligence in this context; tailored strategies are required to take into account the unique context, technology, and threat profiles of each sector.
- Third party risk from dependencies outside of designated critical infrastructure (e.g., Microsoft CrowdStrike incident) has the potential to amplify scale and severity of attacks.
- Improving cyber defense can help shrink attack surfaces and reduce risk, but a focus on the resilience of critical entities and functions is ultimately necessary.
- Sectors are deeply interconnected, and a handful of sectors are critical dependencies for all (i.e., lifeline sectors) during resilience planning.
- There are various authorities and programmatic efforts (e.g., Primary Mission Essential Functions (PMEFs), National Retail Federation (NRF), National Critical Functions (NCF), The National Cyber Incident Response Plan (NCIRP), The White House released National Security Memorandum 22 (NSM-22)), as well as regulatory authorities that may facilitate or impede important actions during a crisis.
- Resilience and business continuity planning (including analogue measures) often requires dedicated long-term efforts within companies and sectors. CISA should prioritize its own short-term focus (before 2027) on resilience measures that can be quickly implemented and on enhanced defense and improved coordination.

Recommendations

- To increase national resilience, CISA's Joint Cyber Defense Collaborative (JCDC) should work with Sector Risk Management Agencies (SRMAs) to ensure resilience, contingency planning, and planning for nation-state conflict are considered in the execution of NSM-22 responsibilities. This should include Sector Risk Assessments and Sector Risk Management Plans.

  - CISA should work with government and industry stakeholders to create a repeatable process to identify and prioritize critical services in Sector Risk Management Plans. This should prioritize the key missions a Critical Infrastructure/Key Resources supports, in addition to the entity's own critical functions.
  - JCDC should work with SRMAs and Federal regulators to establish an effective process to provide sector regulatory waivers necessary to maintain resilience during a crisis. This process should be included in Sector Risk Management Plans.
  - JCDC should sponsor sector-specific and cross-sector exercises set against scenarios related to nation state conflict. These scenarios should test coordination, communication, and contingency/continuity planning.

- To strengthen national cyber defense, JCDC should continue to provide robust threat intelligence that includes risk mitigation solutions, along with threat actor attributions and technical threat indicators.
  - CISA should play the role of targeted intelligence support for SRMAs that currently do not have a mature intelligence function.
  - CISA should provide the Office of the Director of National Intelligence (ODNI) with appropriate guidance so that it may effectively carry out its intelligence support responsibilities under NSM-22.

- To increase the engagement of the vendor community and smaller Systemically Important Entities (SIEs) in CISA advisories and cyber defense efforts, CISA should consider:
  - Identifying critical third parties in the cross-sector risk assessment and designate them as SIEs.
  - Investing in security and resilience outcomes at smaller SIEs through federal grant-funded cyber-in-a-box services. These grants, which have been successful at the state-level (e.g., New Hampshire program), would provide direct funding for multi-year cybersecurity risk assessments and prioritized mitigations.
  - Building a mentorship program to tap more mature, resourced SIEs to work with smaller SIEs on cybersecurity uplift.
  - Exploring ways to cut the noise around advisories and make them more accessible (e.g., work with cybersecurity vendors to integrate into services, tag relevant industries, etc.)

- To measure the impact of CISA advisories on Volt Typhoon and other related threat actors, CISA should work with partners to collect targeted data.
  - CISA should ask SRMAs to determine receipt, adoption, and impact of CISA advisories within their sectors broadly, as well as specific to sector SIEs. SRMAs may collect this data by directly issuing Frameworks for Reducing Cyber Risks to Critical Infrastructure (RFIs) or by asking sector Information Sharing and Analysis Center (ISACs) to survey membership. CISA might also consider whether Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) or a CIRCIA-like authority may facilitate collection of such data from SIEs.
  - The Cyber Safety Review Board (CSRB) should consider, as part of its review of incidents, whether CISA advisories were effective in providing timely and actionable information for critical infrastructure to defend against nation state threats.

Appendix 1:

The following BR subcommittee members contributed towards this report:

- Lori Beer, Chair
- Marene Allison
- Stan Connally
- Sunil Dadlani
- Ben Flatgard
- Brian Gragnolati
- Rekha Gunjal
- Rick Holmes
- Rahul Jalali
- Jon Jenkerson
- Jim Langevin
- Cathy Lanier
- Kevin Mandia
- Stacy O'Mara
- Paula Reynal
- Katheryn Rosen
- Robert Scott
- Suzanne Spaulding
- Claire Teitelman