IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Systemic Cyber Risk Reduction Venture

A RISK-BASED APPROACH TO NATIONAL CYBERSECURITY

In January 2021, the **National Risk Management Center (NRMC)**, within the **Cybersecurity and Infrastructure Security Agency (CISA)**, kicked off the **Systemic Cyber Risk Reduction Venture** (or Cyber Venture) to drive action and innovation around the development of models to assess the ways cyber risks or incidents could affect national security. As the nation's risk adviser, CISA, through the NRMC, will lead the charge to bring together new ideas, cutting-edge research, and enterprise risk management best practices from across the enterprise and cyber risk communities to progress meaningful action to reduce the country's susceptibility to cyber incidents.

What is Meant by Systemic Risk?

Systemic risk occurs when risk is spread across interdependent systems[1] so that a failure of one component has consequences system wide, amplifying the impact of the incident. In this context, the NRMC is looking to identify and understand the ways that cyber risks or incidents in individual pieces or components of critical infrastructure or National Critical Functions could create far-reaching cascading impacts, leading to system-wide functional degradation or failure.

Why a Venture?

A Venture naturally suggests a bold undertaking. With this effort, the NRMC will build on previous work, while also looking toward the future with renewed innovation and collaboration. Through this Venture, we will work with the cyber risk community to build collective energy around applying systemic cyber risk reduction to the national security space in a way that will generate system-wide solutions.

What are NCFs?

To understand the Cyber Venture, it is helpful to have some background about the National Critical Functions (NCFs). The NCFs are the services provided by government and the private sector that have been deemed so important that a disruption in their function would significantly impact national or economic security or public health and safety. They provide an outcome-focused lens, placing the emphasis on the action that must be performed rather than the physical assets that perform it. This functional approach helps provide a more holistic view of the components that support our nation's most important functions and services.

The NCFs are critical to this Venture for three reasons: 1) they provide a common language for outcomes we are trying to avoid, 2) they help to provide insight into how cyber incidents impact *functionality* specifically, and 3) the decomposition of the NCFs into the components and subcomponents that support their functioning is vital in understanding the dependencies and interdependencies through which the impact of cyber incidents can cascade across systems.

LINES OF EFFORT: PUTTING IDEAS INTO ACTION

The work of the Cyber Venture will proceed along three main lines of effort: 1) Risk Architecture Development, 2) Cyber Risk Metric Identification, 3) and Mitigation of Concentrated Risk.

Risk Architecture Development

The National Critical Functions Risk Architecture will analyze relationships between the many components that make up the NCFs. This will help reveal vulnerabilities that could impact the functionality of the NCFs. The Risk Architecture will

[1] Jonathan William Welburn and Aaron Strong, "Systemic Cyber Risk and Aggregate Impacts," *Risk Analysis* (2021), accessed 15 March 2021, https://doi.org/10.1111/risa.13715.

provide the foundation to understand how likely a cyber incident is to degrade a system to the extent that it results in a loss of function and the resulting impacts in terms of core priorities such as safety, national security, community well-being, and economic competitiveness.

Cyber Risk Metric Identification

Simply stated, what can be measured can be managed. Developing usable metrics to clearly articulate cyber risk will inform decision-making and allow for cost-benefit analysis of risk mitigation solutions, driving efficient and cost-effective investment in risk reduction.

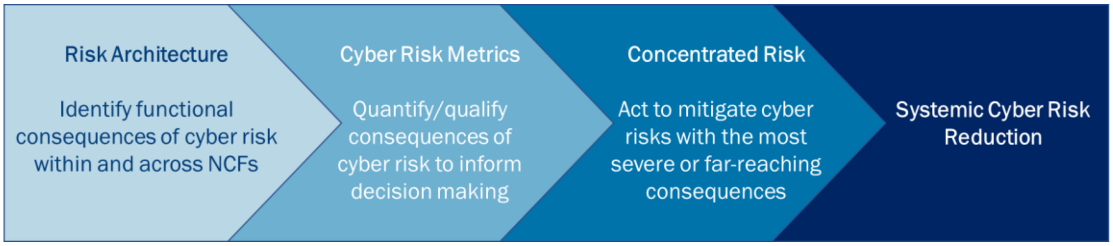
Mitigation of Concentrated Risk

Areas of concentrated risk are those risks that have potential cascading impacts across critical infrastructure because of the interdependencies and connected systems underpinning the National Critical Functions. Developing systemic solutions for these risks will provide high return on investment in terms of overall risk reduction.

A CYBER RISK MODEL

The three lines of effort together allow for a bold approach to understand and combat systemic cyber risk. The Risk Architecture breaks down the components and subcomponents that work together to provide our nation's most critical functions, illuminating the cascading consequences that could result from a cyber risk or incident. Cyber risk metrics provide a way to quantify or qualify the consequences identified by the Risk Architecture, giving policymakers a language through which risk can be measured, discussed, and compared to inform cost-effective risk management and decision-making. As these first two lines of effort identify and measure critical risk to the NCFs, areas of concentrated risk will be revealed, providing opportunities to invest in mitigation strategies that will have system-wide risk reduction impacts. Together, the lines of effort promise an approach that identifies, measures, and combats systemic cyber risks.

Figure 1. The Risk Model



Risk Architecture

Identify functional consequences of cyber risk within and across NCFs

Cyber Risk Metrics

Quantify/qualify consequences of cyber risk to inform decision making

Concentrated Risk

Act to mitigate cyber risks with the most severe or far-reaching consequences

Systemic Cyber Risk Reduction

PARTNER ENGAGEMENT: SUCCESS THROUGH COLLABORATION

The Cyber Venture will rely on expertise and advice from stakeholders across the cyber risk and critical infrastructure communities. This effort will build on existing work surrounding enterprise security ratings and cyber risk governance, and it depends on the engagement of partners across government and in the private sector for its success.

Diverse perspectives will help CISA better understand the relationships among the threats to, vulnerabilities of, and consequences on critical functions. Communities that the Venture will seek to engage include:

- Cyber Risk Innovators
- Critical Infrastructure Owners & Operators
- Risk Managers
- State & Local Cybersecurity Professionals
- Cyber Thought Leaders and more.

If you would like to learn more about ways to get involved with this Venture, please email NRMC@hq.dhs.gov.