

ISA: ANNOUNCES CISO BASED, CROSS SECTOR STUDY ON AI IN CRITICAL INFRASTRUCTURE

By Larry Clinton

Today the Internet Security Alliance (ISA) is releasing the first in a series of blog posts detailing a cross-sector assessment by critical infrastructure CISOs of the security challenges and gaps being created by AI adoption in five critical sectors.

These posts will outline the results of the first two phases in ISA's program "Defining an Effective and Sustainable Model for AI Deployment in Critical Infrastructure." Full results of phases one and two in this study will be presented in a congressional briefing on September second.

Purpose of the project

Top cybersecurity professionals from five critical infrastructure sectors – defense, financial services, healthcare, energy and IT -- were asked to analyze the cybersecurity challenges and gaps they are currently experiencing as artificial intelligence is deployed across their operating environments.

The ultimate goal of the research is to construct a CISO-experiential, AI-infused, cross-sector model that supports a cybersecurity policy approach that is both effective and economically sustainable, and that can be applied to governance in government and private industry alike.

The assessment was grounded in operational experience of Chief Information Security Officers (CISOs) from these sectors. Each participant is accountable for defending an enterprise that already runs AI at production scale. Each was asked what is failing today, which governance practices have proven insufficient, and what would have to change for security to keep pace with deployment.

Key questions analyzed in the study

Each of the five sector reviews was structured against the same four questions.

1. What are the cybersecurity policy gaps and challenges that the introduction of AI is presenting to these privately owned and operated critical infrastructures in the United States?
2. What policy initiatives need to be developed to facilitate a cybersecurity model that addresses those gaps and challenges in the AI era, and that is both effective and economically sustainable for industry and government?

3. What policy initiatives need to be implemented to address gaps and challenges within the specific infrastructure sectors identified?
4. How can industry and government best assure effective cybersecurity governance in the AI era?

Creating a policy framework for effective and sustainable policy

The project uses the Cybersecurity Social Contract as its template. That model is based on two central facts. First, the overwhelming majority of critical infrastructure in the United States is privately owned and operated. Second, market forces alone will not generate the level of security the national interest requires, because much of the threat emanates from better funded nation-state, or state affiliated actors and benefit of private security investment accrues to parties other than the investing firm.

The model therefore pairs industry commitments to demonstrated security practice with government commitments to incentives, legal certainty, and shared capability, rather than relying primarily on prescriptive mandates. The Social contract model has served as a core principle of several successful public policy efforts, including the Cyberspace Policy Review and the bipartisan, bicameral Cyberspace Solarium Commission.

AI does not change that logic. It intensifies it, because AI simultaneously accelerates the threat, expands the attack surface, concentrates dependence on a few providers, and raises the cost of adequate defense.

A social contract model which creates a more fulsome partnership between industry and government enabling a true national approach to cyber defense in the AI era, would differ from the traditional industrial age model. The current research suggests a cross-sector approach with an evolved governance structure will be more responsive to and effective in the AI environment as the same models, providers, and deployment patterns appear in all five sectors, and addressing one shared problem through five separate regulatory regimes multiplies cost without adding security.

Next: Identifying areas of convergence across the industry sectors