Preparing Governments for Future Shocks: Building Cyber Resilience for Critical Infrastructure Protection

This article is adapted from *Preparing Governments for Future Shocks: Building Cyber Resilience for Critical Infrastructure Protection* by Lisa Schlosser (Washington, D.C., IBM Center for The Business of Government, 2024).

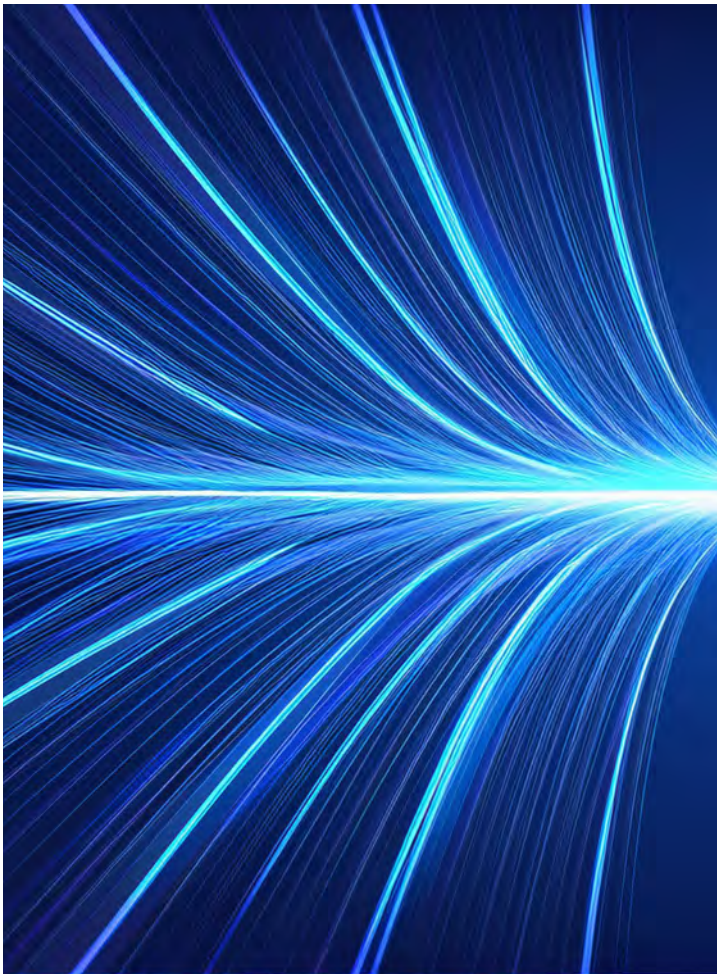
By Lisa Schlosser

Cyber resilience is crucial for protecting critical infrastructure, which includes essential services from the energy grid to clean water distribution These systems are increasingly targeted by cyberattacks Cyber resilience involves not only robust cybersecurity measures to prevent attacks but also the ability to quickly detect, respond to, and recover from incidents.

This ensures continuity of operations and minimizes the impact of cyber threats by enhancing cyber resilience, governments can safeguard critical systems, support the reliable functioning of vital services even in the face of crises, and help build and maintain public trust.

To discuss the above imperatives, the IBM Center for The Business of Government and the IBM Institute for Business Value (IBV) joined with the National Academy of Public Administration (NAPA) to convene a roundtable that identified opportunities and practical actions government can take to address these challenges. The roundtable included executives from the government, nonprofit, academic, and commercial sectors, for a highly interactive, roundtable discussion, "Preparing Governments for Future Shocks: Building Cyber Resilience for Critical Infrastructure Protection." This session addressed three areas essential to the cybersecurity and resilience of critical systems: Emergency Preparedness and Response, Supply Chain Resilience, and Workforce Resilience.

This report summarizes the discussions in this roundtable by presenting the challenges, observations and best practices, and opportunities within each of these areas. Roundtable participants identified multiple recommendations for government action, discussed in the report and highlighted in this article.



Emergency Preparedness and Response Recommendations

Promising new technologies—such as artificial intelligence (AI) and quantum computing—can provide governments with the ability to continuously improve resilience, especially in times of crises Artificial intelligence, for example, offers opportunities but introduces challenges. As AI continues to advance and become more pervasive, so do its risks—from mass disinformation campaigns and deepfakes to fully autonomous weapon systems quantum computing is also adding a new dimension of opportunity and risks. For example, quantum capabilities can help solve large-scale problems much faster such as analyzing compounds to create new drugs and optimizing global supply chains. However, with new capabilities come new risks. Nation-states will

Lisa Schlosser
Cyber Security Advisor
Harrisburg University

Lisa was the former Federal Deputy Chief Information Officer/Deputy Associate Administrator, Office of Management and Budget, under the President Obama administration. Prior to joining the government, she worked as a Senior Manager for Ernst & Young, helping to establish the international cyber security practice.

have a more powerful tool to attack critical infrastructure at scale. Also, given the power of quantum computing, current encryption solutions may be less difficult to crack.

Three recent incidents underscore the need to understand and address these and other risks and impacts, by enhancing preparedness, response, and resilience to sustain critical infra structure operations

- First, the actions taken by the People's Republic of China (PRC) state-sponsored cyber group known as Volt Typhoon have shown how nation-state actors can infiltrate various critical infrastructure domains to gain a foothold for future attacks.
- Second, the Colonial Pipeline ransomware attack caused a critical infrastructure provider to shut down its pipeline system.
- Third, and more recently, a widespread outage, due to a faulty software update from CrowdStrike, led to substantial disruptions across numerous critical infrastructures domains, including airlines, hospitals, banks, and millions of other businesses.

These incidents highlighted many risks to our critical infrastructure.

Participants in the roundtable identified the following emergency preparedness and response recommendations to support the NCS strategy and to ensure readiness to address most effectively these risks.

- Implement National Security Memorandum on Critical Infrastructure Security and Resilience (NSM 22), and the Cyber Response and Recovery Funding (CRRF) Act to align aspirations and resources.
- Continue to look at ways to optimize/streamline/create economies of scale, and created tiered governance structures for ISACs.
- Develop and communicate incentives and resources to help SMBs prioritize cybersecurity.
- Establish response and resilience frameworks that address the physical/cyber nexus and test.
- Consider the inclusion of space systems as a critical infrastructure domain.

Supply Chain Resilience Recommendations

Shocks to supply chains over the past few years continue to reverberate. Whether a supply chain focuses on efficiency and resiliency or on data-led insights and innovations for the future, addressing supply chain challenges involves balancing priorities and navigating the complex ecosystem of modern, global supply chains.

Governments face unique supply chain challenges. They enable commercial supply chains by providing critical infrastructure and security, and oversee massive public-sector networks. However, these escalating supply chain challenges require increased digital transformation and innovation. Both the public and private sectors, nationally and internationally, have encountered challenges in building actionable resilience solutions into supply chains.

The federal government is addressing supply chain in many other ways. On November 27, 2023, the Supply Chain Resilience Center (SCRC) at the Department of Homeland Security was created to protect the supply chain from evolving threats. The SCRC examines security of U.S. port infrastructure and provides recommendations to private sector stakeholders. The SCRC will also analyze vulnerabilities and conduct scenario planning with private sector stakeholders to help mitigate supply chain disruptions, ensure reliable and efficient deliveries of goods and services, and lower costs for the American people.

The participants in the roundtable identified the following recommendations that can help advance supply chain resilience.

- Establish center of excellence for procuring prioritized commodities including technology, electronics and microchips.
- Create formal partnerships and collaboration tools to share, track and visualize supply chain information and risk management across domains such as an SCM control tower.
- Shift to best value vs low-cost procurement models to improve supply chain readiness.
- Use AI to drive real-time tracking, suggested solution and resource maximization.
- Drive policy to delegate the required ATO risk attestations to third-party support.

Workforce Resilience Recommendations

Amidst rapid technological changes and unprecedented industry disruptions, there is a growing disparity between the skills required in the workforce and the professionals who have obtained those skills. Public agencies will need to be able to recruit, retain, and develop a professional workforce who can successfully address emerging critical infrastructure issues now and into the future. Consequently, cybersecurity workforce resilience has evolved as an ongoing challenge, one that requires continuous improvements to address increasing threats to the critical infrastructure. Government faces several workforce resilience challenges:

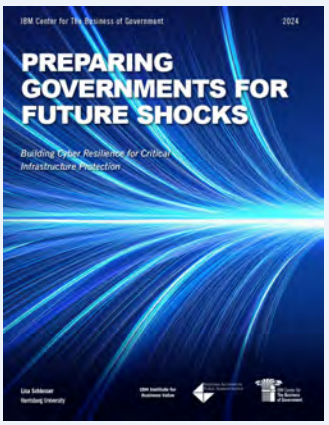
- Huge pay gap exists between the public and private sectors. The long lead time to hire qualified cybersecurity professionals in government compounds this problem, as does the difficulty of matching needs with openings on a nationwide scale—due to the lack of a national database, or a system to identify cybersecurity professionals across geographical boundaries.
- Lack of consistency in academic programs where many institutions do not expose graduates to real-world, hands-on cybersecurity education
- Remote work often diminished coherence and collaboration; consequently, many organizations have moved to reduce remote work.

A consistent theme highlighted in the roundtable is that the government should capitalize on proven models of coordination between the public and private sectors. Roundtable participants also noted that the Office of Personnel Management (OPM) and other agencies need to update cybersecurity classification codes. The updates would define which positions require a college degree, and which do not. Additionally, updated classification codes would help to address cybersecurity jobs needed in the future, even in light of the emergence of AI.

Continued emphasis on employee engagement is also critical for retention of cybersecurity professionals. Employees need to be engaged as organizations determine the appropriate role of AI. Visibility into a career path and promotions should be a priority for employers. Employers must also continue to optimize opportunities for remote work and work-life balance. Roundtable participants also discussed the opportunity to develop a national database of cybersecurity professionals to help to identify and hire qualified individuals more rapidly.

The participants in the roundtable identified the following recommendations to ensure readiness that address more effectively workforce resilience.

- Use AI to improve the hiring process.
- Enhance coordination between the public and private sectors by using proven models.
- Improve cybersecurity classification codes and hiring processes.
- Focus on employee engagement to support retention.
- Create national database of cybersecurity professionals.
- Create role-based cyber education models for disciplines within the organization beyond technical practitioner roles.



Preparing Governments for Future Shocks: Building Cyber Resilience for Critical Infrastructure Protection

by Lisa Schlosser

Available at:
businessofgovernment.org

