Preparing Governments for Future Shocks

Workforce Resilience Roundtable: Read Ahead Materials

Introduction to the Future Shocks Initiative

Government leaders increasingly indicate that what were previously viewed as Black Swan events are now becoming more frequent — and more destabilizing — shocks. The past three years saw acceleration toward a connected world where physical goods and digital services are increasingly interdependent. The vulnerability of social and economic well-being is laid bare by reliance on connectivity and distributed value chains subject to disruption on multiple fronts.

Risks have grown due to complex variables such as geopolitical conflicts, multiple public health emergencies, energy crises, climate-related natural disasters (wildfires, hurricanes, drought), the breakdown of longstanding trade relationships, economic displacement, and economic inequality. The combination of these factors renders current planning models obsolete.

Citizens, non-governmental organizations, and commercial enterprises continue to rely on governments to help manage these uncertainties -- traditional incident response frameworks may no longer be sufficient, as events occur across multiple domains, jurisdictions, and decision-making authorities. Rather, collaborative action to address anticipated threats requires focus and cooperation across a broad ecosystem of partners and stakeholders. Governments must prepare for "future shocks" by supporting stakeholders with insights, resources, innovation, and adaptation that characterizes asuccessful response to any high-impact event.

IBM, working through the IBM Center for The Business of Government and the IBM Institute for Business Value, and in partnership with the National Academy of Public Administration (the Academy), has launched an initiative to help government identify core capabilities critical to building such resilience, and make progress toward addressing major national and international priorities including the Grand Challenges in Public Administration put forth by the Academy.

We are convening a series of international roundtable discussions with global leaders from across the public, private, academic, and non-profit sectors to capture lessons across six key domain areas: Emergency Preparedness and Response, Cybersecurity, Supply Chain, Sustainability, Workforce, and International Cooperation. In each domain, we will harvest insights from the roundtables to identify strategies and solutions for governments to act. Previous roundtables convened leaders in emergency management, cybersecurity, supply chains, and sustainability for insightful discussions of actionable, and practical steps to build resilience to future shocks. Learn more about the initiative by reading the blog, 'Preparing Governments for Future Shocks' or listening to the podcast with Michael J. Keegan, IBM Center for The Business of Government.

Workforce Resilience Roundtable Agenda -- Monday June 26th

9:00 - 9:30 am	**Coffee and Networking**
9:30 – 10:00 am	**Host Welcome and Introductions** • Cristina Caballe Fuguet Senior Partner & Vice President, Global Public Sector, IBM • Dan Chenok Executive Director, IBM Center for The Business of Government • Terry Gerton President and CEO National Academy of Public Administration
10:00 – 10:30 am	**Discussion** • What are key challenges and opportunities to attract and retain talent with skills essential to building a resilient and capable government workforce, considering challenges that include increased cyber threats and climate change?
10:30 – 11:00 am	**Remarks** • Kiran Ahuja Director, United States Office of Personnel Management
11:00 - 11:55 am	**Discussion, Continued** • How can government empower a workforce that can improve productivity by using emerging technologies, such as automation and generative AI? What obstacles exist with enabling such technologies? • What specific actions can governments take to help reskill workers to address evolving needs?
11:55 am – 12:00 pm	**Roundtable summary and next steps for the initiative**

Future Shocks – Workforce Resilience Roundtable Discussion

To address shocks and challenges, public agencies may need their workforce to have different knowledge, skills, and abilities than they have traditionally required. 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 these issues now and into the future, especially in critical areas like emergency preparedness and response, cybersecurity, supply chain, and transition to a cleaner environment.

This roundtable discussion will serve as a strategic framing event for a virtual workforce resilience roundtable hosted by the National Academy of Public Administration on Wednesday, June 28. The in-person roundtable in which you will be participating on June 26 will identify key findings and insights, and results from the roundtable will be discussed at the companion event.

Workforce Resilience – Summary of Highlights from Research

With an increase in the frequency of more challenging future shocks – which can include natural and human-made disasters, cybersecurity crises, and climate events, and more -- there has never been a greater need for a skilled public sector workforce. At the same time, governments increasingly utilize emerging technology to improve performance. Therefore, it is vital for many prospective employees to have expertise in using technological tools. For example, advanced robotics and artificial intelligence (AI) are being used to automate early warning systems, environmental monitoring, and cybersecurity threats. In addition, workers will need to leverage cloud computing and big data which will enable real-time data analysis to improve situational awareness.

The future workforce will also require excellent skills in a variety of analysis, decisionmaking, and communication in various media, including social media platforms. In addition, government entities need to hire more employees with skill sets in identifying and mitigating threats to physical and IT systems. Government entities are also in need of employees with expertise in risk management and research and development on new innovation, as well as diverse skills from varied professional backgrounds ranging from engineering to modeling to telecommunications.

More detail on workforce needs in the three areas of focus for the virtual session follows.

Clean Energy Transition

The detrimental effects of climate change are only growing, with more frequent and deadly storms and dangerously rising temperatures. To address this crisis, we need people reskilled and trained now to make the transition to a cleaner environment and reduce our negative impact on the globe. According to the United Nations Environment Programme, farming, architecture, science, and teaching are sectors that will need employees who can utilize new green skills. Recent reports show that four in 10 workers will need to be reskilled in order to keep up with the demand of new industries. According to the World Economic Forum's Davos Labs Youth Recovery Plan 2021, almost half of young people feel they do not have the proper skills to guarantee them a dignified job in the next five to 10 years. This signifies a need for training and reskilling opportunities that will connect this workforce with an industry that needs it.

The transition to a cleaner environment will require a diverse set of skills from varied professional backgrounds. Core engineering skills – mechanical, electrical, chemical – will always be in demand within the energy sector. However, those pursuing work in the renewable energy field will need more modeling, software, digital, electronics, and telecommunication skills. The green economy will call for workers who can design, operate, and monitor a wide range of systems.

Emergency Preparedness and Response

With an increase in the frequency of more challenging natural and human-made disasters, including cyberattacks, there has never been a greater need for trained emergency management professionals. As a result, we are witnessing a vast expansion of emergency management roles across departments that did not have them previously. Unfortunately, many current emergency management professionals are burnt out after handling a slew of record-breaking disasters back-to-back. Therefore, it is imperative that we build capacity to ensure these roles are being filled.

Governments and private companies increasingly utilize emerging technology to improve disaster detection, prevention, and response. Therefore, it is vital for many prospective employees to have expertise in these technological tools. For example, advanced robotics and artificial intelligence (AI) are being used to automate early warning systems and forecasting. In addition, workers will need to leverage cloud computing and big data which will enable real-time data analysis to improve situational awareness. This field will also require excellent communication skills in various media, including social media platforms.

Cybersecurity

It is no surprise that cyberthreats against the public sector are on the rise, with 58% of state and local government organizations experiencing ransomware attacks in 2021 – a 70% increase from the previous year. Furthermore, 59% of organizations reported an increase in attack volume and complexity over the last year, and 56% reported an increase in the impact of attacks. Yet, most government entities remain woefully unprepared to defend themselves against such attacks. To make matters worse, cybercriminals are constantly innovating, making it difficult for governments to stay protected. In addition, government agencies are the owners and users of highly sensitive data. Yet, shrinking IT budgets, a skills shortage, cloud adoption, and reliance on a wide network of contractors and third-party vendors widen the attack surface. It is imperative that these organizations step up their efforts to mitigate cyber events.

A plethora of skills are needed in the cybersecurity workforce. For example, government entities need to hire more employees to identify and mitigate threats to internal IT systems and networks. For this role, employees should have skills in cyber defense analysis, cyber defense infrastructure support, incident response, and vulnerability assessment and management. Government entities are also in need of employees who can build safer and more secure IT systems, which requires expertise in risk management, software development, systems architecture, and technology R&D.

Key Reports on Workforce for Reference

NAPA Fellows Daniel Chenok and Donald Kettl published The Federal Workplace Is Changing Rapidly, But Merit Principles Must Remain Untouched as the second in a five-part series from the National Academy of Public Administration looking at the challenges and urgency of modernizing the civil service.

The White House report "The Impact of Artificial Intelligence on the Future of Workforces in the European Union and the United States of America" highlights important themes and aspects for consideration in relation to the economics of AI in a balanced manner. Through collaboration between the EC and Council of Economic Advisors (CEA) on this work, the report aims to synthesize the perspectives of the US and the EU, with a focus on implications relevant to policymakers.

The World Economic Forum's article "Here's how companies should navigate generative AI in the world of work" focuses on the rapid ascent of OpenAI's GPT-3 and what this, and the advances of generative AI, means for the future of work. The article provides an outline for navigating the next of work, discussing the strength of generative AI and how that can work collaboratively with the work of human experts.

IBM's Institute for Business Value (IBV) report "The enterprise guide to closing the skills gap" outlines three strategies to help organizations tackle building and maintaining a skilled workforce through leveraging AI in assisting organizations to close skills-related gaps. Additionally, the IBM IBV report "Three keys to competitiveness in an era of economic uncertainty" provides data and insight into how public and private sector leaders can work together to foster national and regional economic competitiveness in an era of uncertainty.

The "Reskilling the Workforce with Technology-Oriented Training" report published by the IBM Center for The Business of Government discusses that as agencies engage in digital transformations, the need for the workforce to transform grows by reskilling to maintain and effectively use new technology. Additionally, the IBM Center for The Business of Government report "Leveraging Data for Racial Equity in Workforce Opportunity" provides insight for government leaders and their stakeholders in designing effective strategies and programs that promote more equitable workforce opportunities across the government.

The OECD report "Artificial Intelligence and Employment" discusses concerns around the adoption of AI in the workplace, positioning that AI might increase disparities between workers who have the skills to use AI effectively and those who do not – highlighting the need to skill workers appropriately.

Key Reports on Emergency Management, Cybersecurity, and Sustainability

IBM's Institute for Business Value (IBV) report 2022 CEO Study – Own your impact: Practical pathways to transformational sustainability reveals sustainability's dramatic emergence onto the mainstream corporate agenda – and the need to act. Additionally, the IBM IBV report Sustainability as a transformation catalyst examines a group of leaders known as the Transformation Trailblazers that have acted on their sustainability strategy, outpacing the competition in both revenue growth and sustainability outcomes, and identifies 6 primary areas they stand out.

The Department of Homeland Security and FEMA issued the National Preparedness Report discussing the need for the emergency management community to continue to have agile policies to address emerging risks in complex operating environments and the ability to continue to operate when normal operations are disrupted. The FEMA report, Lessons Learned from FEMA's Initial Response to COVID-19, examines the response to the COVID-19 pandemic and provides recommendations to improve current and future response operations.

The National Academy of Public Administration also recently published A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Future. This congressionally mandated study for CISA examined the government-wide cybersecurity workforce development strategy and CISA's strategy for developing the nation's cybersecurity workforce and its partnership models. The report found that CISA and other agencies have made progress on individual cybersecurity workforce development programs; however, the absence of a government-wide cybersecurity workforce development strategy and lack of clarity about federal agency roles and responsibilities has hindered the federal government's ability to tap the capabilities and resources in the private sector, academia, and other levels of government. The report offers recommendations related to this government-wide strategy and the governance structure required.

Sources used in Highlights from Research

- World Economic Forum's Davos Lab Youth Recovery Plan 2021.pdf (weforum.org)
- Top three skills needed for a career in green and clean energy - RMIT University
- Green your career – get these skills, says UN | World Economic Forum (weforum.org)
- Top 10 Emergency Management Trends & Innovations in 2023 (startus-insights.com)
- Cybersecurity Guide: Securing Government Agencies – Sophos News
- A D for NASA, a C for HUD: Senate report warns agencies unprepared for cyberattacks (nbcnews.com)
- Workforce Framework for Cybersecurity (NICE Framework) | NICCS (cisa.gov)