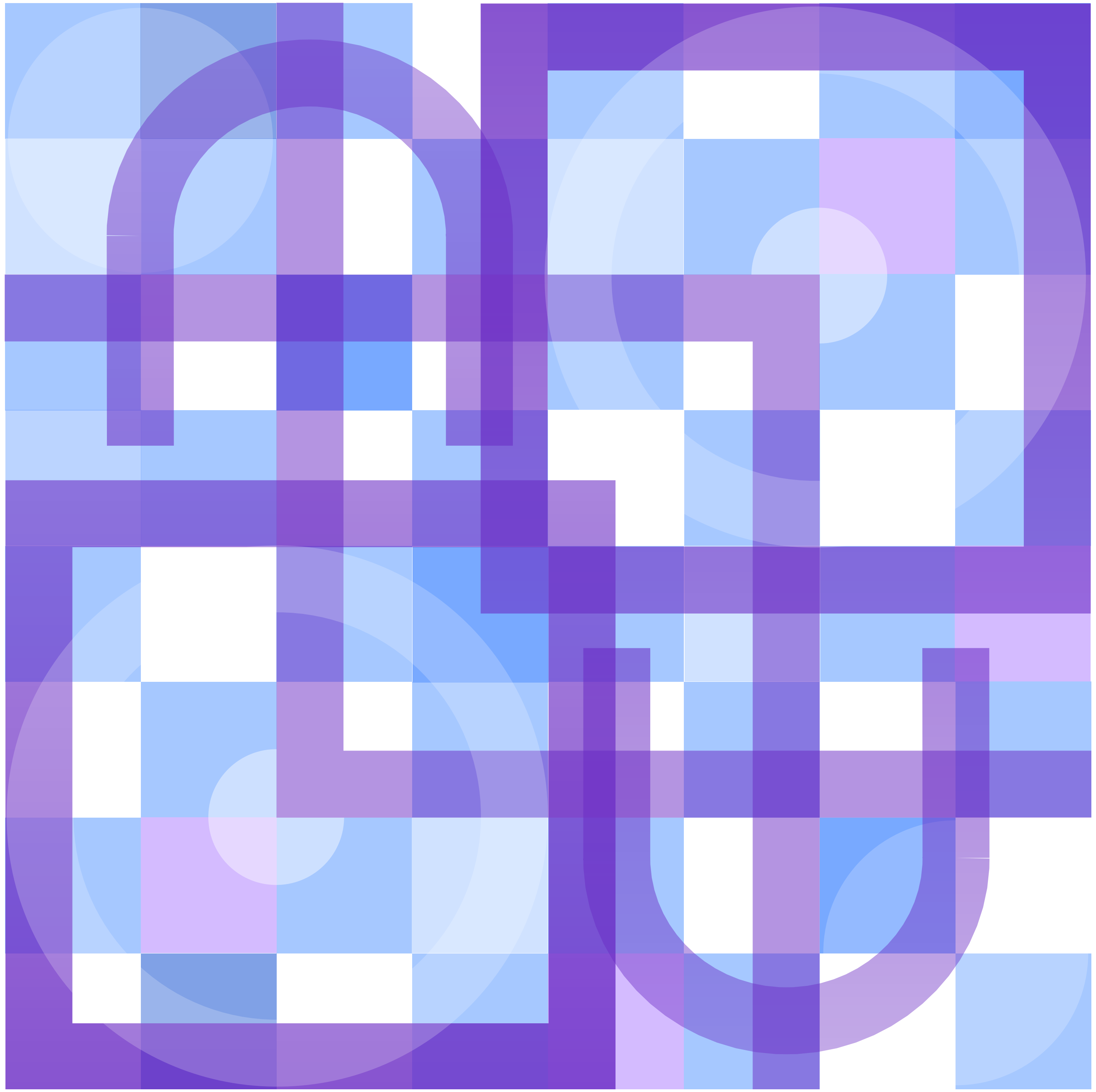
IBM Institute for Business Value | Research Brief

Preparing governments for future shocks

An action plan to build cyber resilience in a world of uncertainty



In collaboration with

National Academy of Public Administration®

IBM Center for The Business of Government

CENTRO STUDI AMERICANI

IBM

Introduction

> *"We help government leaders build resilience against future adversity by identifying and protecting their crown jewels and vital systems. By simulating cyberattack scenarios, we can show them what a really bad day looks like."*
>
> **Cristina Caballe Fuguet**, Vice President, Global Public Sector, IBM

Since the advent of the internet, criminal groups, hacktivists, and state-sponsored threat actors have put governments in the crosshairs of cybercrime. During the last half of 2022, the number of cyberattacks targeting governments increased by 95% worldwide, compared to the same period in 2021.[1] The cost of public sector data breaches also increased 7.25% between March 2021 and March 2022, with an average cost per incident of $2.07 million.[2]

Government digital platforms—and the sensitive information they store—represent target-rich environments. Economic globalization and digital interconnection of nearly every aspect of commercial and government activity have created an intricate digital ecosystem. Cyberspace has reshaped physical borders and governance models, and global networks mean that the impacts of threats and incidents can quickly escalate in magnitude and breadth if not addressed with speed and effectiveness.

In recognition of today's complex cyber threat environment, and the government's responsibility to secure a safe and secure digital ecosystem, the White House announced a comprehensive National Cybersecurity Strategy in March 2023. This strategy sets a path to make cyber defense easier and more cost-effective. It also focuses on reducing the impact of cyber incidents through resiliency and aligning efforts with national values to secure the promise of a digital future.

Over the last year, two roundtable events were hosted by the IBM Institute for Business Value (IBV) and the IBM Center for The Business of Government in collaboration with the National Academy of Public Administration and the Center for American Studies. Held in Washington, DC, and Rome, Italy, these events featured in-depth discussions about cyber resiliency and government leadership. Findings from these roundtables could help the US, Italy, and governments around the world develop and implement cybersecurity strategies that promote resilience through public-private partnerships.

After wide-ranging discussions, attendees outlined a series of actionable steps designed to help governments emerge stronger from current and future cyber shocks.

About the author

Tony Scott
President and CEO, Intrusion, Inc.

Prior to becoming CEO of Intrusion, Inc., a provider of security software solutions, Tony founded the TonyScottGroup, a Washington, DC- and Silicon Valley-based consulting and venture capital firm focused on cybersecurity and privacy technologies. He has also held senior executive positions in government and business organizations.

During the Obama administration, Tony served as Federal Chief Information Officer, with oversight, budget, and management responsibilities for the more than $85 billion the Federal Government spends annually on IT.

Tony has also served as CIO of Microsoft, CIO of the Walt Disney Company, and CTO of General Motors. He was inducted into CIO Magazine's "CIO Hall of Fame;" is a multi-year recipient of the Fed 100 Award; and has been a frequent keynote speaker, panelist, and advisor at numerous industry and government events.

Representatives from sponsor organizations

Dan Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com
linkedin.com/in/chenokdan/

Dave Zaharchuk
Research Director
IBM Institute for Business Value
David.zaharchuk@us.ibm.com
linkedin.com/in/david-zaharchuk-59564519/

Terry Gerton
President and CEO
National Academy of Public Administration
tgerton@napawash.org
linkedin.com/in/terry-gerton-b43aa73a/

Step #1:

Increase the cyber talent resource base

To address the rapidly growing gap between supply and demand for cybersecurity professionals, roundtable participants stressed the importance of increasing the cyber talent resource base and putting it at the top of the list of actionable priorities.

Key takeaway

- Ensuring that governmental organizations can meet the cybersecurity staffing challenge will require a multi-pronged effort and new thinking to recruit talent from a wider population.

To address the rapidly growing gap between supply and demand for cybersecurity professionals, roundtable participants stressed the importance of increasing the cyber talent resource base and putting it at the top of the list of actionable priorities. As noted by several participants, cyber skill shortfalls impact a broad set of disciplines including analysis and engineering, software development, threat intelligence, penetration testing, auditing and consulting, digital forensics, and cryptography.

One participant referred to systemic science, technology, engineering, and math (STEM) education issues in the US and observed, “We’re drawing a small pool from a small pool. The challenge of finding STEM-educated American citizens able to obtain security clearances is like searching for unicorns.”

Another participant pointed out that worldwide, the cybersecurity workforce deficit is approximately 3.5 million people. She also noted how the competition for talent is driving up salaries, making it more difficult for many organizations to meet staffing requirements.[3] Because many private sector employers offer higher compensation for cybersecurity positions, governments are often at a disadvantage when recruiting for analysts, responders, security architects, developers, managers, and other roles also in demand by private sector employers.

While massive digitization remakes economic sectors, digital technology is also transforming how services are designed and delivered. Consequently, cyber disruptions are becoming more common and further reaching, putting even more pressure on government-based cybersecurity resources.

Participants suggested a wide range of options to develop the cyber talent pipeline feeding government, including:

- Waive the requirement of a four-year college degree for some skilled areas.
- Include cyber education early in K-12 curricula.
- Tighten the focus on reskilling people already in the workforce.
- Develop multidisciplinary programs, such as cyber plus business and cyber plus medical.
- Expand cybersecurity apprenticeship programs.
- Increase the number of women in STEM educational programs—and cyber education in particular—by making these fields more attractive for women, who currently comprise only 24% of the cyber workforce.[4]
- Reinforce workforce actions at the state and local level and in the business community, where decisions can impact workforce outcomes.
- Leverage the supply of military veterans with cyber skills and develop more veteran training programs that focus on cyber skills.
- Re-examine selected high barriers to entry into cyber careers, such as mandatory security clearances and required baseline skill sets.
- Strengthen the cybersecurity workforce by promoting diversity, equity, inclusion, and accessibility.
- Create an inclusive workplace culture to attract those who may not conform to a traditional security-focused mission.

In addition to these observations, the National Academy of Public Administration recently released a report about the government’s role in building a cybersecurity workforce. This call to action can be accessed here: https://napawash.org/academy-studies/dhs-cybersecurity-workforce.

Step #2:

Improve organizational collaboration for faster response

Participants agreed that collaboration and information sharing between national and international governmental organizations—as well as between government and business stakeholders—is complex and slow moving.

Key takeaway

- In response to threat actors quickly adapting new technologies to penetrate networks and thwart countermeasures, governments must increase collaboration and expedite information sharing to stay a step ahead.

Despite recent progress in improving public-private coordination,[5] increased cooperation between cyber attackers continues to be an ongoing threat. Threat actors are developing and promoting criminal infrastructures and services that hostile governments and gangs can use for illegitimate purposes.

Bad actors are also adopting new technologies quickly to penetrate networks and thwart efforts to contain threats, which can be difficult to counter when those efforts depend on coordination across entities with differing standards, missions, and priorities. Coordination and collaboration are key themes in the National Cybersecurity Strategy paper released by the White House in March 2023. This strategy stresses partnerships between civil society and industry and boosts collaboration with allies to strengthen norms of responsible state behavior, hold countries accountable for irresponsible behavior, and disrupt criminal networks behind cyberattacks.

Participants noted a lack of transparency regarding the many interdependencies, complexities, and related risks of digitally connected services. As a result, the public often has difficulty understanding the fragility of systems and the cascading effects associated with service disruption, including the impacts on downstream suppliers and partners.

Examples of such interdependencies include open-source software, supply chains, and critical infrastructures that increasingly rely on technology services for operations, fulfillment, and platform security. Participants recognized that emerging ecosystems concentrated on coordinated economic activities need to be more aware of their shared responsibility for cybersecurity and resilience.

Methods to improve collaboration suggested by the participants include:

- Focus on broad, policy-driven cybersecurity initiatives to establish baselines for critical infrastructure and close gaps in regulatory frameworks.
- Strengthen law enforcement capabilities.
- Prioritize standard cyber risk assessment frameworks to facilitate more efficient collaboration.
- Accelerate feedback loops and improve sensor capabilities to correct for over- and under-estimates of cyber risk.
- Conduct cyber incident response training to coordinate operational support across ecosystem partners and use drill exercises to improve resiliency across public and private sectors.
- Share cyber expertise and costs across agencies involved with digital operations and service provision, and support agencies not equipped to provide for their own security from common government or commercial centers of cyber excellence.
- Take advantage of shared cyber services more broadly, and secure cloud services in particular, along the lines of the US Department of Homeland Security Cyber Safety Review Board.[6]
- Encourage proactive investment to prepare for threats coming from advances in AI and quantum computing technologies.
- Use AI and automation technologies to strengthen cyberdefenses more broadly and counter the use of these technologies by cyber adversaries and threat actors.

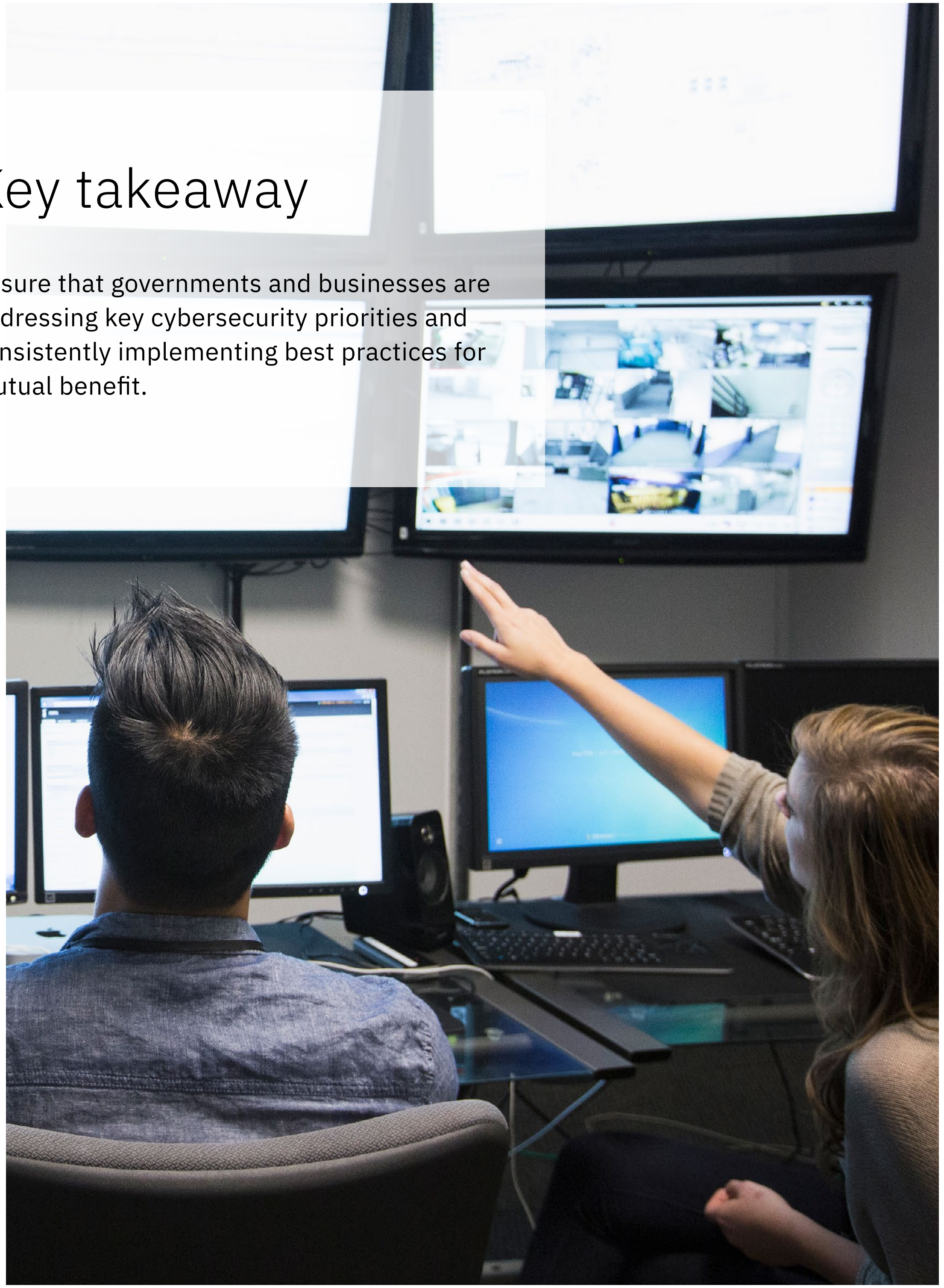
Step #3:

Align public and private sector cybersecurity priorities

By identifying common challenges, sharing best practices, and exploring avenues for cooperation, participants highlighted numerous ideas for industry and government cooperation to improve cybersecurity on a broad scale.

High-priority opportunities for alignment include:

- Emphasize recruiting from a wider array of backgrounds for the cyber workforce.
- Sharpen focus on security innovation as a competitive advantage.
- Support zero-trust frameworks that assume network security is always at risk to internal and external threats.
- Institutionalize continuous and pervasive cyber education from “K through Gray.”
- Improve understanding of cyber issues among elected officials and their support staffs, as well as key government decision-makers.
- Improve cybersecurity expectations, standards, metrics, and data to strengthen understanding of threats, and the need for public and private investment to counteract and contain the threats.



Key takeaway

- Ensure that governments and businesses are addressing key cybersecurity priorities and consistently implementing best practices for mutual benefit.

Step #4:

Study ways to bolster democratic institutions against cyberattacks

Roundtable speakers expressed concerns about how cyber warfare actors target the functions of democratic states and institutions through misinformation and disinformation campaigns.

These attacks are designed to influence public support and involvement in electoral, legislative, or regulatory processes and include attempts to steer public opinion or undermine democratic norms of behavior.

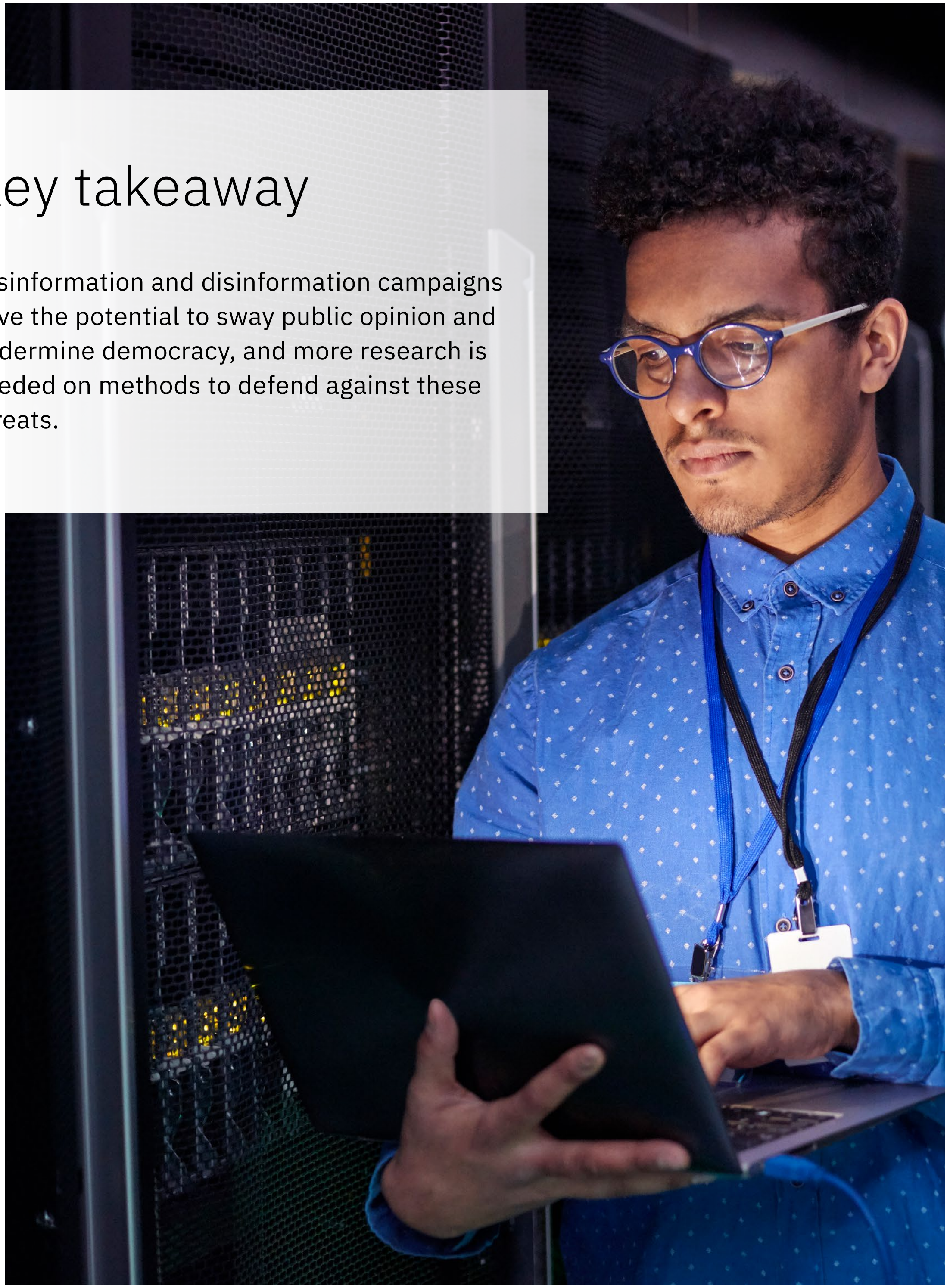
While the primary objective of these overt or covert campaigns is to sow confusion and promote social discord in the near-term, participants recognized that longer-term efforts could succeed in swaying public opinion. Due to the complexities represented by these cyber challenges to representative forms of government, participants did not reach a broad consensus on the most effective ways to defend against this growing threat and called for more research into measures that can counter cyber threats to democracy.

Among the concerns expressed were:

- State-backed efforts to shape public opinion through the broad suppression of public information available on media platforms. Participants shared the examples of China, Russia, and other authoritarian regimes that engage in search engine restrictions and strict censorship policies.
- Consumer behavior information collected by popular mobile social media applications, such as TikTok.
- The potential for highly automated and effective disinformation campaigns in more open democracies presents asymmetric threats that are difficult to identify and counter. Attendees agreed that this topic requires more in-depth research to understand the implications in terms of cyber risk, threats, and resiliency.

Key takeaway

- Misinformation and disinformation campaigns have the potential to sway public opinion and undermine democracy, and more research is needed on methods to defend against these threats.



Conclusion

Build cyber resilience leaders for future readiness

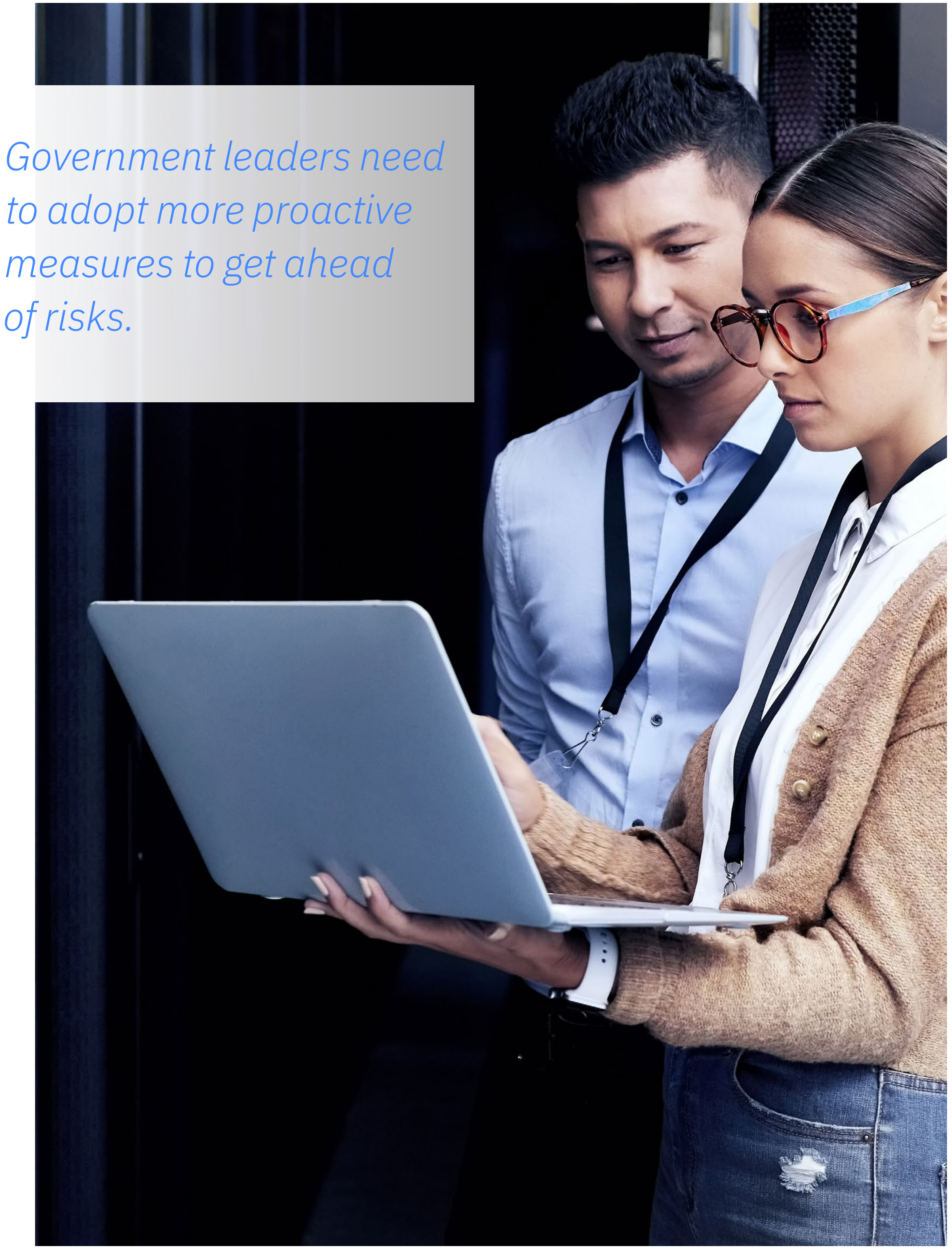
Just as prior waves of dramatic technology innovation have impacted our society and our common welfare, today's massive digitization has wide-ranging implications.

Global reliance on open technology underscores what makes communities prosper—notably social connectivity, communications, and collaboration. These factors drive national and international well-being; at the same time, reliance on digital interactions makes them prime targets for cybercriminals.

Current safeguards work some of the time but fall short in too many cases. Government leaders need to adopt more proactive measures to get ahead of risks. While technology shapes the consumption of information and the platforms used for social discourse, the growing sophistication of cyber threats impacts public and private sector stakeholders around the world.

Governments have a vital role in working with key stakeholders to identify cyber risks. This starts with building response capacity and resilience in the face of these risks. But government officials need to go further—executing leadership agendas that drive change toward a more resilient future, while also reflecting the unique identity and sense of purpose that defines each government in the eyes of their constituents.

Government leaders need to adopt more proactive measures to get ahead of risks.



Roundtable at the Center for American Studies in Rome, Italy

To add an international perspective to the Washington, D.C. event, a cybersecurity roundtable was hosted by the Center for American Studies in Rome, Italy. Experts from across Europe discussed and developed more insights on many of the action items introduced in Washington.

With Rome's proximity to the war in Ukraine, much of the cybersecurity discussion focused on defense and mutual security assistance. Participants emphasized that cybersecurity is an ecosystem issue in Europe. To be successful, agencies and governments must support cyber cooperation at a high level and eliminate boundaries as much as possible.

Participants recognized that strengthening cybersecurity supports technological sovereignty and protects critical infrastructure, supply chains, health data, space/satellite security, and other systems. These priorities were reflected in The National Cybersecurity Strategy report released by the National Cybersecurity Agency in Italy, which aims to make the country safer and more resilient.

Rome roundtable participants

Major General Luciano Antoci
CIS Division Chief
Italian Army General Staff

Lorenzo Benigni
Senior Vice President, Governmental and Institutional Relations
Elettronica SpA

Stefano Bonifazi
Direttore BU Difesa, Spazio e Sicurezza dello Stato
BV-Tech

Cristina Caballe Fuguet
Vice President, Global Public Sector, IBM

Cristiano Cannarsa
Chief Executive Officer, CONSIP

Marco Carlini
Partner, Public Sector, IBM Italy

Dan Chenok
Executive Director
IBM Center for The Business of Government

Riccardo Croce
Vice Questore Aggiunto, Responsabile del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
Polizia Postale e delle Comunicazioni

Gennaro Faella
SVP Strategic Innovation & Development
Leonardo Cyber & Security Solutions

Luca Frusone
Presidente della Delegazione parlamentare italiana presso l'Assemblea parlamentare della NATO

Ivano Gabrielli
Direttore Servizio Polizia Postale
Polizia di Stato

Sara Marini
Manager of Government and Regulatory Affairs, IBM Italy

Roberto Menotti
Editor-in-Chief of Aspenia online, Deputy Editor of Aspenia print edition and Senior Advisor - International Activities
Aspen Institute Italia

Julian Meyrick
Senior Partner and Vice President,
Security Strategy Risk & Compliance, IBM

Karim Mezran
Resident Senior Fellow, Rafik Hariri Center for the Middle East
Atlantic Council

Alessandro Picardi
Presidente Esecutivo, Olivetti

Enrico Prati
Professor, Università degli Studi di Milano

Alessandra Santacroce,
Director, Government and Regulatory Affairs, IBM Italy

Lieutenant General Sergio Antonio Scalese
Commander, Cyberspace Operations Command
Italian Air Force

Daniela Scaramuccia
Lead Client Partner, Public Sector, IBM Italy

Paolo Sironi
Global Research Leader, Banking and Finance
IBM Institute for Business Value

Mike Stone
Managing Partner, Global Government, IBM

Francesco Stronati
Managing Director, Health & Public, IBM Italy

Francesco Teodonno
Security Brand Leader, IBM Italy

Shue-Jane Thompson
Managing Partner, Global Deal Leader, Strategic Sales, IBM

Afterword

A global pandemic. A major war in Europe. Historic floods in Pakistan, California, and Australia. Dangerous heat waves in China. As these and other far-reaching events demonstrate, "future shocks" aren't future phenomena. They are happening now.

To help government leaders identify core capabilities critical for resilience in the face of future shocks, IBM has launched an initiative through the IBM Center for The Business of Government and the IBM Institute for Business Value, in partnership with the National Academy for Public Administration.

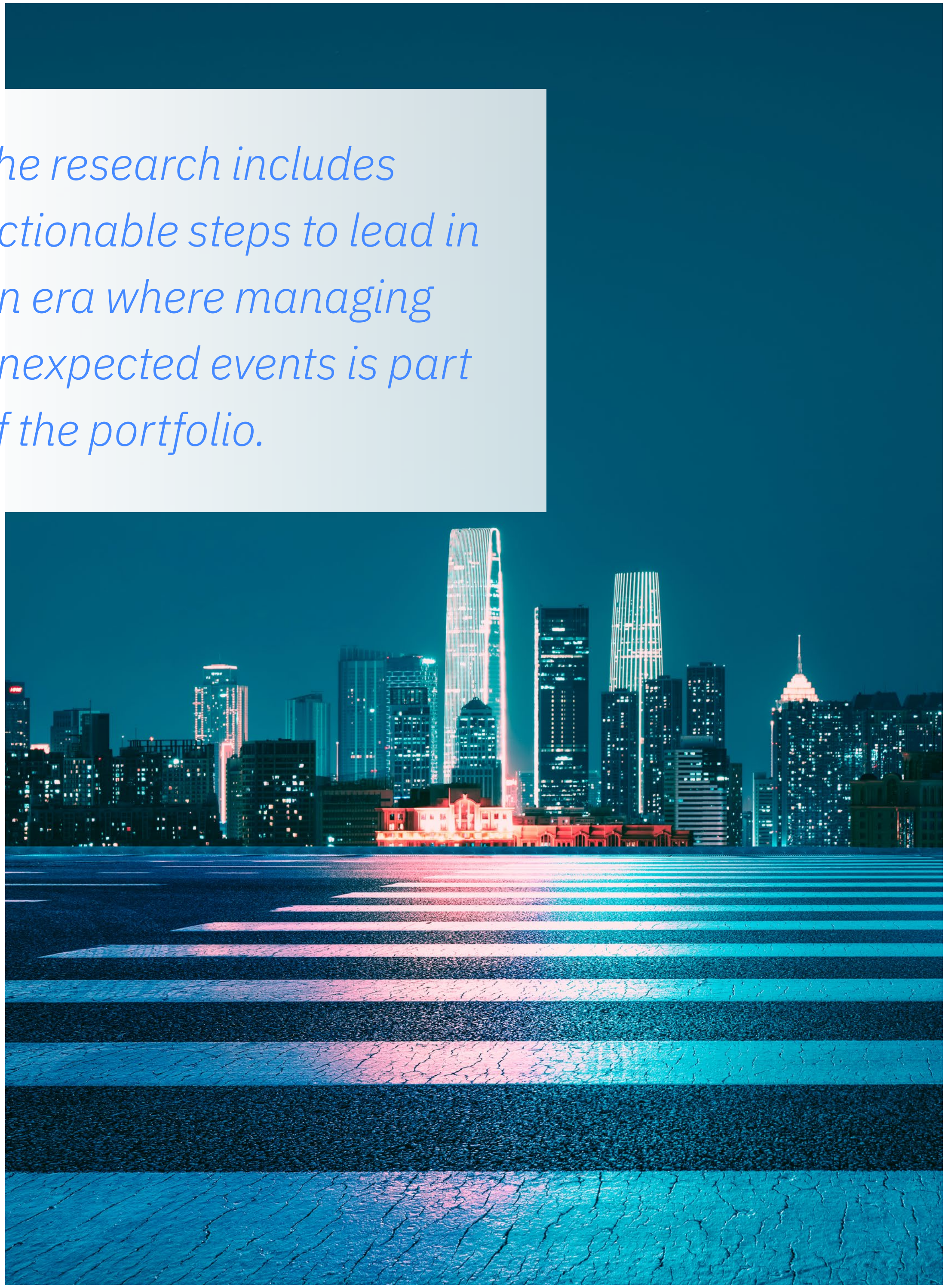
This initiative identifies six key domain areas where government leaders need to prepare for future shocks. To discuss and develop plans of action, we are convening a series of international roundtable discussions with global leaders from public, private, academic, and other sectors.

In 2022, the first roundtable event in this series was held in Washington, D.C., focusing on emergency preparedness and response. A research brief, "Partnering for Resilience: A practical approach to emergency preparedness." was published and includes pragmatic and actionable steps to lead in an era where managing unexpected events is now part of the portfolio.

Cybersecurity, the domain area of this brief, was the focus of the second series of 2022 roundtable events held in Washington, DC and Rome, Italy. In 2023, four additional roundtable events will discuss the topics of supply chain, sustainability, workforce skills, and international cooperation.

In each of these domain areas, insights from the roundtables will be used to identify strategies and solutions to help governments anticipate and address the challenges that lie ahead. We plan to leverage previous work that captures wisdom from past experiences, such as the IBM Center for The Business of Government report, "Covid-19 and its Impact: Seven Essays on Reframing Government Management and Operations", published in 2021 on lessons learned from the pandemic. And then we will critically apply this knowledge by identifying practical and specific recommendations for near-term implementation and long-term readiness.

The research includes actionable steps to lead in an era where managing unexpected events is part of the portfolio.



The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow us on LinkedIn at https://ibm.co/ibv-linkedin.

About the National Academy of Public Administration

The National Academy of Public Administration is an independent, nonprofit, and nonpartisan organization established in 1967 and chartered by Congress in 1984. It provides expert advice to government leaders in building more effective, efficient, accountable, and transparent organizations. To carry out this mission, the Academy draws on the knowledge and experience of its over 950 Fellows—including former cabinet officers, members of Congress, governors, mayors, and state legislators, as well as prominent scholars, career public administrators, and nonprofit and business executives. The Academy helps public institutions address their most critical governance and management challenges through in-depth studies and analyses, advisory services and technical assistance, congressional testimony, forums and conferences, and online stakeholder engagement. Learn more about the Academy and its work at https://www.NAPAwash.org.

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels. For more information, visit https://www.businessofgovernment.org

About the Center for American Studies

Headquartered in Rome, the Center for American Studies is one of the oldest and most prestigious institutions in Europe dedicated to the study of the US and its culture. The Center promotes transatlantic relations and dialog between America, Europe, and Italy and hosts seminars and conferences that address international politics, economics, and other topical issues, often in cooperation with other leading US and European organizations and experts. Meetings, exhibitions, screenings, and concerts at the Center, including US literary figures, journalists, artists, musicians, and filmmakers, offer rich cultural experiences for visitors and the general public.

Washington, D.C. roundtable participants

Zalmai Azmi
President and COO
Innovative Management and Technology Approaches

Lisa Barr
Director of Federal Cybersecurity
Office of the National Cyber Director

Florian Breger
Vice President, Civilian Government
IBM

Cristina Caballe Fuguet
Vice President, Global Public Sector
IBM

Dan Chenok
Executive Director
IBM Center for The Business of Government

Kelvin Coleman
Partner, Cybersecurity
IBM

Paul Dant
Senior Director
Cybersecurity Strategy & Research
Illumio

Curt Dukes
Executive Vice President & General Manager
Center for Internet Security

Candice Frost
Commander, Joint Intelligence Operation Center
United States Cyber Command

Terry Gerton
President and CEO
National Academy of Public Administration

Hope Goins
Majority Staff Director
House Homeland Security Committee
US Congress

Marilu Goodyear
Interim Director, School of Public Affairs and Administration
University of Kansas

Margie Graves
Senior Fellow
IBM Center for The Business of Government

Terry Halvorsen
General Manager, US Federal
IBM

Manuel Hepfer, Ph.D.
Cybersecurity Researcher
Head of Knowledge & Insights
ISTARI & Oxford University

J. Christopher Mihm
Former Managing Director, Strategic Issues
Government Accountability Office
Adjunct Professor, Public Administration & International Affairs Department
Syracuse University

Joe Mitchell
Director of Strategic Initiatives & International Programs
National Academy of Public Administration

Tim Paydos
Vice President & General Manager, Government
IBM

Greg Porpora
Distinguished Engineer and Distinguished Industry Leader
IBM

Franklin Reeder
Founding Chair
Center for Internet Security

Douglas Robinson
Executive Director
National Association of State Chief Information Officers

John Roche
Public Governance Directorate,
Governance Reviews and Partnership
Organisation for Economic Co-operation and Development (OECD)

Ronald Sanders
Staff Director, Florida Center for Cybersecurity
University of South Florida

Matt Scholl
Chief of Computer Security Division
National Institute of Standards and Technology

Tony Scott
Chief Executive Officer
Intrusion Inc.

Jim Sheire
Branch Chief
Cybersecurity and Infrastructure Security Agency

Kee Won Song
Global Research Leader, Government
IBM Institute for Business Value

Renata Spinks
Cyber Technology Officer
US Marine Corps Cyberspace Command

Bobbie Stempfley
Business Security Officer
Dell Technologies

Mike Stone
Managing Partner, Global Government
IBM

Shue-Jane Thompson
Managing Partner, Global Deal Leader
Strategic Sales
IBM

Kiersten Todt
Chief of Staff
Cybersecurity and Infrastructure Security Agency

Costis Toregas
Director
Cyber Security Policy and Research Institute
George Washington University

Daniel Weitzner
3Com Founders Principal Research Scientist,
Computer Science and Artificial Intelligence Laboratory
MIT

Dave Zaharchuk
Research Director
IBM Institute for Business Value

Notes and sources

1 Venkat, Apurva. “Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says.” CSO. January 4, 2023. https://www.csoonline.com/ article/3684668/cyberattacks-against-governments-jumped-95-in- last-half-of-2022-cloudsek-says.html

2 “Cost of a Data Breach Report 2022.” IBM Security. July 2022. https://www.ibm.com/resources/cost-data-breach-report-2022

3 Lake, Sidney. “The cybersecurity industry is short 3.4 million workers–that’s good news for cyber wages.” Fortune.com. October 20, 2022. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

4 “Women make up just 24% of the cyber workforce: CISA wants to fix that.” CBS News. March 19, 2022. https://wtop.com/business-finance/2022/03/women-make-up-just-24-of-the-cyber-workforce-cisa-wants-to-fix-that/

5 “Readout of Cybersecurity Executive Forum on Electric Vehicles and Electric Vehicle Charging Infrastructure Hosted by the Office of the National Cyber Director.” The White House Briefing Room. October 25, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/25/readout-of-cybersecurity-executive-forum- on-electric-vehicles-and-electric-vehicle-charging-infrastructure- hosted-by-the-office-of-the-national-cyber-director

6 “DHS Launches First-Ever Cyber Safety Review Board.” U.S. Department of Homeland Security. February 3, 2022. https://www.dhs.gov/news/2022/02/03/dhs-launches-first-ever-cyber-safety-review-board

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | March 2023

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.

PJNRBN7E-USEN-00