

The background of the page is a teal color with a subtle grid pattern. The grid lines are thin and light, creating a sense of depth and structure. The overall aesthetic is clean and professional.

FORUM ON CYBER RESILIENCE

2016 ANNUAL REPORT OF ACTIVITIES

FORUM ON CYBER RESILIENCE 2016 ANNUAL REPORT

MISSION

The Forum on Cyber Resilience is a roundtable of the National Academies of Sciences, Engineering, and Medicine. It was created to facilitate and enhance the exchange of ideas among scientists, practitioners, and policy makers who are concerned with urgent and important issues related to the resilience of the nation's computing and communications systems. The Forum serves as a source of knowledge, insight, and expertise and as a catalyst for stakeholder collaborations. It offers a venue in which to examine and discuss emerging challenges and issues as they become evident. At the same time, as a standing body, the Forum provides a base of engaged, long-term sustained thinking about emerging and future trends as cyber infrastructure challenges, threats, and issues evolve.

CONTEXT AND OPERATIONS

The Forum fosters sustained and candid dialogue among its government, academic, and industry members, and it serves as an independent focal point for honing and refining questions and issues that may not otherwise arise elsewhere or through the traditional Academies study-development process. The Forum is designed to foster activities developed by its members and to advocate for consensus studies or other activities, as needed, to inform its future meetings, and to raise awareness of issues and consequences in the wider public.

The Forum convenes senior representatives from government, universities, and industry to define and explore critical issues that are of shared interest, frame critical questions and needs, and incubate activities of ongoing value to participants. Broad themes it addresses include:

- traditional notions of cybersecurity and trustworthiness, such as maintaining security in the face of attacks, resistance to degradation, and the ability to recover from adverse events,
- ways to foster resilience in the face of natural and man-made disasters, disruptive technological change, and diverse and dynamic user populations,
- how to sustain capacity for innovation and adaptation, and
- ways to reflect the values—such as privacy, openness, trust, expression, usability, dignity, access—and needs of many stakeholders.

The Forum engages the policy community and multi-disciplinary research communities, along with industry practitioners, those who support and maintain critical infrastructure, and the broader public. One of the Forum's strengths lies in its convening power—the reputation of its members and of the Academies attracts key stakeholders to its activities. As an Academies convening body, the Forum offers opportunities to bring experts and practitioners together who may not otherwise get a chance to interact, to share insights across sectors and across communities, and to invite public participation in activities.

The Forum serves as a vehicle for framing new research questions, connecting stakeholders with needed expertise, and enhancing communication and understanding between sectors and disciplines. It is often in the intersections between areas and between disciplines where some of the most innovative thinking occurs. A key goal of the Forum is to surface and explore insights

related to the broad challenge of cyber resilience in ways that help change the conversation around these topics in productive ways. The Forum also works as an objective, technically-grounded, and technically-rigorous body, to help clarify the option space for policymakers.

MEMBERSHIP

The scope of the Forum is broad, encompassing technology and engineering as well as associated social and policy challenges. Accordingly, the membership consists of senior experts from a variety of disciplines, with a broad range of expertise, who represent a number of institutional perspectives and who can help lay a strong foundation for the roundtable to persist as a standing body. Forum activities span 3 axes of interest: ranging from immediate challenges to strategic long-term challenges related to infrastructure and resilience; from practical or operational needs to basic research; and from technical issues to social and policy issues:

IMMEDIATE CHALLENGES	<----->	STRATEGIC THINKING
PRACTICAL/OPERATIONAL	<----->	RESEARCH
TECHNICAL	<----->	SOCIAL/POLICY/ORGANIZATIONAL

The Forum membership was appointed with these axes in mind, and it includes experts and practitioners from academia and the private sector, along with ex-officio members from federal agencies (the National Science Foundation, the National Security Agency, and the National Institute for Standards and Technology). Forum members have backgrounds in law, policy, ethics, computer science and engineering, and cybersecurity.

Fred B. Schneider, a member of the National Academy of Engineering and **Samuel B. Eckert** Professor of Computer Science at Cornell University, was appointed as the inaugural chair of the Forum.

Membership will be periodically updated or expanded and membership will rotate over time. **Susan Landau** and **David Vladeck** joined the Forum in May 2016.

FORUM MEETINGS & ACTIVITIES

The Forum on Cyber Resilience met three times in 2016 for Forum meetings (January 12-13, May 9-10, and August 29-30) to engage with experts, host workshops, and plan activities. Forum activities connect experts and stakeholders across disciplines and sectors, provide a sounding board for leaders of other cybersecurity studies and programs, explore topics in depth and put information and insights into the public record, and affect the practice and research activities of those who participate in its activities. They provide opportunities for informal discussion with and among private sector participants and government official in a neutral setting.

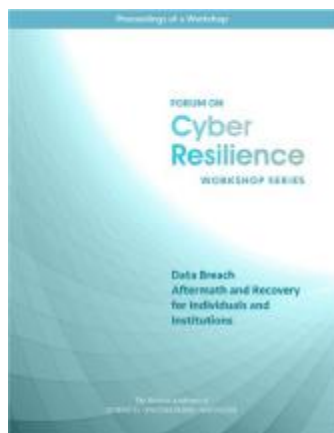
The Forum also advises and supports other cyber resilience-related Academies activities through a variety of interactions with other Academies groups and activities. Forum discussions provide input to and spin-off separately organized workshops and studies. Forum members suggest topics and experts to participate in these activities, and routinely serve as committee members and peer reviewers. The Forum convenes 1 or 2 public workshops and symposia each year on topics identified by its members (including sponsors). The goal is to push the conversation

'beyond the headlines' and to surface critical and sometimes unanticipated policy implications as well as technical research questions.

Expert Inputs & Dialogues

The Forum engaged with a number of experts about a wide range of topics during its second year. Each meeting provided opportunities to further advance strategies and plan for future Forum activities, and to engage around previously identified themes of interest.

January 2016



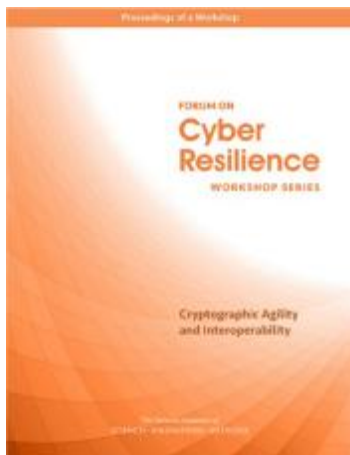
The January meeting featured a half-day, public workshop on Data Breach Aftermath and Recovery for Individuals and Institutions. Members heard a variety of presentations and engaged in discussions with participants surrounding:

- existing technical and policy remediations;
- and possible new mechanisms for better protecting and helping consumers in the wake of a breach.

The workshop resulted in the publication of *Data Breach Aftermath and Recovery for Individuals and Institutions: Proceedings of a Workshop*.¹ In addition to hosting the public workshop, the Forum invited **Anne-Marie Mazza** from the Committee on Science, Technology, and the Law to speak about the work of that committee and its intersection with technology policy, privacy, and cybersecurity topics.

Co-chairs of the Special Cyber Operations Research and Engineering (SCORE) Working Group, **Kathleen Bogner** and **Tim Polk** also spoke to the committee. The SCORE Working Group invited Forum members to comment on and provide feedback regarding its research agenda.

May 2016



The meeting featured a full-day, public workshop on Cryptographic Agility and Interoperability. Speakers at the workshop covered a wide-range of subjects, including:

- the history and practice of cryptography,
- standards and security implications;
- engineering at scale and user implications;
- research, industry, and policy implications;
- and future possibilities.

The workshop resulted in the publication of *Cryptographic Agility and Interoperability: Proceedings of a Workshop*.²

¹ Available online at: <https://www.nap.edu/catalog/23559>

² Available online at: <https://www.nap.edu/catalog/24636>

The forum also heard from **Kiersten Todt**, White House Commission on Enhancing Cybersecurity, and **Lauren Alexander Augustine** from the National Academies.

August 2016

The August meeting of the Forum on Cyber Resilience featured sessions on:

- safety and security in the emerging bioeconomy with a conversation with **Ed You** of the FBI;
- an exploration of cybersecurity challenges in regulated industries with presentations from **RADM Paul Thomas** of the US Coast Guard and NAE Member **George Cotter**;
- and a discussion of NIST Priorities and Updates on the Commission on National Cybersecurity with **Donna Dodson** and **Kiersten Todt**.

New ex officio Forum member and the head of the National Science Foundation's Computer & Information Science & Engineering (CISE), **Jim Kurose**, offered informal thoughts on NSF activities and priorities.

The Forum anticipates and welcomes additional interactions with policymakers on a range of topics over time. Its working list of potential future topics and activities includes:

- International norms and boundaries
- Internet governance and implications for network resilience
- Hardware and the supply chain
- Social values and institutional practice
- Affording confidence and engendering trust in systems
- Health IT & cybersecurity
- Bioeconomy & cyberbiosecurity
- Actionable improved cyber resilience
- Cyber resilience of the electric grid
- Mobile security, IOT

PARTICIPATING WITH THE FORUM

The Forum is the first roundtable to be developed by the Academies' **Computer Science and Telecommunications Board (CSTB)**. A pioneer in exploring Internet and information technology policy, CSTB convenes the nation's foremost computer science, telecommunications and information technology experts. The Forum on Cyber Resilience draws on CSTB's nearly three decades of foundational work in cybersecurity, privacy, and IT systems and is designed to leverage that and other Academies' work. Forum and CSTB members and staff collaborate closely to ensure alignment of the work of both.

During 2016 the Forum also engaged with several other groups within the National Academies and with several government groups to explore topics of mutual interest. National Academies groups included:

- Board on Health Care Services
- Committee on Science, Technology, and the Law
- Program on Risk and Resilience
- National Academy of Engineering

Agencies and government groups the Forum interacted with included:

- Department of Defense
- Federal Bureau of Investigation
- Federal Trade Commission
- National Institute of Standards and Technology
- National Science Foundation
- National Security Agency
- Special Cyber Operations Research and Engineering Working Group
- United States Coast Guard
- White House Commission on Enhancing National Cybersecurity

* * *

In May 2016, in collaboration with the **Academies' Health and Medicine Division** and its **Board on Health Care Services**, the Forum brought together approximately 20 experts to discuss current challenges and policy issues in the cybersecurity of health information technology (IT) and to consider whether the IOM/NRC could be of assistance in improving the security of health IT through a consensus study or other activities. At the meeting, participants shared information about their current activities and their perspectives on whether an IOM/NRC activity in this area would be of value.

* * *

The Forum serves as a guide and resource for other groups within the Academies grappling with tough cyber resilience issues within particular domains. Such interactions also provide fodder for the Forum's own strategic thinking and planning.

* * *

The Forum's website is www.cyber-forum.org. Members of the public who would like to be notified of upcoming Forum activities and meetings are invited to contact staff or to subscribe directly to an email list there.

In addition to core activities, the Forum is open to requests for potential collaboration. For example, the Forum could assist in making stakeholder connections, identifying experts, providing input to other activities, or disseminating information. Possible collaboration mechanisms include coordinating small stakeholder meetings, convening working groups, or co-organizing workshops.

The Forum is interested in hearing from the broader community about key cyber resilience topics and questions to address in its core work. Queries, requests, and ideas may be sent to the Forum at cyberforum@nas.edu.

For more information about the Forum and upcoming activities, see www.cyber-forum.org. The Forum on Cyber Resilience is sponsored by the National Science Foundation and the National Security Agency on behalf of the Special Cyber Operations Research and Engineering Interagency Working Group.

MEMBERSHIP OF THE FORUM ON CYBER RESILIENCE
as of December 31, 2016

Dr. Fred Schneider, Chair, NAE

Samuel B. Eckert Professor of Computer Science
Department of Computer Science
Cornell University

Dr. Anita Allen

Vice Provost for Faculty
Henry R. Silverman Professor of Law and Professor of
Philosophy
University of Pennsylvania

Dr. Bob Blakley

Global Head of Information Security Innovation
Citigroup

Fred Cate

Distinguished Professor and C. Ben Dutton Professor
of Law
Maurer School of Law
Indiana University

Dr. David Clark, NAE

Senior Research Scientist
Computer Science and Artificial Intelligence Lab
Massachusetts Institute of Technology

Hon. Richard Danzig

Senior Advisor
Center for a New American Security

Dr. Eric Grosse

VP Security and Privacy Engineering
Google, Inc.

David A. Hoffman

Director of Security Policy & Global Privacy Officer
Intel Corporation

Paul Kocher, NAE

President and Chief Scientist
Cryptography Research, Inc.

Dr. Tadayoshi Kohno

Short-Dooley Professor, Department of Computer
Science and Engineering
University of Washington

Dr. Butler Lampson, NAS, NAE

Technical Fellow
Microsoft Corporation

Susan Landau

Professor of Cybersecurity Policy
Worcester Polytechnic Institute

Steven B. Lipner, NAE

Independent Consultant

Deirdre K. Mulligan

Associate Professor, School of Information
University of California, Berkeley

Tony Sager

Senior VP
Center for Internet Security

Dr. William H. Sanders

Department Head and Donald Biggar Willett Professor
of Engineering
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Peter Swire

Nancy J. and Lawrence P. Huang Professor of Law
and Ethics, Scheller College of Business
Georgia Institute of Technology

David Vladeck

Professor of Law
Georgetown University Law Center

Mary Ellen Zurko

Principal Engineer, Security Business Group
Cisco Systems

Ex Officio Members:

Donna Dodson

Chief Cybersecurity Advisor
National Institute for Standards and Technology

Dr. Jim Kurose

Assistant Director, National Science Foundation
for Computer and Information Sciences and
Engineering

William "Brad" Martin

Research Advisor to the National Security Agency
Director's Special Assistant for Cyber
National Security Agency

Staff:

Lynette I. Millett, Director

Emily Grumbling, Program Officer

Katiria Ortiz, Research Associate

Shenae Bradley, Sr. Program Assistant