BCG

The Boston Consulting Group

TOWARD A MODEL FOR PUBLIC-PRIVATE COLLABORATION IN CYBERSECURITY

By Walter Bohmayr, Stefan Deutscher, and David Mkrtchian

Many will remember 2017 as the year of the big hack: two major cybersecurity events made headlines and put millions of people and their data at risk. The first was the WannaCry ransomware attack in May. Among other things, it froze operations at multiple hospitals in the UK's National Health Service and caused hundreds of millions of dollars in damages. The second, in September, was the Equifax credit bureau breach in which more than 140 million individual records were compromised.

Policymakers and business leaders have begun to recognize the need for more and better collaboration between the public and private sectors on issues related to cybersecurity, including encryption, data sharing, and data localization. On many of these topics, persistent misunderstandings over both policy and technical issues have created and exacerbated tension among public- and private-sector leaders.

To promote action-oriented and productive collaboration between the public and private sectors, The Boston Consulting Group supported the World Economic Forum in developing its report *Cyber Resilience: Playbook for Public-Private Collaboration.* The Forum and a cross-industry working group identified the policy issues where collaboration is imperative and presented 12 case studies that illustrate key technical and policy concepts. For each issue, the Forum's working group described all of the available policy options and their implications, rather than promoting one particular policy approach above others.

Countries will continue to pursue their own cybersecurity policies; every country has unique capabilities, risks, and values that shape its approach. Security policy is often mired in prolonged indecision. The Forum's report brings a clear-eyed view to help expedite policy development.

Key Policy Topics

The Forum's report identifies 14 key policy issues with respect to cybersecurity:

- **Research, Data, and Intelligence Sharing.** What is the government's role in sharing threat intelligence and promoting its dissemination?

- **Zero-Days.** To what extent should the government be involved in the research, collaboration, and purchase of zero-day vulnerabilities and exploits? To what extent should the government share these vulnerabilities with the private sector?

- **Vulnerability Liability.** Who is liable for securing software, and what are the tradeoffs associated with different liability regimes? How should liability shift when products reach the end of their useful life?

- **Attribution.** How should governments engage with the private sector when the private sector publicly alleges that a particular actor is responsible for an attack?

- **Botnet Disruption.** What should be done to prevent the proliferation of botnets? How should existing botnets be researched and studied? How should actors throughout the ecosystem disrupt botnets?

- **Monitoring.** To what extent should different actors be able to monitor internet traffic and enforce security protocols? What traffic should nonusers be able to monitor in order to promote security and other national interests?

- **Assigning National Information Security Roles.** Which entities and organizations should serve in national information security roles?

- **Encryption.** Who should be able to access sensitive data and communications?

- **Cross-Border Data Flows.** What are the security and nonsecurity implications when countries exert control over data?

- **Notification Requirements.** When should companies be required to notify relevant stakeholders that they have been breached or have otherwise experienced a cyberincident? What sanctions should policymakers apply to compromised organizations?

- **Duty of Assistance.** How should public resources be drawn upon in the wake of a cyberincident?

- **Active Defense.** What technical measures should the private sector be empowered to use to deter and respond to cyberthreats?

- **Liability Thresholds.** What is the reasonable duty of care that an organization should have? Who should bear the residual damages resulting from cyberincidents when an organization has sufficiently invested in security controls?

- **Cyberinsurance.** What incentives, if any, should be offered to obtain cyberinsurance? Which entities should be prioritized for these incentives?

Common Themes and Approaches

Across these topics, there are multiple linkages and interdependencies. For example, an effective intelligence-sharing policy helps constrain the spread of malicious software, and wider adoption of encryption may limit the ability to monitor and police network traffic. In practice, what these cross-topic connections mean for business leaders and policymakers is that cybersecurity policymaking efforts should be more collaborative and deliberative. Policy should stem from an ongoing iterative process, not from ad hoc and crisis-driven responses that lead to patchwork legislation. The report makes five recommendations on how to pursue collaborative policies.

First, the acceptable scope of action for the public and private sectors should be more clearly defined. For example, current policy around data and intelligence sharing is hin-

dered by the absence of clear guidance on what constitutes protected industry collaboration. And in the public-private context, the private sector is often reluctant to share data with the public sector owing to concerns that the data will one day serve as the basis for regulatory actions.

Second, the boundaries of permissible activity for security practitioners need to be well described. In many jurisdictions today, legitimate cybersecurity researchers—colloquially called "white hat" hackers, as opposed to the malicious "black hat" hackers—are uncertain as to the techniques and tools they are legally empowered to use when they test systems.

Third, the policy decisions made in national contexts should consider international implications—cyberspace recognizes no geographic boundaries. To predict the longer-term effects of a policy position, it is useful to consider the impact of a symmetric international policy response.

Fourth, policies to promote compliance, and thus security, should strike an appropriate balance between outlining regulatory objectives and specifying actual security controls, because the latter can result in undue compliance cost burdens. In an effort to develop cybersecurity governance structures, policymakers and, in particular, regulators, have begun to specify exhaustive processes and technologies for organizations to implement. But improved compliance by itself will not necessarily advance cyberresilience.

Last, security policy should focus on preventive efforts to minimize the frequency of the more contentious tradeoffs that are made in response to security issues. For example, significant debate and intellectual energy have been devoted to the question of how software vulnerabilities should be disclosed. Considerably less attention has been given to software coding quality standards. More secure software would reduce the stakes of the debate.

Cyberrisk will continue to be one of the most pressing challenges in the fourth industrial revolution. Leaders across the public and private sectors appreciate that mitigating this risk requires continued collaboration. The Forum's report, which can be viewed here, helps all stakeholders move toward this goal.

About the Authors

Walter Bohmayr is a senior partner and managing director in the Vienna office of The Boston Consulting Group and the global leader for cybersecurity. You may contact him by email at bohmayr.walter@bcg.com.

Stefan Deutscher is an associate director in the firm's Berlin office and the global topic leader for cybersecurity. You may contact him by email at deutscher.stefan@bcg.com.

David Mkrtchian is a consultant in BCG's New York office, on secondment with the World Economic Forum. You may contact him by email at mkrtchian.david@bcg.com.