Chapter Two

Cybersecurity

INTRODUCTION

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 percent worldwide, compared to the same period in 2021.[1] The cost of public sector data breaches also increased 7.25 percent 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.

This chapter examines today's complex cyber threat environment, and the government's responsibility to secure a safe and secure digital ecosystem. It focuses how best to reduce the impact of cyber incidents by developing and implementing cybersecurity strategies that promote resilience through public-private partnerships. The chapter recommends a series of actions designed to help governments emerge stronger from current and future cyber shocks.

Setting the Context

The adverse use of cyber tools by nation states and by other actors threatens national security, disrupts government service delivery and our daily existence, and supports criminal activity. And artificial intelligence (AI) can defend against nefarious activity, and also be an enabler. Research on areas where progress can be made is essential. Some of these areas were outlined in the Presidential Executive Order 14028 on Improving the Nation's Cybersecurity, and include:

- Improvements in threat information sharing between the government and private sector

Source: The IBM Center report, Preparing Governments for Future Shocks: An Action Plan to Build Cyber Resilience in a World of Uncertainty, *by Tony Scott, CEO of Intrusion, Inc.—as well as informed by the Future Shock Roundtable discussion and resources.*

- Government use of stronger cybersecurity standards such as zero trust architectures, encryption, and multifactor authentication

- Improvements in software supply chain assurance

- Improvements in detection, response to, and recovery from cyber incidents

One recent cyber incident illustrated gaps in security in government, commercial enterprises, and critical infrastructure. The Solar Winds incident showed vulnerabilities in the software development lifecycle process and the global supply chain. In the area of software supply chain assurance, "DevSecOps" principles can drive ecosystems for developing software based on those principles. As highlighted in a recent IBM Center report, *Achieving Mission Outcomes Through DevSecOps* by Margie Graves, using DevSecOps supports a preapproved software development environment where developers can experiment. Developers can code, test, prove, or disprove initial hypotheses about how the code will work, adjust the software build according to what they learn, and then continue iterating. Capability and features are developed into viable products. Security is incorporated into the build, and continuously tested.

Another recent incident, the ransomware attack on Colonial Pipeline, illustrated another vulnerability. The White House has initiated international partnerships to accelerate cooperation on improving network resilience, addressing the financial systems that make ransomware profitable, disrupting the ransomware ecosystem via law enforcement collaboration, and leveraging the tools of diplomacy to address safe harbors and improve partner capacity. AI has emerged as a key tool to guard against such attacks. Key questions that leaders addressed in considering cybersecurity resiliency as part of the Future Shocks initiative are summarized on the following two pages.

Key Questions for Protecting Cybersecurity and Critical Infrastructure

Fostering resilience and continuity of operations. Threats to undermine both organizational resilience and continuity of operations include shocks such as ransomware and climate catastrophe.

How can governments define a base level of preparedness required to withstand shocks and continue to provide essential citizen services?

Adapting governance to a shared responsibility model. Governments must plan for and evaluate cybersecurity governance in terms of defining responsibility for defense and resilience and develop policies and standards that align to agency missions (including modernizing security governance to support the implementation of zero trust principles).

How can partners best work across the broader ecosystem in addressing potential threats and the societal impact of cyberattacks?

Coordinating with stakeholders across all levels of government. Threats exist at all levels of government—national, state, local, tribal, and territorial. Some actions to take involve combining resources, activating public-private partnerships, coordinating incident response, and sharing leading practices.

How can communication informed by cyber expertise help governments understand policy gaps, implement coordinated policy solutions, and still maintain privacy?

Modernizing security of critical infrastructure. Defending critical infrastructure requires both an understanding of systems and a defense strategy that repels attacks but also has robust intrusion response.

How can governments work with industry to help make security intrinsic to infrastructure architecture and system design and more frictionless for end users?

Standardizing cyber incident response. An incident response strategy must be established well before a cyber incident. This should include robust testing and training processes and an efficient communications framework.

How can governments identify and engage stakeholders across domains?

Key Questions for Enabling Hybrid and Distributed Work

Using automation and connectivity to optimize capacity, skills, and resources. Building new capabilities around connected devices and connected services, embracing modernization and emerging technologies, and developing new technologies that keep pace with advancing threats.

How can governments work with industry and academia to stay ahead of the innovation curve and develop resilient systems, given potential threats to cyber, physical, and natural hazards?

Improving security hygiene. Understanding the collective impact of human behavior. Developing strong cyber hygiene for all individuals acting in both private and professional capacities is essential.

What strategies can all stakeholders take to promote security ABCs—awareness, behaviors, and culture?

Developing the cyber workforce. Anticipating skill demand, identifying talent gaps, and attracting and retaining talent in key security positions represent issues that government and industry are dealing with in many domains—issues addressed in a recent congressionally-mandated NAPA report for DHS CISA.[3]

How can we meet current and future cybersecurity demand, via better engagement with traditional and nontraditional sources of talent?

Re-envisioning technology, security, and data integrity as public goods. Security concerns exist for many forms of technology that are based on implicit trust, including the dissemination of misinformation and disinformation through social media. Additionally, many platforms operate across multiple levels of government and across international borders, introducing complex operational and compliance demands.

How can leaders reinforce the public's ability to securely access networks with accurate, high-value information anytime, anyplace, anywhere?

Recognizing the significance of emerging technologies, including quantum computing. Anticipating new threats from technology innovations, including the dangers posed to existing digital encryption protocols by quantum exploits as well as new ways of working with solutions based on distributed (versus centralized) authority (e.g., consensus-based solutions, distributed ledgers).

How should governments prepare for the future by addressing security vulnerabilities created by new technologies such as quantum computing and blockchain?

Insights and Recommendations

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.

U.S. and global leaders participating the Future Shocks Cybersecurity Roundtable outlined a series of recommendations designed to help governments emerge stronger from current and future cyber shocks.

Increase the cyber talent resource base

To address the rapidly growing gap between supply and demand for cybersecurity professionals, governments can work to increase the cyber talent resource base as an action at the top of the list of actionable priorities. 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. Moreover, 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.

Options for Developing the Cyber Talent Pipeline

Options to develop the cyber talent pipeline feeding government include:

- 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.
- 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.
- Reexamine 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.

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.

ACTION STEPS

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

Improve organizational collaboration for faster response

Collaboration and information sharing between national and international governmental organizations—as well as between government and business stakeholders—are complex and slow moving.

Despite recent progress in improving public-private coordination,[4] increased cooperation between cyberattackers 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.

A lack of transparency exists in 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. Emerging ecosystems concentrated on coordinated economic activities need to be more aware of their shared responsibility for cybersecurity and resilience.

Methods to improve collaboration 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 U.S. Department of Homeland Security Cyber Safety Review Board.[5]
- Encourage proactive investment to prepare for threats coming from advances in AI and quantum computing technologies.
- Use AI and automation technologies to strengthen cyber defenses more broadly and counter the use of these technologies by cyber adversaries and threat actors.

ACTION STEPS

- 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.

Align public and private sector cybersecurity priorities
By identifying common challenges, sharing best practices, and exploring avenues for cooperation, numerous areas exist 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 staff, 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.

ACTION STEPS

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

Study ways to bolster democratic institutions against cyberattacks
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, longer-term efforts could succeed in swaying public opinion. Due to the complexities represented by these cyber challenges to representative forms of government, a broad consensus has yet to be formed on the most effective ways to defend against this growing threat—more research into measures that can counter cyber threats to democracy is needed.

Additional challenges include:

- State-backed efforts to shape public opinion through the broad suppression of public information available on media platforms. For example, China, Russia, and other authoritarian regimes 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. This topic requires more in-depth research to understand the implications in terms of cyber risk, threats, and resiliency.

ACTION STEPS

- 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.

LOOKING FORWARD

Just as prior waves of dramatic technological 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.

Taken together, the insights and recommendations outlined in this chapter provide a viable road map for governments to follow in the continual improvement of their cybersecurity posture. Government agencies, reliance on digital networks in the response and recovery from the pandemic will likely only grow in their efforts to weather an uncertain future.

Endnotes

1 Venkat, Apurva. "Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says." CSO. January 4, 2023, https://www.csoonline.com/article/574275/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/downloads/cas/3R8N1DZJ.

3 A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Future, https://napawash.org/academy-studies/dhs-cybersecurity-workforce.

4 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.

5 "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.