THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Conference Report

GW Business & Policy Forum: Attacking Cybersecurity Risks

An Industry-Government-Academia Discussion

On April 25, 2023, the George Washington University launched the inaugural GW Business and Policy Forum bringing together leaders from the private and public sectors to address the most significant issues in the evolving landscape of cybersecurity and emerging technologies, with a focus on policy and regulation. The forum, under the theme "Attacking Cybersecurity Risks," attracted more than 700 registrants and 28 expert speakers.

This conference report describes the key themes that emerged as representatives from government, industry, and academia discussed current cybersecurity threats, their potential impact on the economy and national security, and solutions for the future. Although this document represents a snapshot in time against the accelerating backdrop of cyber threats, it is underpinned by the shared interest and responsibility of business, government, and higher education to find durable strategies for a safe digital ecosystem.

Introduction

Humanity has become inextricably reliant on information systems and digital connections. Indeed, emerging technologies have become a dominant force in our society—driving economic security, policy and culture, equity and prosperity, cutting-edge research and science, and accounting for more than US$40 trillion in global nominal GDP.

Billions of individuals across the globe log into digital devices daily, sharing and generating data. Each new device and each new login provides an opening for cyber attackers. Some of these attacks endanger national security and critical infrastructure. Some penetrate business firewalls and plant ransomware. Still others circulate disinformation and misinformation that undermine democratic institutions, news coverage, and corporate reputations. All of these assaults disrupt the lives of citizens in far-reaching ways.

In releasing the National Cybersecurity Strategy on March 2, 2023, the Biden administration called for rebalancing the responsibility for defending cyberspace, shifting the burden away from individuals, small businesses, and local governments and onto the stakeholders that are best-positioned to mitigate risk for all. The GW Business and Policy Forum brought together three principal stakeholders in the cybersecurity debate—government, industry, and academia—to discuss how to build resilient defenses against accelerating threats to the digital ecosystem and disarm the bad actors behind them.

A series of overarching themes emerged from the forum, emphasizing the need to:

- foster an intentional culture of cyber safety;
- engender a powerful collaborative effort that transcends sectors and borders;
- elevate speed and agility in identifying and mitigating attacks;
- employ the resources and insights of a diverse field of knowledgeable players and policymakers;
- increase strategic investments that build resilience into systems and operations;
- create accountability through thoughtful and nimble norms, rules, and regulations;
- leverage academia's strengths in building a defensible digital ecosystem.

Creating a Pervasive Culture of Cyber Safety

"Can you pick out all the bad apples acting? Absolutely not. But can you increase your entire cyber program in ways that you can use automated tools to detect some of those anomalous behaviors…. I think there are opportunities there to do that."

—Renata Spinks, U.S. Marine Corps Assistant IT Director and Deputy CIO of Information Control, Communications, and Computers

The digital landscape and human development are now inseparably connected. Nearly every aspect of daily living in the United States is touched by technology. Cybersecurity has never been more important, urgent, or daunting.

Cyber threats come from countless directions—from the criminals who steal digital identities to the malicious actors who threaten power grids to the nation-state attackers who embrace cyber espionage and wield disinformation as a weapon. Participants at the GW Business and Policy Forum uniformly underscored the need to intentionally build cybersecurity into the design of all operational systems and platforms and to embed it in workplace culture at every layer.

The challenge, however, is to ensure that this security is effective within a landscape where advances come "at the speed of digital." In discussing how artificial intelligence (AI) is transforming cybersecurity, Kent Walker, president of global affairs at Google, said this company's commitment to secure systems is so rigorous that the multinational tech giant has delayed the launch of technology until it felt adequate safeguards were in place. Several other times during the course of the daylong forum, the promise of AI was weighed against its peril—with a call for harnessing AI's remarkable potential as a cyber sleuth capable of detecting patterns that signal attempts to disrupt digital life.

During a cyber wars discussion with *New York Times* National Security Correspondent David Sanger, Microsoft Corporation Vice President Tom Burt predicted AI algorithms that detect suspicious codes will become increasingly effective and "provide the defenders with a significant advantage." But operational fortresses against advanced threats are only effective if their weakest links—humans—are also onboard as defenders. A click on a malware link or a poorly guarded password can have far-reaching and devastating results. Training and education are valuable tools in offsetting worker error. But cybersecurity integrity cannot depend on constant watchfulness over the individual users of digital technology. Systems must be designed with solid safeguards to circumvent human-error lapses and minimize downside risk

A United Front: Marshaling Information, Insight and Intelligence

"We're looking at collaboration on steroids."

—Sudha Vyas, Chief Cybersecurity Architect, Department of Defense CIO

Citizens must be able to trust that their essential services, infrastructure, and national security are impregnable. Yet no lone business or agency, no single infrastructure sector, no individual nation is assured success in defending against cyberattacks on its own. Collaboration is crucial for a clear and current picture of the cyberthreat landscape. It is also vital in successfully anticipating future dangers.

As cyber assaults rise dramatically so, too, do the stakes. The federal government may sit at the vanguard of security, but more than 80 percent of critical infrastructure is owned by private sector organizations. One of the biggest complaints is the federal government's failure to provide timely and actionable intelligence related to cyber threats. Small businesses, entrepreneurial operations, and local governments are especially vulnerable. An estimated 60 percent of small businesses do not survive a significant cyberattack.

Global industry leaders and government officials need to robustly advance cybersecurity in the context of public-private partnerships that include academia. New hubs to cultivate this

recalibration are already appearing. The NSA's groundbreaking Cybersecurity Collaboration Center (CCC) is one example. It relies on industry partnerships and academia to help prevent foreign cyber threats to national security systems, the Department of Defense, and the defense industrial base. The CCC optimizes the strengths of its collaborators in securing the country's most critical networks.

The private sector, too, continues to build its defenses through partnerships such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), whose membership—more than 7,000 financial institutions—share cyber threat indicators with the government, and vice versa. Jason Witty, chief security officer at USAA, said while the construct works well, it represents a self-contained solution in a world that must break down sector silos for more resilient cyber defense.

Accelerating broader cooperation is essential, but it is not always easy. It requires a cultural shift in the relationship between industry and government, a relationship that, traditionally, is more often adversarial than collaborative. Within this shift toward collaboration, the value of sector-specific engagement magnifies when it serves as a springboard for broader integration and innovation. Information exchange across disciplines is especially urgent in the area of critical national infrastructure—energy grids, health care systems, transportation systems—where a collaborative defense, at speed and scale, can best address challenges distinctive to those sectors.

National partnerships build strongholds against intrusions. But cyberattacks, like cyberspace, are borderless. That means the United States must also craft partnerships and guiding frameworks with other countries and scale the sharing of threat information. Multinationals, in particular, need global standards and guidelines that align across national borders. There are no security or investment efficiencies from having one technological solution in France and another in Japan.

Leveraging the Agility and Speed of Innovation

> ***"The opportunity is to innovate for good at a faster rate than we've ever innovated before. If you do that in an ethical framework, progress will be the outcome."*** *—Deloitte CEO and Chair Dan Helfrich*

Cybersecurity operates on a frenzied landscape where attackers maximize agility and speed as advantages. While it is a daunting challenge for government and industry to keep ahead of vulnerabilities, it is imperative that they accelerate their ability to prevent and respond to cyber threats, identify bad actors, and anticipate the next vulnerability.

There is potential to drive faster and more robust responses through the use of quantum computing, machine learning, and the underlying power of artificial intelligence (AI) within the standard organizational cyber infrastructure. These evolving technology advances are making headway in threat preparedness and prevention. However, similar tools are also available for high-stakes threat actors, who are accelerating cyberattacks with increasingly acute impacts. That means leadership must step up its game.

Industry executives recognize they have an escalating responsibility to understand the cyber threat landscape so they can respond proactively, but they can be overwhelmed by the frenetic pace of digital advances. Delays in discovering or reporting major cyberattacks are a problem. IT leaders, the C-suite, and corporate boards need to better—and more frequently—communicate with one another about their organizations' cybersecurity goals and challenges.

Government, too, faces an uphill climb. Pivoting from its current technology systems, some of them designed decades ago with multiple contractors and varying programming languages, is complicated. There is also concern that government regulation, guidelines, and policy—or lack of them—are not evolving fast enough to open nimble pathways toward resilient security. And some government agencies have not yet fully embraced a cyber safe culture.

To ensure a cyber safe culture, the actions, attitudes, assumptions, and values of an organization must align with cybersecurity. Such a culture is shaped by the goals and policies of its leadership and buy-in at every level of the organization. Fundamental to a cyber safe culture is the acknowledgement that people are both an organization's best defense against cyber perils and its weakest link. A strong digital ecosystem is built on employees' understanding of how their daily actions can mitigate risk.

Speed and agility remain a cyber-defense challenge of large organizations and, especially, government. But there are exceptions. The Transportation Security Administration (TSA) in the Department of Homeland Security, for example, operates at a fast-changing front line with passengers and industry, protecting physical and digital infrastructure, little of which it owns. It acknowledges that there are still significant vulnerabilities, such as the 2021 ransomware attack that closed off East Coast gas and natural gas supplies, but it has shifted toward outcome-focused solutions and works more closely with private industries. It is providing a model for other agencies and organizations.

Reshaping the Cyber Workforce and its Leadership

> ***"There will be entirely new jobs that come out of this."***
>
> *— Robert Cunningham, Vice Chancellor for Research Infrastructure, University of Pittsburgh*

This has never been a more important and in-demand career field for smart energetic people than cybersecurity. Matching workforce needs with the right talent, however, requires new thinking about skillsets, not only for workers but also for those in leadership.

C-suite and government leaders, the drivers of the new economy, must begin a sustained effort to deepen and update their understanding of the threat landscape. People who rose to leadership roles without cyber expertise should be upskilled and reskilled against the current body of knowledge. This could happen formally or through greater exposure to cyber experts within their organizations. Absent that, persistently low C-suite engagement around cybersecurity will leave companies in peril, endanger their industry partners, and divert resources to the aftermath of attacks rather than their prevention.

Even while re-envisioning current management skillsets, industry must look forward to thoughtfully designing future management teams with a broad range of experiences. The field needs the best and brightest from across multiple disciplines. Diversity—experiential, racial, gender, and in expertise—will be essential in a properly-prepared cyber workforce.

One of the current labor challenges is talent retention. Both industry and government will be pressed to identify and develop the cyber talent they need both now and in the future. Interesting new pathways to careers could emerge, and universities will be pushed to build more dynamic talent pipelines.

Lawmakers and policymakers must also dramatically deepen their cyber safety knowledge and expertise. U.S. Senator Mark Warner, who co-founded the Senate Cybersecurity Caucus and co-sponsored two legislative acts aimed at strengthening American cybersecurity, told the forum that Congress has not moved fast enough or creatively enough on the issue, and much of its action has been reactive rather than proactive.

Last year, National Cyber Director Chris Inglis committed to developing a National Cyber Workforce and Education Strategy designed to address talent gaps in the cyber workforce. But participants at the GW Business and Policy Forum advocated for action on a more widespread landscape. Business and academic leaders called for cyber education to be part of fundamental education, saying that physicians, lawyers, and other professionals in non-technical fields could benefit from such an approach. It was suggested that cyber education could be incorporated as a component of all continuing education.

Investment Must Be Stepped Up

> ***"We need to spend more resources to get cybersecurity programs right, and we need to do it rapidly. Right now, the advantage is very much in favor of the attackers."***
>
> *– Michael K. Atkinson, Partner, Crowell & Moring*

By the year 2025, according to *Cybercrime Magazine*, global losses incurred as a result of cybercrime activity are estimated to reach US$10.5 trillion. With data breaches, malware, ransomware, fraud, phishing attacks, and identity theft, cybercrime affects every kind of enterprise, from small businesses to multinational corporations. Reputational losses incurred as a result of data and intellectual property theft by cybercriminals can be incalculable.

Valerie M. Cofield, chief strategy officer for the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), the national coordinator for 16 critical infrastructure sectors, said defenders of the digital ecosystem must be prepared for not just the impact of an attack but also the cost of its cascading effects. She pointed as examples to the water sector, which lacks cyber expertise and is not well resourced, and K-12 schools, which are attractive targets for ransomware attacks.

Is government investing enough in its cyber resources? Is the private sector? The answers are currently 'no' and 'no.' But the amount of investment is only one gauge of cyber safety. The *goal* of the investment may be an even more important indicator. Industry, in particular, must shift how and why it invests, moving from its current reactive approach toward a proactive vision focused on prevention. The consideration should not be on how much investment but, rather, the more complex question of what outcome is being sought.

Investment alone will not stop all cyber assaults, and those attacks can be pernicious, bringing with them considerable—even crippling—mitigation costs. Cyber insurance can be valuable in those cases, yet the "how much" challenge remains. How much cyber insurance does a company need? Cyberattacks are not one-time occurrences. Companies and public sector entities can be targeted repeatedly. How does an enterprise measure its cyber risk? Business has become better at enumerating its losses and potential losses, but it cannot predict the probability that it will be targeted or the frequency with which it might be attacked. If a company over-invests in its firewalls and insurance or sets aside excessive capital to mitigate cyber damage, it takes away resources from other areas of the organization and may diminish its ability for growth. If it under-invests, it makes itself vulnerable.

On this front, there is an opportunity for AI to improve predictive information available to industry. Academic research, too, may help in calculating risk.

Accountability: Rethinking the Conversation

> ***"When you try to bring regulation to quick-moving technology, you risk regulating something that is already [in the] past. You need a large stakeholder discussion … to talk about guidelines."***
>
> *– Hans Vestberg, Chairman and CEO, Verizon*

As collaboration advances to address advanced threats, cybersecurity protections must also be in place to make it harder for adversaries to disrupt the digital ecosystem. The Biden administration has created cybersecurity requirements in certain critical sectors. In other sectors, new authorities will be tasked with hammering out regulations to foster better cybersecurity practices at scale.

Regulation until now has been largely voluntary, and that has allowed some companies and contractors to be haphazard about their systems and software—leaving the digital ecosystem only as strong as its weakest components. Both government and industry seem engaged in a course correction, with growing consensus around the need for thoughtful, nimble regulation that incentivizes business collaboration.

Flexible guidelines that spring from a collaborative discussion promise to bring a competitive advantage to the U.S. cybersecurity arena. Incremental regulation will be key.

Leveraging Academia's Strengths

Higher education is positioned for a linchpin role in cybersecurity, identifying and preparing the workforce of the future, advancing ethics in the arena, contributing to the ongoing development of AI and other technologies, and spearheading the research and scholarship needed to stay ahead of cyber threats and challenges.

Even as they strengthen their role in these areas, universities will need to step up the pace and agility of their operations and research to match the unrelenting demands of the digital ecosystem. They will also be called upon to deepen their partnerships with government agencies and technology firms, including defense contractors. And they will be watched for their guidance on workforce requirements for the future.

Higher education already carries an entrenched role in cyber workforce development. The reskilling and upskilling of government and industry leadership will be in its hands, as well as the preparation of tomorrow's digital workforce. It will also be called to provide data-driven policy guidance and training for lawmakers and policymakers. As cyber skills become more deeply desired across disciplines and career fields, higher education will shape the programming and transfer of knowledge that makes it possible.

Higher education is positioned to step up its cutting-edge research and data-driven analysis around cybersecurity, but speed and agility will be challenges. The nature of scholarly research makes it difficult to keep up with hyper-paced technological advances. Academia will also be watched for guidance on what cybersecurity and AI research collaboration with other academic institutions around the world should look like.

Elham Tabassi, associate director of emerging technologies at the Information Technology Laboratory (ITL), one of six research laboratories at the National Institute of Standards and Technology (NIST), noted that academia is also a starting ground for cybersecurity innovation, pointing to the broad pathways from academia to the startup space. She also cited open sourcing as an avenue for putting innovative techniques in the public space.

Academia will be the hub for convening dialogues with stakeholders in and defenders of cyber space. Cyber ethics, an area that lags technology's fast pace, will be part of those discussions. As Tabassi noted at the forum, students and young workers already are embracing new value considerations. Rather than asking themselves if they "can" do something, as past generations have, Tabassi said they now ask whether they "should" do something.

Like other stakeholders, academia will face critical considerations related to its investment in cyber education, research, and information dissemination. The George Washington University used the GW Business and Policy Forum to launch Cyber at GW, a facilitator for bringing together the private and public sectors and their global leaders to develop informed solutions and policy recommendations on privacy and cybersecurity. Research, education, and community engagement and collaboration are the pillars of the initiative.

Acknowledgements

The George Washington University School of Business, which spearheaded the Business & Policy Forum, is grateful to the many people who helped ensure a thoughtful and productive public discussion focused on one of the greatest threats facing the country and the world.

We are especially grateful to:

- Christopher Alan Bracey, Provost and Executive Vice President for Academic Affairs
- John Lach, Dean, GW School of Engineering and Applied Science
- Dayna Bowen Matthew, Dean, GW Law School.
- Irina Orlova, Assistant Dean for Strategic Initiatives and Special Projects, GW School of Business
- Liesl Riddle, Dean, GW College of Professional Studies
- Mark S. Wrighton, President, George Washington University (2022-2023); and

We would also like to express a special word of gratitude to all of the forum speakers and moderators who provided the expert insights that are composed within this report.