WHITE HOUSE DEBRIEF:

Advancing Cybersecurity in Academia: Safeguarding the Student Experience

The Call for Action

The Biden Administration has made cybersecurity a priority and since taking office has taken extensive measures to highlight the issue and enhance the nation's security. On May 12th, 2021, the White House issued an Executive Order (EO) on Improving the Nation's Cybersecurity. It calls on the private sector to adapt to the changing threat environment, and ensure products are built and operate securely to foster a more secure cyberspace. The EO also tasks public sector organizations to accelerate cloud adoption, with a preference for cloud capabilities that implement or advance the adoption of zero trust. Zero trust architecture requires constant verification during digital interactions to prove that users are who they say they are.

> ***"It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security."***
>
> **President Biden**
> (May 12, 2021, Executive Order on Improving the Nation's Cybersecurity)

Then, in August, President Biden convened a summit of industry and government leaders at the White House to discuss the "whole-of-nation" effort needed to address cybersecurity threats. The Summit noted that recent high-profile cybersecurity incidents demonstrate that both U.S. public and private sector entities face sophisticated malicious cyber activity. In parallel, the White House's August Fact Sheet states that "incidents affect businesses of all sizes, small towns and cities in every corner of the country, and the pocket-books of middle-class families."

As today's higher education institutions and K-12 schools continue to incorporate the use of technology for teaching and learning, their efforts are increasingly hampered by cybersecurity attacks.

A Campus Technology "pulse survey" from July 2021 among higher education IT leaders and professionals found that two-thirds of institutions (63%) have reshaped their cybersecurity incident response, either putting the finishing touches on their strategies or improving their capabilities in response to these increasing cyber threats.

The case is no different in K-12 districts, where schools have long collected personal data, including student health and wellness information and family and staff financial details — targets for any cybercriminal – are also now being forced to take preemptive measures.

Meeting the Call: Industry Commitments to Cybersecurity

At the August Summit, several participants announced commitments and initiatives aimed at bolstering the nation's cybersecurity. These commitments, highlighted below, build on the already extensive work that many are already doing to ensure the security of their infrastructure and that of their customers.

> *"Most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone."*
>
> **President Biden**
> (August 26, 2021, Google, IBM, Tech Executives Unveil Cybersecurity Commitments at White House Summit)

Google Cloud

- Investing $10 billion over the next five years to expand zero-trust programs
- Taking action to secure the software supply chain and enhance open source security
- Helping 100,000 Americans earn industry-recognized digital skills certificates providing the knowledge that can lead to secure high-paying, high-growth jobs

Microsoft

- Investing $20 billion over the next 5 years to accelerate efforts to integrate cybersecurity by design and deliver advanced security solutions
- Immediately making $150 million available in technical services to help federal, state, and local governments upgrade security protection
- Expanding partnerships with community colleges and non-profits for cybersecurity training

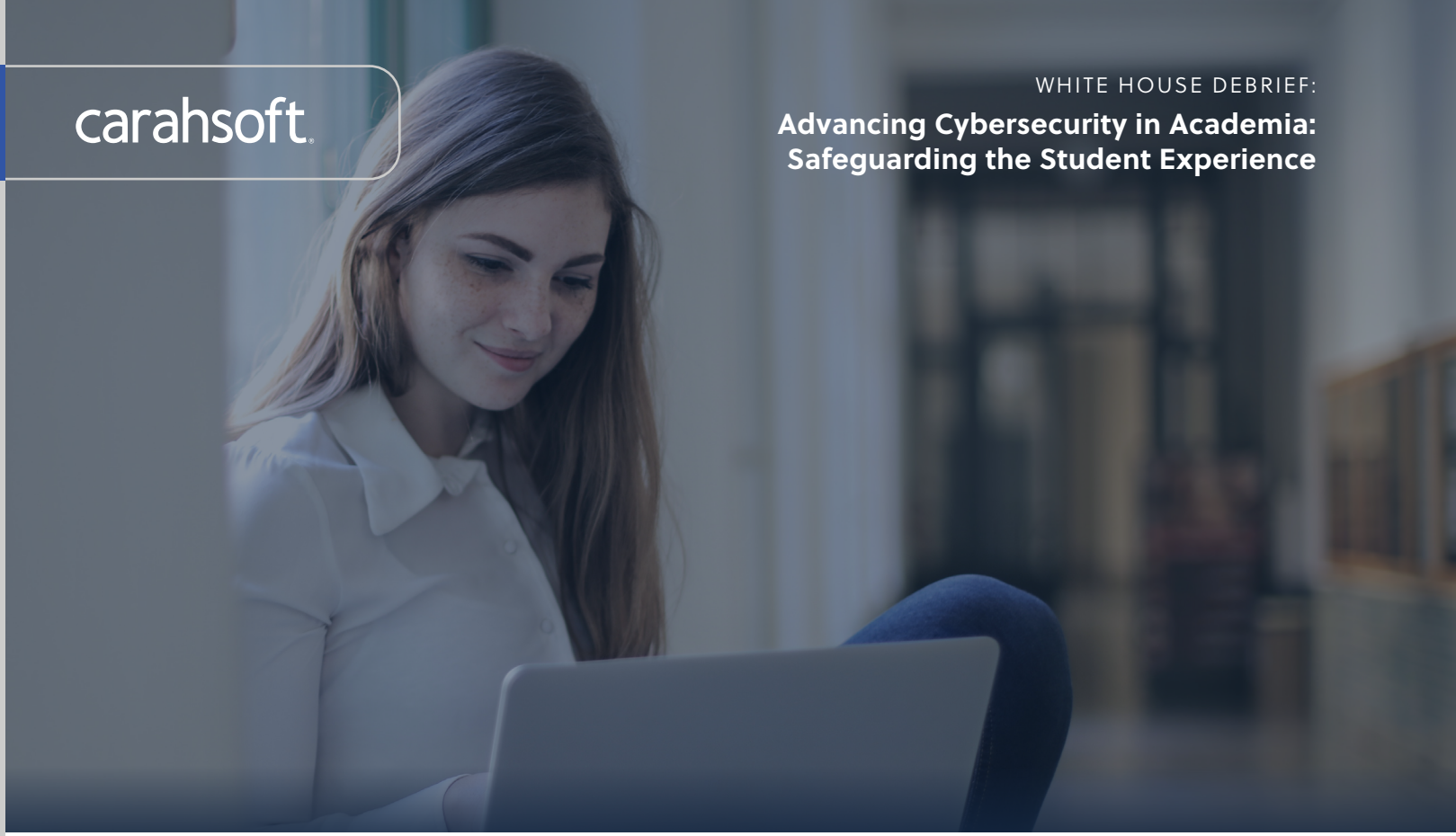
IBM

- Training 150,000 people in cybersecurity skills over the next three years
- Partnering with more than 20 historically black colleges & universities to establish Cybersecurity Leadership Centers to and grow a more diverse cyber workforce

aws

- Making available to the public at no charge the security awareness training it offers its employees
- Offering AWS account holders a multi-factor authentication device to protect against cybersecurity threats like phishing and password theft—at no additional cost

For more information, visit carah.io/WhiteHouseCyberFactSheet



carahsoft

WHITE HOUSE DEBRIEF:

Advancing Cybersecurity in Academia: Safeguarding the Student Experience

With these commitments, today's leading technology manufacturers are raising the bar on domestic cybersecurity practices and standards, which strongly aligns with educational institutions' needs to protect faculty and students. Carahsoft is here to help. With our expertise, vendors like AWS, Google Cloud, IBM, and Microsoft, and through our contract with E&I Cooperative Services, it's never been easier to incorporate top-rated cybersecurity technology for a more seamless and secure learning experience.

To learn more, call (703) 673-3518, email E&ISales@carahsoft.com or visit carahsoft.com/EandI.

E&I Cooperative Services

Sourcing. Strategy. Savings.®

WORKS CITED

"Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity." The White House, The United States Government, 25 Aug. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

"Executive Order on Improving the Nation's Cybersecurity." The White House, The United States Government, 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.