COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 9. September 09, 2021 To Combat Cyber Crime, White House Initiative Promises Tools; Some Seek Funding, New Laws

By Jane Anderson

As ransomware attacks become epidemic and breaches get larger, the Biden administration is partnering with private industry to bolster security and education in an effort to step up defenses against cybercrime. As part of the initiative, at least one company that offers cyber insurance will require that its policyholders adhere to a set of standards.

Still, health care cybersecurity and compliance experts told *RPP* that additional steps will be needed—and quickly—to protect health care entities from phishing, hacking and ransomware.

"I think this initiative is a big step in the right direction—it's great to see that the U.S. government is seriously addressing cybersecurity and working to get ahead of the problem. In addition, seeing the commitment for cybersecurity training is a good sign," said Adrien Gendre, chief product officer and co-founder of Vade Secure, which offers artificial intelligence-based cybersecurity. "How quickly the initiatives will deliver remains to be seen, and some of them are intended as long-term solutions (i.e., the initiatives focusing on cybersecurity skills and education)."

Gendre said moves by insurers to hold insured companies to a high standard could induce faster change in the private sector. "Cyber insurance companies requiring that businesses meet a threshold of best practices can have an immediate and long-lasting impact, as it forces businesses to get serious about their security or lose their coverage as a result," he said.

At a White House meeting held Aug. 25, the Biden administration announced that the National Institute of Standards and Technology (NIST) will collaborate with industry and other partners to develop a new framework "to improve the security and integrity of the technology supply chain."[1]

Top tech companies and insurers, including Microsoft Corp., Google Inc., IBM, the Travelers Companies Inc. and Coalition Inc., committed to participating in the NIST-led initiative. "The approach will serve as a guideline to public and private entities on how to build secure technology and assess the security of technology, including open source software," according to the fact sheet.

Firms Pledge Resources, Training

As part of the White House initiative, several tech companies announced their own security programs:

- Apple said it would "establish a new program to drive continuous security improvements throughout the technology supply chain. As part of that program, Apple [said it would] work with its suppliers—including more than 9,000 in the United States—to drive the mass adoption of multi-factor authentication, security training, vulnerability remediation, event logging, and incident response."
- Google said it would "invest $10 billion over the next five years to expand zero-trust programs, help secure the software supply chain, and enhance open-source security. Google also announced it will help 100,000

Americans earn industry-recognized digital skills certificates."

- IBM said it would "train 150,000 people in cybersecurity skills over the next three years." In addition, IBM said it would "partner with more than 20 Historically Black Colleges & Universities to establish Cybersecurity Leadership Centers to grow a more diverse cyber workforce."
- Microsoft said it would "invest $20 billion over the next 5 years to accelerate efforts to integrate cyber security by design and deliver advanced security solutions. Microsoft also announced it [would] immediately make available $150 million in technical services to help federal, state, and local governments with upgrading security protection, and will expand partnerships with community colleges and non-profits for cybersecurity training."
- Amazon said it would "make available to the public at no charge the security awareness training it offers its employees." In addition, Amazon said it would "make available to all Amazon Web Services account holders at no additional cost, a multi-factor authentication device to protect against cybersecurity threats like phishing and password theft."
- Resilience Cyber Insurance Solutions said it will "require policy holders to meet a threshold of cybersecurity best practice as a condition of receiving coverage."
- Coalition said it would "make its cybersecurity risk assessment & continuous monitoring platform available for free to any organization."
- Several educational organizations, including Code.org, Girls Who Code, the University of Texas System, and Whatcom Community College in Bellingham, Washington, announced new initiatives or expansions of cybersecurity programs. For example, the Texas system said it will work to "upskill and reskill over 1 million workers across the nation by making available entry-level cyber educational programs through UT San Antonio's Cybersecurity Manufacturing Innovation Institute." Meanwhile, Whatcom Community College has been designated the new National Science Foundation Advanced Technological Education National Cybersecurity Center and will provide cybersecurity education and training to faculty and support program development for colleges to fast-track students from college to career.

Health care cybersecurity experts praised the joint public-private initiative while also saying more is needed to protect the medical industry.

John Riggi, senior advisor for cybersecurity and risk at the American Hospital Association, said in a statement that "the solution to this national security threat will rely on leveraging public/private expertise and capabilities and expanding the cyber workforce."

Still, Riggi added, "we also recognize that defense is only half the solution to this national security threat. We urge the government to continue a coordinated campaign utilizing all diplomatic, financial, law enforcement, intelligence and cyber military capabilities to disrupt these foreign-based ransomware gangs, seize their illegal proceeds and increase consequences for those nations which harbor them—as we effectively did in the global fight against terrorism."