September 14, 2021

To Combat Cyber Crime, White House Initiative Promises Tools; Some Seek Funding, New Laws

Health Care Compliance Association (HCCA)

+ Follow Contact

[author: Jane Anderson]

Report on Patient Privacy 21 no. 9 (September, 2021)

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.”

Advocates Want Law

Vade Secure’s Gendre said that health care customers want tech vendors to supply solutions that anticipate coming threats, and added, “they have also expressed an interest in the government raising awareness around cybersecurity threats.”

Roger Shindell, founder and CEO of Carosh Compliance Solutions, said that to address cybersecurity threats within the health care industry, Congress needs to pass the 2021 Cyber Shield Act, which would create a voluntary program for devices that have backdoor access built in. “My personal complaint is that nothing has been mentioned regarding the 2021 Cyber Shield Act,” he told *RPP*. “Pass the Cyber Shield Act of 2021 and make it required, not just voluntary.”

The Cyber Shield Act, introduced by Sen. Edward Markey, D-Mass., and Rep. Ted Lieu, D-Calif., would create a voluntary cybersecurity certification program for internet-connected devices. According to Markey, the bill would establish an advisory committee of cybersecurity experts from academia, industry, consumer groups, government and the public to create cybersecurity benchmarks for internet-connected devices.[2]

The legislation would require the Department of Commerce to establish the program for internet-connected devices. It also would require the department to establish a Cyber Shield Advisory Committee to recommend: 1) the format and content of Cyber Shield labels for covered products, and 2) the process to identify, establish, report on, adopt, maintain and promote compliance with industry-leading cybersecurity and data security benchmarks to enhance cybersecurity and protect data.

In addition to passage of the Cyber Shield Act, Shindell said he wants to see the Food and Drug Administration restructure its requirements for security patches of FDA-covered medical devices. “The [current] process is way too slow and onerous,” he said.

Richard Tracy, chief security officer at security firm Telos Corporation, said that funding from the infrastructure package currently being debated in Congress might help health care organizations make investments in cybersecurity. “Many organizations, especially smaller organizations, do not have adequate resources to make appropriate investments on their own,” he told *RPP*.

In addition, Tracy said, the federal government could offer industry-specific cybersecurity framework implementation guidance, which might offset some possible confusion about how to implement the framework for specific environments and industries.

Call for Integration, Evolution

Finally, the federal government could offer additional guidance on how to protect against various threat types, Tracy said. “NIST is already working on a CSF [cyber security framework] ransomware profile to help organizations better understand which controls, policies [and] practices are critical for addressing ransomware,” he said. “Perhaps other profiles to address different threat types would make sense.”

Tom Badders, senior product manager also with Telos Corporation, added that the initiatives by the Biden administration and major tech companies “will clearly set the stage for rapid adoption and ensure that these standards are applied in commercial industries as well as within the federal government.”

At a minimum, information and security officers need the federal government to meet three primary objectives, Badders said: 1) continue to evolve the security standards through understanding evolving threats and developing mitigating technologies, practices and policies; 2) evolve standards that were designed specifically for federal agencies so that they also apply to commercial needs; and 3) use the newly announced partnership as a foundation for continued efforts with technology leaders—both those involved in the partnership and others

—“for a cooperative government-industry approach to solving this escalating problem of cyberattacks.”

Badders said that both revolutionary and evolutionary methods of protecting critical assets are needed. “Health care institutions are prone to cyberattacks due to the many requirements to connect remotely with patients, implement and integrate IoT [Internet of Things] devices for connectivity of critical information to their information network, and store highly sensitive patient information, just to name a few,” he said. “All of these requirements can potentially open attack surfaces for cyber criminals to leverage. There is no one-size-fits-all product or standard that can solve all these issues. Integration of multiple cybersecurity technologies into a solution that meets unique and varying needs is a goal that should be set for a way forward.”

Contact Shindell at rshindell@carosh.com and Gendre, Tracy and Badders via Erin Wise at wise@merrittgrp.com.

[1] White House Briefing Room, “FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity,” August 25, 2021, https://bit.ly/3mT3oiq.
[2] Ed Markey, “Senator Markey and Rep. Lieu Reintroduce Legislation to Improve the Cybersecurity of Internet of Things Technology,” news release, March 24, 2021, https://bit.ly/3DCoVPf.

[View source.]

Send Print Report

LATEST POSTS

- **Report on Patient Privacy Volume 21, Number 9. Privacy Briefs: September 2021**
- **To Combat Cyber Crime, White House Initiative Promises Tools; Some Seek Funding, New Laws**
- **[Event] Louisville Regional Healthcare Compliance Conference - October 29th, Louisville, KY**
- **[Event] Chicago Regional Healthcare Compliance Conference - October 22nd, Chicago, IL**
- **Hooper, Kearney and Macklin on Cutting Edge Topics in the False Claims Act** Audio

See more »

WRITTEN BY:

Health Care Compliance Association (HCCA)

Contact + Follow

PUBLISHED IN:

Biden Administration + Follow

Cyber Attacks + Follow

Cyber Crimes + Follow

Cyber Threats + Follow

Cybersecurity + Follow

Data Breach + Follow

Data Security + Follow

Electronic Protected Health Information (ePHI) + Follow

Funding + Follow

Hackers + Follow

National Security + Follow

New Legislation + Follow

more

HEALTH CARE COMPLIANCE ASSOCIATION (HCCA) ON: