Privacy and Cybersecurity: How Health Agencies are Navigating the Overlap

The two disciplines used to run parallel, but federal officials are finding themselves having to create the processes and policies that protect health data and systems.

Tue, 01/29/2019 - 23:39

Photo Credit: LeoWolfert/iStock

Advancements in technology and connected devices paired with constant data-breach attempts and the need to protect personally identifiable information have led to the overlap of privacy and cybersecurity, which is directly impacting federal health agencies.

The Office of Management and Budget released a memorandum in December for heads of executive departments and agencies to strengthen cybersecurity by enhancing the High Value Assets program, an initiative operated by the Homeland Security Department and created in 2015 directing agencies to identify their most critical assets.

DHS and OMB then assessed agency HVAs, resulting in the discovery of critical areas of weakness. The agencies plan to remediate those weak areas. The memo addresses enhancing HVAs with special attention to policies and processes for safeguarding PII.

Protecting health data is linked with protecting health IT, according to Servio Medina, branch chief of Cybersecurity Oversight, Governance, and Strategy at the Defense Health Agency.

Then there's the National Institute of Standards and Technology's second revision to its Risk Management Framework for Information Systems and Organizations released in December. According to Medina, NIST increased the number of occurrences of the word "privacy" from five in the first revision to more than 1,000 in the second, demonstrating the importance of privacy, and integration of privacy and cybersecurity.

So, following these documents and the interconnectivity of privacy and cybersecurity, health agencies are taking steps to integrate the two in their own practices and processes.

Role of the Chief Privacy Officer

At the Veterans Affairs Department, the position of privacy officer has been moved under the Chief Information Security Officer, according Paul Cunningham, VA CISO.

"The privacy officer works for me, but he has a dotted line to the [chief information officer]," Cunningham said at the Jan. 29 AFCEA Health IT Summit in Bethesda, Maryland, in a panel Medina moderated. "My goal is to provide him with an environment where he can be successful."

Part of that means ensuring that if there were an issue, the CISO and privacy officer would tackle it as partners, rather than compete for resources.

It's a mindset Cunningham observed at the Energy Department, where he served as CISO before joining the VA in January. “They were lining their privacy up with the CIO, and again, the CISO and the privacy officer see each other as true partners with a common goal,” he said.

At the Centers for Medicare and Medicaid Services, the current CISO seat is recently vacant, but the previous CISO also served as the privacy officer. “I see that as a good thing because in terms of who is the mitigator of decisions related to cybersecurity, it existed in the same person,” said Conrad Bovell, director of the Division of Information Systems Security in the Office of Financial Management at CMS, at the summit.

With this model, both cyber and privacy had to be considered in the decision-making process, considering both sides were within one person.

At the Health and Human Services Department, the privacy officer is looped into decisions as they are made within the office of the CIO.

“Our privacy officer was in the Office of the CISO, and in the last year, it was moved,” said Janet Vogel, acting CISO at HHS, at the AFCEA event. And while the position still falls under the CIO shop, Vogel said the privacy officer is brought in as HHS looks at all of its process improvement activities. “We’re looping privacy in as we go,” she said.

Medina said this variance of the position of the privacy officer is reflective of the overall cybersecurity and privacy integration process. “It’s not a cookie-cutter approach to managing risk, nor is it for the responsibilities of privacy,” he added.

But the roles of the CISO and privacy officers aren’t the only way agencies are tackling the overlap.

Integrating Security and Privacy

Cunningham has noticed through his previous positions in government and talks with cybersecurity professionals that as the maturity of cybersecurity evolves, as does the importance of privacy. And now, the VA is in a position, both from awareness of senior leadership and from policies being developed, that cyber and privacy are starting to align in a way that allows the VA to implement them both in a concerted effort, working together to champion goals on both sides and move forward. “And that’s what really needs to happen,” Cunningham said. “People have been striving for this.”

Being more compliance-focused also helped drive the interconnect between privacy and cybersecurity, which was previously challenged by risk. “That common lexicon helped us get passed that,” Cunningham said, and get passed the challenge and onto honest discussions.

Vogel said HHS is still struggling to bring privacy into cyber. She said they are very different perspectives, but have key commonalities.

“I think they’re pretty misunderstood,” Vogel said, in that cybersecurity seems scary unless you’re involved in it, then it seems even scarier. And privacy-driven people have been evangelizing the stress and importance of privacy for years, only for it to now have a strong spotlight.

“So we’re running these two things together, somewhat still in parallel, and we’re trying to merge them,” Vogel said.

Part of that challenge is HHS’ cyber fluency, as each discipline has its own language. Vogel compared this to software versus operations. “You’re not talking the same language if you talk software development, as when you’re talking to your operations and your hosting team,” she explained, “so we have to bridge that language gap all the time.”

HHS is trying to do this, in part, by merging privacy and security, and by building a common language that all disciplines will understand through published publications and guidance that anybody can apply and use, not just at work, but also at home. “Cybersecurity is everywhere. It’s everywhere you are,” Vogel said.

Focusing on High Value Assets

Bovell is in an interesting position for cyber and privacy, as the system he’s securing — the Healthcare Integrated General Ledger Accounting System — processes about $1.5 trillion a year. “So, there’s a tremendous amount of scrutiny,” Bovell said. “We’re in a constant state of audit.”

And with the system being an HVA comes an additional layer of scrutiny.

To ensure privacy and security, DHS executes an assessment of HVAs, which are “critical to maintain an unbiased view of the risk associated with maintaining an HVA,” according to the OMB memo. But Bovell said it’s not just a penetration test of the system, as it also goes after the agency.

“They will look at specific individuals within our organization and target those CMS.HHS.gov email accounts for the purpose of infiltrating the system,” Bovell said. The assessors are also provided with CMS accounts, so they can examine the structure of the system’s account management and maneuver within the system with privileges associated with those accounts. Then they execute the penetration test of the system, Bovell explained.

“For us, my team, penetration tests are wonderful training opportunities,” Bovell said, adding that it provides insight into what an actual hack attempt looks like, so CMS can begin to identify the activity and stop it.

Operationally, this thorough assessment is crucial. “You cannot look at a checkbox or a piece of paper and say that you are secure. You must have evidence that you have done things correct,” Bovell said, and this assessment provides that evidence.

Furthermore, it’s not a one-and-done practice and must be executed over and over again.

“When someone says, ‘Are you secure?’ My response is always, ‘Based on the analysis of the activity occurring in our environment, I see nothing consistent with compromise,’” Bovell said, “because we do not know today about successful exploits that exist in the environment.”

View printer friendly version
security
Health Human Services
Veterans Affairs
Health IT
privacy
Federal Cybersecurity