Governance, Vendor Partnerships & Frameworks: Leaders Share the Formula for Cloud Security

08/02/2023 By Kate Gamble

Sanjeev Sah, VP & CISO, Centura Health

In recent years, attitudes toward cloud computing in healthcare have shifted quite a bit. What was once viewed with a healthy dose of skepticism is now being widely adopted. In fact, as organizations dive deeper into digital transformation, the role of cloud services is becoming increasingly vital. "These solutions play a critical role in determining how quickly we can adapt, excel, and expedite our digital strategies," said Sanjeev Sah, CISO at Centura Health, in a panel discussion.

Of course, it comes with risks, which means leaders must "have a heightened trust and confidence in the efficacy, security, and resiliency of the service" in question, he added. "A thoughtful and programmatic approach is needed."

And a cloud strategy needs to cover all the bases, including selecting the right vendor, leveraging standards like HITRUST, ensuring proper safeguards and controls are in place, and forming a solid governance strategy.

During the webinar, he and co-panelists Michael Carr (CIO, Health First) and Andy Gilbert (Chief Revenue Officer, ClearDATA) shared insights into their own approaches to cloud security.

Governance: "Open Conversations"

First is the governance structure, which should facilitate partnerships between security and the business side, enabling the former to "provide input, advice and architectural decisions and standards that help shape overall decision-making." And that means having open conversations about how a presented idea might fit into the architecture and which security considerations need to be taken into account.

By being able to provide input, information security teams can "guide our business partners and colleagues" in a way that produces positive outcomes in terms of stability and resilience, Sah said.

Taking it a step further, Carr advised embedding engineers, technologists, and security professionals into the planning process with vendors. That way, they can help "influence the roadmap to make sure that as they're building out new functions and capabilities, they're not forgetting the security aspect," he noted. And "the earlier you get involved, the better."

Michael Carr, VP & CIO, Health First

Vendor Partnerships: Red Flags & Check-ins

Doing so, however, requires a strong vendor partnership, according to the panelists, who offered guidance on what to expect and where to draw the line.

- **Do your due diligence.** There's no shortage of cloud products on the market. And so, during the vetting process, leaders need to ask, 'Is it really a cloud solution or are you hosting this in someone else's data center?' according to Carr. The next question involves the level of security, which vendors may oversell. "Just moving to the cloud doesn't inherently make it any more or less secure." It's important to understand what type of service is being offered, and how it operates compared with on-prem solutions.
- **Joint accountability.** From the get-go, leaders need to establish shared accountability with vendors when it comes to protecting assets, he said. "When they're managing it, there's sometimes a penchant for people to say, 'Well, the vendor owns that.' No. We're still accountable, even if the vendor is managing it. We still have to assess them."
- **Prove it.** The same goes for auditing, noted Carr, adding that vendors sometimes fail to pick up the slack. "That's where a lot of them struggle," he said. "It's great that you have the certification, but show me that you have these controls." Sah agreed, noting that he has also seen vendors "struggle to meet expectations" when it comes to auditing.
- **Testing, testing, testing.** Another red flag is when vendors describe having a resilient architecture — with geographically diverse data centers and a full disaster recovery environment — but haven't tested it, noted Carr. "You might have one, but it's not effective if you can't prove that it actually works." Sah likened it to having an incident response plan, but never having conducted a tabletop exercise, which does little good when disaster strikes. "If you have one, please exercise it," he cautioned. "If you don't, put one together and conduct an exercise. It'll be a huge advantage when you need it."
- **Regular check-ins.** Through his decades of experience on the vendor side, Gilbert has found that one of the dynamics CIOs and CISOs value most in a vendor relationship is "having a regular cadence with them, whether it's monthly or quarterly, and a process for continually reviewing what's going on," he said. "They want to see that history."

To help busy clients that sometimes forget to flip a switch or two, ClearDATA's platform automatically does some remediation from a compliance perspective — such as if the encryption function wasn't turned on. It can also leverage its large client base (more than 250) to conduct threat intelligence and report back on industry trends, he added. "We're able to say, 'Here are three things that mattered in the

past month, and here's how we dealt with them. Being able to present analytics and show a continuous knowledge of what's going on is very valuable for our clients."

Frameworks: "An ongoing presence"

Another important component of cloud security strategy is compliance with frameworks such as HITRUST, which is particularly critical for organizations that handle sensitive patient information and must adhere to strict regulations, according to the company's website. Through its CyberHealth Platform, ClearDATA generates report mapping to HIPAA controls and requirements, and enables customers to inherit around 60 percent of the 545 requirements.

And Sah is high on HITRUST, saying, "it gives us confidence that the organization is capable of handling all aspects that are important from a security, privacy, and compliance perspective." Having HITRUST certification, he believes, helps ensure that periodic assessments are happening. "We need an ongoing presence of safeguards and controls and how effective they are," he noted, especially as the landscape continues to shift. "Environments change. Architectures change. People, processes, and technologies change."

Andy Gilbert, Chief Revenue Officer, ClearDATA

And an outside eye can't hurt, especially when some vendors just add security to the application developer's to-do list, rather than focusing unique resources on the issue, according to Gilbert. "Oftentimes it's application developers who are saddled with this. They don't want to deal with that; they want to focus on their day job."

As for the health system side, Carr says it's important that no one become so mired in the "daily grind" that they lose sight of the big picture, said Carr. "It's continuing to have the right data and analysis from endpoint detection and response tools to ensure you're protecting against new threats." At the same time, CIOs and others need to continue to have "a thoughtful approach to build it right, execute, and periodically check to make sure those things are being done," while also keeping up with the demand of users — both inside and outside of the organization — and developing analytics. "Those are the best practices we see."

It may seem like a lot, but for IT and security leaders, that's the reality.

"At the end of the day, you need a thoughtful, methodical process that gives you the courage and trust to adopt any new technology, including cloud services," said Sah. "That's what we're all looking for."

To view the archive of this webinar — Strategies to Secure Your Move to the Cloud (Sponsored by ClearDATA) — please click here.