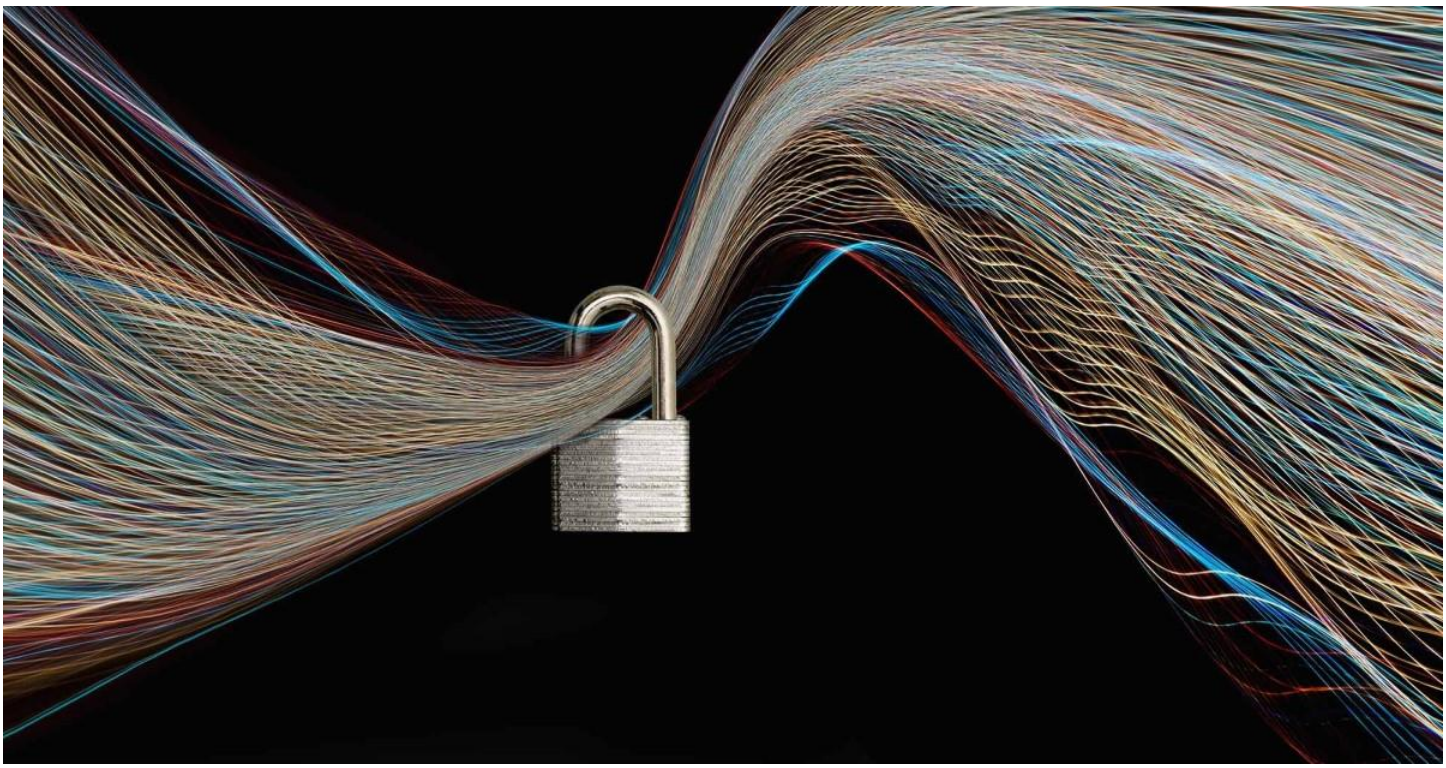
Healthcare IT News

CIOs describe their cybersecurity investment plans for the next 5 years

Six health IT leaders lay out some of their security strategies as healthcare continues to be a prime target for cybercriminals.

By Bill Siwicki December 01, 2021



Healthcare C-suite executives do not need a PowerPoint presentation from the CISO to understand that cybersecurity should be a top priority for healthcare provider organizations today. They just need to read all the headlines of security breaches at hospitals across the country. But are they doing so?

Nearly a third of hospitals and health systems are planning to implement biometrics (29%), digital forensics (28%) or penetration testing (28%) within the next 24 months, according to new HIMSS Media research. (HIMSS is the parent company of *Healthcare IT News*.)

However, 43% say funding is keeping their organizations from executing on security challenges they have, the research shows.

This is the fourth installment in *Healthcare IT News'* latest feature series, "Health IT Investment: The Next Five Years." This fourth feature focuses on cybersecurity.

The series offers interviews, mostly with CIOs, to learn from them the path forward through the priorities they set with their investments in six categories: AI and machine learning; interoperability; telehealth, connected health and remote patient monitoring; cybersecurity; electronic health records and population health; and emerging technology and other systems.

Click here to access all the features currently available.

The five CIOs and one COO discussing their plans for the next five years in this installment include:

- **Cara Babachicos**, senior vice president and CIO at South Shore Health, a health system based in Weymouth, Massachusetts.
- **Matt Hocks**, COO at Sioux Falls, South Dakota-based Sanford Health, a $6 billion health system serving a predominantly rural population over a four-state footprint with both payer and provider arms.
- **Mike Mistretta**, vice president and CIO at Virginia Hospital Center in Arlington.
- **B.J. Moore**, CIO of Providence, a health system that operates 52 hospitals across seven states – Alaska, Montana, Oregon, Washington, California, New Mexico and Texas.
- **Michael Restuccia**, senior vice president and CIO at Penn Medicine in Philadelphia.
- **Dr. Umberto Tachinardi**, CIO at Regenstrief Institute in Indianapolis.

'A tremendous amount of money'

"Cybersecurity is ever-changing as new technologies and threats emerge," said Mistretta of Virginia Hospital Center. "We have spent a tremendous amount of money in the past two years hardening our defenses and filling gaps so we are compliant with best practices.

"The interesting thing on this front is now the insurance companies are getting involved, dictating specific security capabilities be in place in order to provide any type of cyber coverage," he noted. "In our last renewal, we had to fill out an extensive survey from three separate companies just to receive quotes."

"We have spent a tremendous amount of money in the past two years hardening our defenses and filling gaps so we are compliant with best practices."

Mike Mistretta, Virginia Hospital Center

The organization also had to focus on a workforce transitioning to a home setting, so it enhanced network traffic monitoring to assist in early identification of a potential breach.

"Our leadership has been extremely generous in funding these efforts over the past few years, as we have had several local healthcare entities locked offline due to ransomware that raised the risk profile for the organization," he explained.

In the next few years, Virginia Hospital Center will invest in cybersecurity as needed to stay compliant with insurance; the organization is comfortable with current investments.

"I see our next investment related to this to focus more on recovery in the event a breach were to happen," he explained. "Currently we are investigating immutable backups to the cloud with either Azure or Amazon that will provide a layer of insulation between our current systems and a reliable restore point should it ever be needed.

"For us, selling these investments to our board has been relatively easy: The news cycle has been able to convey other healthcare entities near us that have been breached, so it lightens the justification requirements," he added.

Healthcare IT News is a HIMSS Media publication.