PROFILES IN *Confidence*

# MATT SHAW

## CISO
## Southcoast Health

**Headquarters:** New Bedford, MA

**Employees:** 8,100

**Annual Revenue:** $1.5 Billion

Matt Shaw didn't begin his career in cybersecurity, he shares. "I started out in banking, many years ago, basically as a bank teller," he recalls. "I was working as an accounting manager, and the bank was notified they needed to move to a new data processor. With no dedicated IT staff, I saw it as an opportunity and managed the data conversion project." That decision launched a new career in technology.

What began as a foray into IT during a systems migration in the early 2000s evolved into a full-fledged career in security leadership. "In banking, it's very regulated," he explains. "You're dealing with federal examiners, a lot of oversight, and that always kept security top of mind; even in an IT role."

Over time, Matt moved into fully dedicated information security roles, eventually taking on larger responsibilities across financial institutions before transitioning to the healthcare industry. Today, he is the CISO at Southcoast Health, a not-for-profit health system that serves communities across southeastern Massachusetts and Rhode Island as the largest provider of primary and specialty care in the region.

"Going from banking to healthcare was a significant change," he says. "Although the basic concepts are the same, the mission is very different. It took a while to shift from protecting customers' personal information and money to protecting patients' private health data and the systems that care for them."

### NAVIGATING THE GRAY AREA OF HEALTHCARE SECURITY

That industry shift revealed stark differences in how cybersecurity is applied. "Banking is very black and white, and rigid in terms of regulation," Matt explains. "Healthcare is more complex, there are more gray areas. Data flows, patient care systems – it's all interconnected."

The complexity of protecting electronic health records and clinical workflows shaped Matt's leadership style. "It's not just about technology and security. You have to build relationships across the organization," he says. "People need to see you as a resource, someone who helps them find solutions that support the business securely."

### LEADING WITH RESPECT AND VISION

Matt's leadership philosophy centers on empathy, accessibility and mentorship. "I do tend to lead by example, especially in how I treat people," he says. "Security teams are sometimes seen as blockers to business initiatives. I want my team to be collaborative, supportive and respectful. I want colleagues across the organization to see the security team as a resource, and to reach out with any questions or problems, so we can provide them with secure solutions that support their needs. At the end of the day, we rely on employees' awareness and vigilance to help keep us secure, so we need to maintain good relationships and be seen as a partner."

That also means investing in his team's growth. "We're big proponents of promoting from within. Whether someone's going the technical route, such as an engineer, or into a less technical GRC role, I try to support them and provide career paths that keep them engaged."

He's also hands-on by nature. "Sometimes I'm in the weeds more than I should be," he admits. "But being a smaller team, I think it helps to stay close to the details."

### BUILDING A PROGRAM

In recent years, Matt's team has invested heavily in top-tier security tools. Now, the focus is shifting toward optimization. "The next 12 months is all about further leveraging the tools we've implemented, and maturing the program," he says.

He's especially wary of overlapping functionality. "The number of security products available continues to grow

very rapidly, as does their functionality. We try to be selective and minimize tool overlap. Making sure we get the most out of our products helps the team be more efficient with fewer dashboards and more focused attention."

The goal: reduce redundancy, tighten integration and ensure engineers aren't spread too thin. Having too many consoles and not enough eyes on them is not efficient and increases the chances something gets missed.

## IDENTITY, INTEGRATION AND THE QUIET RISE OF RISK

One of Matt's top concerns is identity. "There's a lot of risk in identities – especially as systems become more integrated," he says. "Conditional access, behavioral analytics – these are must-haves."

With cloud-based platforms like Microsoft 365 becoming ubiquitous, he sees threats increasing. "Office 365 is one of the most phished platforms out there. So, it's about having systems that know the baselines of normal user behavior and alert us when something's off and atypical activity is detected, indicating a user account may be compromised."

He's also focused on increasing awareness of how attackers evolve. "Although phishing has been around for many years, it continues to be a huge risk. Attackers are using AI to enhance their efforts and look more credible, and they are constantly evolving their tactics to improve their chances of success. Keeping folks aware of emerging threats and tactics is an important part of helping to keep our employees safe."

## AWARENESS OVER ASSUMPTIONS

Matt's team is moving toward more targeted, role-specific awareness training. "Someone in accounts payable is going to get different threats than someone in HR. So why give them the same training and phishing tests?"

That tailored approach is designed to reduce fatigue and increase engagement. "It's about awareness and training opportunities; it's not about punishing people for clicking on a phishing test. The goal is to help them understand the risks and why vigilance is important."

In healthcare, he adds, the stakes are too high, and one-size-fits-all approaches aren't as effective. "There are certain groups of staff who may use email only once a day, and they're just as likely to be targeted. So, we try and layer controls to limit exposure and minimize impacts if they fall victim to a phishing email."

## THE HIRING DILEMMA: SKILLS AND SOFT SKILLS

Matt acknowledges the industry-wide challenge of hiring. "The biggest challenge for us is people. It's always hard getting enough of them and finding the right mix of experience and soft skills."

He's looking for a balance. "Having the technical skills is essential, but our team members also need to collaborate and support the employee population. Within our department, everyone is employee-facing, so we can't afford to have someone with poor interpersonal skills. It's not good for the organization, the team, or how we want to be perceived by the organization."

Certifications are also part of his team's DNA. "When I started, I was the only one on the team with industry certs. Now, almost everyone on the team has at least one. Although certs are not the ultimate determinant of someone's tech skills, they demonstrate an understanding of specific security concepts, and help keep employees in sync with industry changes due to the need for Continuing Professional Education (CPE). We support them in getting certified and keeping up with CPEs."

## ON BUZZWORDS AND BURNOUT

Ask Matt which buzzword he'd like to retire, and his answer is simple: AI. "With AI in the forefront these days, every product seems to tout AI functionality, but it's often older technology rebranded for today's marketplace and not really AI. It's overused and often misused."

And while AI certainly does play an increasingly important role in security and technology, he warns against overreliance on hype. "With everything claiming to be AI, it's important to make sure you know what you're getting, that it meets your needs, and that it works as advertised."

## INVESTING IN THE FUTURE – PEOPLE FIRST

For Matt, building a strong program isn't just about the right tools, it's about people. "At the end of the day, we're a support organization for Southcoast Health. We're here to protect the organization, and that starts with helping people do their jobs securely."

He stays current through a steady diet of news feeds, peer groups and vendor conversations. "Our security partners are great resources, and we value our relationships with them; they see a broad landscape. We're in constant dialogue, not just when we're looking to buy something."

In a complex, fast-moving field, Matt keeps his focus simple: "Be collaborative. Be curious. Be clear. That's how you move security forward."