PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TIM SWOPE

CISO, Catholic Health Services Long Island

HEADQUARTERS: Long Island, New York

EMPLOYEES: 18,400+

ANNUAL REVENUE: $2 billion

> “An advantage of my consulting background is that people who are in an organization for a long period of time, might not see the whole picture. My entire career, I’ve been on the outside, so I see the whole picture a little bit better than others.”
>
> - Tim Swope

Currently the CISO of Catholic Health Services of Long Island (CHSLI), Tim Swope’s career stands out due to his lengthy experience consulting and partnering with healthcare organizations in a wide range of strategic roles. While many CISOs come up the ladder through promotions in their respective security roles, Swope’s consultative background has enabled him to consistently interact with C-levels and department heads. These include working with multiple executives from the finance department, HR, application development, and many others. He says, “An advantage of my consulting background is that people who are in an organization for a long period of time, might not see the whole picture. My entire career, I’ve been on the outside, so I see the whole picture a little bit better than others.”

Beginning his career in business intelligence and data analytics for pharmaceutical companies, Swope recognized how his projects were rapidly evolving to include information security components. This included when he began identifying ways to provision people and put in the right security controls. He then started working as a consultant for New York-based hospitals. Swope says, “Across the board I want to make sure these hospitals all have the same security controls for patient safety and patient privacy information. Not being a doctor, I’m agnostic as to where they go. I don’t care where they go, but as a patient that comes into any of the hospitals I interact with, I want to make sure their privacy is the same throughout.”

Coming into CHSLI, Swope began working with their newly appointed CIO on key initiatives including ensuring the hospital could pass a DOH audit in six months’ time, something that had not been conducted before. He comments, “The biggest challenge was right when I came in, they were under federal requirements. There’s this program called DSRIP, where hospitals get paid for giving better service, reducing emergency room visits by certain percentages for Medicaid patients, etc. To do that, they had 402 security controls that had to be verified, tested, and documented across the organization. And they didn't have them." Swope also addressed specific policy and procedure issues and implemented risk management programs that were not previously in place at CHSLI.

MOVING AWAY FROM SECURITY AS AN AFTERTHOUGHT

Whether it comes to digital transformation or engaging in a new project, Swope believes security should never be considered an afterthought. He strongly relies on empowering executives with information and knowledge that validates the need to include security in all strategic discussions.

As a healthcare leader, Swope understands the strong impact digital transformation has on the industry and he continues to ensure security is baked-in all cloud decisions from the start. One challenge he recognizes is the need to sometimes take vital time during decisions to ensure nothing is implemented unless he can guarantee it can be done securely.

Swope says, "Digital transformation is a big impact. A lot of our services are cloud-based. We also have clients who require a certain type of information that will go into a cloud area so that they can retrieve it easily. Over one third of the security controls from the National Institute for Standards and Technology for federal systems, which covers the Department of Health, are based on cloud security. So that's really changed the landscape a lot."

In organizations where security may be an afterthought to project decisions, Swope emphasizes the importance to mandate security as a core component. In his experience, to guarantee security is part of key considerations, he encourages strong secure development lifecycles and data distribution lifecycles for all vendors and healthcare professionals. He initially implements a security review, so no project gets approval until a thorough security assessment is completed. Once a vendor passes, or after necessary remediation takes place, only then can they get approval to move the project forward.

FOCUS ON RISK MANAGEMENT LEADERSHIP

While many security leaders focus on cybersecurity, Swope focuses his programs on risk management. He explains, "Risk management is the overriding thing for cybersecurity because, let's say you have the cybersecurity tools, right now, they'll tell you what happened. You can do a lot of anomalous behavior analytics and it'll tell you what's happening, but only through risk management do we identify the security risks upfront before anything happens, and then we remediate them before they're a problem. I spent a lot of time with clients and hospitals looking at what could be a risk in the future, like medical device security, things like that. And rather than attacking it with software, we look to remediate a lot of those issues before they even happen."

When coming into a new organization as a CISO leader, Swope strongly believes in conducting an internal assessment to get an understanding of what controls and technologies are in place. While some CISOs may rely on an outside firm to conduct these, Swope chooses to do them himself, putting himself in an outside auditor's shoes. He says, "So rather than looking at somebody else to do it for me, I'll do it myself and I think that's the key thing a CISO should do, is understand his or her landscape and do their own personal assessment and only then can you see what you really have. That's the only way to get a good feel of it, by doing it yourself. That's the biggest hands-on thing a CISO should do in the first couple of months."

Swope strongly believes in starting cybersecurity governance councils within organizations bringing together the board of directors, CIO, head of audit and compliance and any other key executives. He explains, "I bring them all into the conversation and let them know that if they look at security first, it won't hold up these projects, but they actually do have to be a piece of the plan. I let everybody know what our plan is long-term. So, it's not a surprise to them because a lot of people really don't know what information security does and they look at it as a detriment to their progress, not an enhancement."

The Need for Virtual CISOs

Due to the salaries skyrocketing for New York CISOs, Swope believes the option of virtual CISOs may become normalized. He says cost is one of the key benefits, with New York CISOs average salaries around $400,000, something not all hospitals can afford.

He explains, "The advantage of a virtual CISO, is there are a set of federal requirements that govern hospitals, and this is just with security. All of these hospitals have the same requirements. So, the value I bring to one is the same that I bring to the other, and they could share the cost. The reason why the cloud is so cost effective is because you're sharing it with other companies. It's the same sort of thing. They're going to share me with others. It's got to be the same industry, the same size entity. So, it would be, let's say three hospitals the same size as Catholic Health Services. I could officially do those because the type of attacks, vulnerability requirements, they're all the same. Let's say there's a huge incident at one or you need to enact a disaster recovery at one without the others. That's when you rely on the team and you have to build a very good team under you. It's like a coach of 11 players on the field. They're all doing it. I'm telling them how to do it."