TIM SWOPE

CISO
CATHOLIC HEALTH

HEADQUARTERS: Rockville Centre, New York

EMPLOYEES: 17,000+

REVENUE: $3 Billion

For over three years, Tim Swope has worked as CISO for Catholic Health, an integrated health care delivery system in Rockville Centre, New York. As a security leader, Swope focuses on identifying gaps related to key IT security processes and the implementation of information security and risk management.

With over twenty years of experience, Swope understands the connection between productive, proactive security programs and business priorities. As a seasoned leader, he emphasizes the importance of strong communication with business leaders and executives in all departments of an organization. In this profile, Swope shares his thoughts on the progression of CISO responsibilities and valuable advice for other leaders.

EVOLVING CISO RESPONSIBILITIES

Swope says CISOs must constantly adapt to changing business environments, especially in healthcare organizations which have seen dramatic shifts in digital transformation, remote workforces, the internet of medical devices, and more. Swope says responsibilities that fall under CISOs are not just data security related anymore, they have grown to include patient privacy and safety.

He explains, “In the post-COVID world, people are going to start seeing that there’s a patient privacy initiative. In other words, who can tell if you’re securing these records? Did you get your vaccination? Did you have COVID? Those sorts of things are very big issues because of the patient privacy initiative. And that’s from a healthcare standpoint, part of the CISO’s initiative. But also response to threats. We have to do as much as we can do proactively, but a lot of companies have been attacked by bad actors with ransomware. You also have to prepare yourself with your response and how fast you can get your system up and running and get back to daily operations.”

Another area CISOs must adapt to is changing budgetary issues, especially as new government directives emerge, requiring organizations to implement or change existing policies, technology, or other areas of investment. While these types of government directives are beneficial to continue to increase the security of organizations, security teams must then reevaluate their budgets and organize accordingly.

Digital transformation is also impacting CISO responsibilities, and Swope says, “There’s been some studies that, especially millennials, are very into the wearable technology, so you can have proactive healthcare. Such as - what’s my heart rate today, what’s my blood pressure, am I eating healthy, getting enough exercise? These go into a medical record where a healthcare provider like us can analyze them. So the digital transformation expands our ability to give help.”

He continues, “Also, the potential attack surface has expanded

by more than a hundred-fold. So as we've moved from the confines of our productive, traditional, and safe walls, now you have more outwardly public facing websites, applications, and ways to interact, be it zoom, digital, or other ways. And that opens up an attack surface for you that you never had before. So these are some areas of concern that a CISO now works with and is defining. When you look at those initiatives, is it something that we can secure and do we have the funds outside of the project to do that?"

TOP FOCUS AREAS

Protecting endpoints is a top area of focus for Swope, because as the hospital system grows, more endpoints emerge that require protecting. With an influx of outside medical devices being dropped off to patients' homes, security must adjust and set strong protective measures. He comments, "You must make sure that our remote staff and now our remote vendor endpoints are protected. Imagine all the vendors, consultants, and service providers we have who all sent their workforce to work remote. So when we certify a vendor for a risk assessment, now they just went outside their own area that we conducted the assessment against. Those are some big concerns over the next 12 months. And they'll continue to be."

Another concern for Swope is the uptick in daily requests for data related to COVID patients. Accessing and protecting this data requires security resources, and he is working hard to find easier means to get this type of information to the right parties.

SECURITY PROGRAM STRUCTURE

Establishing a proactive and diligent program is paramount to Swope, and he has organized his team to address key cybersecurity areas. The cybersecurity governance group has direct control of future and current information security and new systems. For any new systems coming in, his team has comprehensive oversight into them. They also have a strategic planning function for not just security, but also for infrastructure and architecture, another crucial group within his program.

He explains, "Under my cybersecurity governance group, we have our infrastructure and architecture group, which includes networking. We make sure from a top-down level that anything that's put in follows certain requirements for security or privacy for architecture and how data is set up and the like. Then those we can actually manage, there's the audit functions."

He continues, "Then we have the policy and procedure lifecycle, that's big because those touch everything from security, privacy, infrastructure standards, architecture standards, and how that information is disseminated within our entire corporation. That would also include corporate risk management, IT risk management audit functions, strategic planning, and risk management for patients."

> *"Identifying what the priorities are and making sure that you're picking the right ones is an ongoing exercise. Especially with the rapid evolution of threats, something that may be low priority today might become really important tomorrow."*

INVESTMENT AREAS

Along with increasing their footprint for endpoint security, Swope and his team plan to put significant investments in Privileged Access Management. They currently have remediated all the privilege access to a point where they have a strong benchmark, but with a standard amount of employee turnover, it continues to be a challenge.

With patients being seen outside of hospital walls, Swope plans to investment in Identity and Access Management solutions to address these concerns. Patients are now accessing their information from their phones, tablets, or other devices, and security must keep pace with ensuring only the patient themselves are accessing that data.

From a proactive standpoint to address ransomware attacks, they are planning to invest in a secondary data disaster recovery. He comments, "People have offsite applications, but we are literally creating a mirror image of our site and air gapping it, so if we do have a ransomware attack, then I'll have a mirror image that's up to date and can be turned over rather than backing up what we've got from backups. I'll flip a switch and we're up and running within 15 minutes on the total shutdown. That is a significant investment. It's one that most people can't make. These are some of the methodologies I give seminars on, how you can stop ransomware attacks or help yourself afterwards."

By focusing on proactive risk management, Swope hopes to identify risks in the organization before they happen. Swope says if you can identify the danger first, you have the opportunity remediated. He will focus on looking proactively at what they can remediate and protect before something happens, while monitoring everything else. He explains, "Some people are looking for a methodology to protect them. I can't give them one that's one hundred percent, but I can give them one that puts them on that journey. That comes from first, identifying the risks that you have, and then looking at the criticality of them as attack factors, then putting in some strategy to remediate those while monitoring everything else."