

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
LEADING THE WAY FOR
CONFIDENT SECURITY
PROGRAMS



JEREMY WALCZAK CISO, CATHOLIC HEALTH

HEADQUARTERS: Buffalo, NY

EMPLOYEES: 9,000+

ANNUAL REVENUE: \$1.1 Billion

Jeremy Walczak, currently the CISO of Catholic Health, exemplifies a security leader with a unique, business-oriented background. Walczak studied Marketing at the University of Buffalo, and through a recommendation from a friend, he also completed his Management in Information Systems degree.

When discussing his undergraduate degree background in Marketing and Management of Information Systems, Walczak says, "I find these degrees to be very valuable in the sense that it helps with communicating, relating, and selling IT and information security needs to others in the business."

After spending several years living and working in Dayton, Ohio for NCR Corporation where he obtained his M.B.A. from The University of Dayton, Walczak returned to Western New York and worked at Delaware North, a global food service and hospitality company, where he had his first exposure to working in information security. He says, "It was more of a compliance focus at the time in the sense that we were marching toward adhering to PCI guidelines. Those were our drivers, but that's how I first got into a formal information security role and started branching away from traditional IT. It is not because I necessarily chose this path, it was more making myself available and relying on the skillsets I had developed earlier on to point me in this direction."

After moving on to Independent Health, a health plan

and services organization, Walczak spent the next eight years working his way up from Security Architect, to Director of Information Risk, to eventually becoming their Chief Information Security Officer. During his time at Independent Health, Walczak strategically established a link between the work his team did from an information security perspective to ensuring they comprehensively enabled customer trust. He comments, "That was our value proposition, to enable customer trust. It was the strategic angle about making our consumers feel comfortable working with us. And the moment we break that trust is when there are dire consequences or events that may potentially lead to more costly healthcare."

Early on in his career, Walczak was told by a former business mentor to find a way to get out of IT in order to leverage more of his business skills. In his role at Independent Health, he had the opportunity to interact with other business leaders to a greater extent because his role was not as heavily focused on the management of technology. He grew in terms of understanding how the business operated, what the business needs were, and then translating this back into technology or security solutions. The heavy focus was more on risk management, something Walczak regards as a formative transition in his career.

BUDGET, PRIORITIZATION, AND ALIGNMENT

Walczak has almost one year under his belt as the CISO of

Jeremy Walczak's Thoughts on IoT

"I think IoT is interesting. I look at medical devices as our IoT here, in the sense that we have our traditional server farm, we have our workstation, we have our WiFi, but then you've got this whole other area of connected wired and wireless medical devices that are out in our facilities, and it's something that you have to be very careful and deliberate when you go out and attempt to affect these devices from a security perspective. The last thing you want to do is interrupt operations or services at a critical point of care. That's a whole area of risk that can go well beyond traditional infosec risk as it also can have a significant operational risk. How do we manage that smoothly? It brings in a whole other subset of leaders within the organization, which is new for me when you compare it back to my time in manufacturing, travel & entertainment, or health insurance."

Catholic Health, a comprehensive healthcare system based in Buffalo, New York. Walczak viewed the role as an opportunity to join a larger organization with more responsibility. He explains, "Fortunately, I stepped into an area and to a company that had already accomplished a great deal in terms of the security program. However, there's certainly a lot left to do, whether it's standing up new capabilities and technologies or continuing to mature what we have in place today. So, I'm excited to do that. For me, it was time for that new opportunity."

Before joining Catholic Health, Walczak ensured he would receive sufficient budget, be aligned with the prioritization process, and have strong alignment to other leaders. To kick start the inherited program and maintain a strong security standing, he chose to focus on a few key, high-level priorities. He says, "What I found to be successful in the past, is coming into the year with three high priority things that I'm expecting to get done. I'll always have three, four, or five other scenarios or solutions thought through in my back pocket because what I've found is depending on what external events or circumstances unfold throughout the year, I may be presented with other opportunities to react with dollars that were not previously budgeted to solve an emerging threat."

THE KEYS TO BUSINESS ALIGNMENT

To ensure strong alignment with other executives, Walczak believes in finding ways to become indispensable to an organization. He does this through being willing to help business leaders solve challenges and offer a helping hand to those in need. He comments, "I try to find out how I can help. Something I picked up early on in my career is figuring out how to become indispensable by being willing to jump in and work to solve other people's issues. It might be working with the CIO on a key technical challenge, or it could be helping to push basic process improvements that have been waiting to be completed for some time." Walczak tackles challenges such as this by understanding if there are any security barriers inhibiting this, or if there is anything that can be done from a security perspective in order to overcome the other person's challenge.

By approaching board alignment in this same manner, Walczak believes CISOs may become more valuable through building strong trust, and focusing on continued engagement and communication. He explains, "There is a difference

between management and oversight. I truly believe that executive leadership has a responsibility and accountability to manage day-to-day operations. However, you must find the right level and the right type of detail to ensure your board is appropriately and reasonably informed of the issues you are managing. And you've got to find the right balance. You need to do your job as a manager, but then the board also has to do their job and ensure they've been properly informed and can validate the decisions that you have made. I try to do that through risk indicators, performance indicators, as well as the right type of dashboarding, so to speak."

MAPPING BACK TO STRATEGIC GOALS

Walczak leads his security program with the core strategic value of continuing to map and mature to their adopted framework and ensuring all information security objectives map back to Catholic Health's strategic goals. He believes everything his team does, no matter the project scope, must tie back and support the organization's end goals.

In order to continue to accomplish this goal, Walczak must overcome challenges related to funding, prioritization, and entrenched business processes. He discusses why prioritization and entrenched business processes pose unique challenges to his strategic goals and growth. He says, "Group think can be dangerous. It can maintain certain entrenched customs that may not add value and it's those customs that you're now competing with for dollars and resources. This is where a good risk management process can come into play to help bring visibility to an organization's evolving risks and lead to improved allocation of resources and funding. This is important because you can't boil the ocean."

He continues, "For prioritization, that's where a couple of things can come into play. It is where your risk assessment process and mapping to a framework and then building out a maturity model are important. So, if I'm the lowest level on my maturity model and I know through whatever risk assessment I'm doing, it points out that "XYZ" is a significant issue, you can then begin to have a more data driven discussion around highest risk and prioritization of effort. It also comes down to what's tolerable from an organizational perspective. How much change can I inflict in one fell swoop or in one calendar year to move the needle for the organization."