PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

JIM DIDONATO
CISO, BAYSTATE HEALTH

HEADQUARTERS: Springfield, MA

EMPLOYEES: 12,000+

ANNUAL REVENUE: $2.1 Bliion

FROM HIPAA COMPLIANCE TO THE HITRUST CSF

Jim DiDonato has worked at Baystate Health, a large healthcare organization in Massachusetts, for over twenty five years. During DiDonato's early career, he worked twenty years in internal audit where he audited taxes, financial forms, IT controls, and many other areas. Just prior to 2000, he made the switch to IT where he filled the first security position at Baystate Health. While his first large project consisted of contingency planning and efforts to meet the Y2K challenge, DiDonato quickly transitioned into preparing the company for HIPAA. "HIPAA was really instrumental for me, and everyone in the industry, because it gave us a path or roadmap to create the organization's first comprehensive security program," said DiDonato. He continued, "Of course, that was back when security was based on compliance and not best practices." The industry and DiDonato have changed paths since then.

In 2001, DiDonato was named Information Security Officer at Baystate Health, a position mandated by HIPAA. With that title, his role and responsibilities evolved and again in 2015 when he was promoted to Director & Chief Information Security Officer. He recognized that more could be done to build out a stronger security posture. "Three years ago, a new CIO came on board and I proposed a change in our security program. I explained that a targeted HIPAA compliance program was not sufficient to cover information security for Baystate. We were both in alignment that we needed to find another security standard to adopt."

"We make a good team," said DiDonato, of his relationship with the CIO. "He supports my requests and he has the support of senior leadership. We have made significant changes in the last three years. Before, there were two of us doing information security for the organization and today there are six of us, with plans to hire two more this Fall. The President and the Board are showing their support with staffing and the resources to acquire the security technology tools we need to build out the program. "

DiDonato and his team have aligned with the HITRUST Common Security Framework (CSF), which is designed specifically for the healthcare industry. The HITRUST Alliance website describes the CSF as a "certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management". HITRUST was chosen by DiDonato, because the framework is designed specifically for healthcare providers and payers, is frequently updated for regulatory changes and has three levels of graduated safeguards depending upon an organization's size and complexity.

"Before we adopted the CSF, we had a security assessment done, so we knew what we needed to accomplish. We set a baseline and now we know that we are gradually elevating up the maturity ladder. The ladder gives us a grading system to make it very clear how we are performing," said DiDonato. For him, the CSF ladder represents a tool to easily communicate information security and risk to other business people. "We can clearly articulate our current level, the steps needed to get to the next level, and how getting to the next rung makes us better prepared and more secure."

DiDonato said that nearly every CISO knows how well prepared or exposed their organization is, but it may be difficult to explain current postures to business people. "Pictures help – the ladder gives a clear indication of where we are, and where we are headed. Our plan for this multi-year effort is to continue to execute on security priorities to move up the ladder."

DiDonato benefits from a very supportive CIO, President, CEO and Board, who are all interested in making continued security improvements. He continues to rely on the CSF within his presentations to senior leadership and the Board. DiDonato said, "They are very receptive to the CSF and they understand the value of aligning with the framework."

DiDonato's meetings with the Board are not just presentations of the CSF. He said, "The Board does not want to see detailed flow charts or diagrams of networks. They need to understand the security program from a business perspective. I build credibility with them by explaining security's impact on the things they care about." They are outcome oriented. For example, DiDonato recently presented on the opportunity security has to become a competitive advantage for the organization.

COLLABORATING ON SECURITY OUTSIDE OF IT

At Baystate Health, interest in security extends down from the Board throughout the entire organization. Senior leaders, including the General Counsel and the CFO, stay engaged with DiDonato. "Our CFO is concerned about the potential financial impact of breaches and incidents, so he purchased cyber insurance as a way to manage that risk. His group has been targeted for wire transfer fraud, but they are an alert group and always investigate first. Our General Counsel is always sharing phishing scams, news of viruses and regulatory alerts with me."

DiDonato believes that working with others outside of IT is both a big challenge and great opportunity for CISOs. Bringing other business units on board with information security efforts is vital to the program's success. "It is the CISO's responsibility to interact and communicate with leadership and people outside of IT," said DiDonato, whose early career in auditing gave him an understanding of business terminology and objectives. DiDonato acknowledged that for CISOs who grow up in IT, collaborating with other departments might pose bigger challenges.

DiDonato acknowledged the fact that information security is relatively new to many departments, with little to no historical precedent for collaboration. "Most departments have no idea how they can best help us. We need to educate, and reach out to them, to set expectations for our role and how we can work together," said DiDonato.

In the Information Security Office within Baystate, DiDonato puts in a strong effort to ensure his own team understands how meaningful and key their job is to the overall organization. He said, "One way I do that is by removing barriers for them. I show them we are getting the resources to make the program stronger. I depend on the professionals on my team to put together criteria for the technology resources that we need and then I go get it for them."

Baystate Health continues to make investments in information security, enabling DiDonato's team to grow and further advance their skill sets. "When they have the chance to learn new technologies it is exciting for them. When we give them tools and resources to do another level of investigation and analysis of incidents they are intrigued and motivated," said DiDonato.

This on-the-job-growth is an important aspect of DiDonato's team management approach, as he has almost exclusively hired from within. "My approach is to identify true professionals who take their jobs seriously and are dedicated and interested in security. Most of my hires have shown a dedication to security even before they join my team, by sitting for the CISSP certification, for example." However, DiDonato did not rule out looking outside of the organization for his next two hires to bring on more advanced security expertise along with unique skill sets. It will depend upon the skills of each hire.

Regardless of who joins the team and the specific skill set they bring, the group already knows it has a clear focus and strategy for the future – to continue to climb the HITRUST CSF ladder and further evolve the security program for Baystate Health.