PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

KEVIN BROWN
CISO, BOSTON SCIENTIFIC

HEADQUARTERS: Marlborough, MA

EMPLOYEES: 24,000

OPERATIONAL REVENUE: $8.1 Billion

"I have strong knowledge and experience in cybersecurity, but I also have a business background, managing significant cybersecurity profit and loss portfolios," said Kevin Brown, CISO at Boston Scientific. "That combination helps me make a difference in the CISO role at Boston Scientific."

Brown started his information security career with the Federal Government as a U.S. Navy officer where he worked with the National Security Agency. After leaving the Navy, Brown was an early member of SAIC's startup information security division, where he spent seventeen years growing the business unit to $180 million in annual revenue. As a Senior Vice President at SAIC, and later Vice President at Raytheon, Brown was responsible for profit and loss organizations providing information security services, technologies, products and consulting to federal government, commercial and international customers, particularly in support of CISOs.

After twenty years into his commercial information security career, Brown decided it was time to get back to his cybersecurity roots and work internally as a CISO. Brown wanted to work for a company that was making a difference in the world, and Boston Scientific, with its medical device innovations transforming lives, exemplified a strong fit. With ten months as CISO under his belt, Brown possesses a strong will to expand his program while working closely with other business departments.

DATA PROTECTION AND A TRUSTED SECURITY PARTNER

Shortly after his arrival at Boston Scientific, the company launched a global Data Protection initiative led by the Chief Security Officer, Senior Counsel-Global Privacy & Data Protection, and Brown as the Chief Information Security Officer. The leadership team conducted a cross-functional and stakeholder data review identifying location, owner(s), classification, protection, access, and sharing/collaboration in order to ensure that the company's comprehensive data protection strategy remains robust. As part of its' initiative, the company also established a formal Global Data Protection Council.

The Council is an important partner and channel for Brown's team in many ways. He says, "Through the Council, the security team is more easily connected across the corporation not only for ensuring the protection of Intellectual Property and personal information, but as a way to further enhance our security awareness efforts.

The cybersecurity team and Council have aligned on key initiatives such as threat intelligence, privacy, forensics, and employee education and awareness."

Through coordinated efforts with the Council, Brown and his security team work actively on partnering and engaging various organizations throughout Boston Scientific. "As the CISO and member of the Global Data Protection Council, I meet regularly with the leaders within the businesses as well as key partners such as Legal, Human Resources, R&D, and Finance, for example," Brown relates, adding "but the real partnership comes from the interaction my security team provides with those same organizations at their level." Brown describes this interaction as recruiting "Security Champions" throughout the company which act as primary points-of-contact who the team works regularly with in such areas as awareness and training, alerting, and support. "Top down leadership is a necessary start, but fostering an enterprise-wide culture of awareness and ownership is really the best way to ensure engagement," Brown believes.

MEDICAL DEVICE CYBERSECURITY INTEGRAL TO PATIENT SAFETY

In support of Boston Scientific's Digital Health Initiative, Brown and his security team have focused efforts on ensuring security around the company's products and medical device components and applications, resulting in a clear competitive advantage for the organization. "Digital Health is a strategic priority at Boston Scientific and several things we are doing in security will be differentiators for the company. We always ensure our products meet requirements for medical device security, but we are going further than that. There is so much information that can be housed on medical devices, or accessed through medical devices. It is not just protected health information (PHI) or personally identifiable information (PII). Hackers and cyber criminals will exploit any access point to get to a hospital's data or any other system the device may interconnect with, and if left unsecured, a medical device connected to a hospital network may create an access point. While many are focused on just the devices, we are also looking at what supporting infrastructure and applications can be used to pivot into our devices or a customer's network. We want our customers to be comfortable adopting our entire ecosystem, not just our devices. We want to build upon our trusted partnerships. Those are the types of things we are thinking about with our medical device security program. Ensuring security at those points can be a differentiator for us with the hospitals and healthcare providers."

> Top down leadership is a necessary start, but fostering an enterprise-wide culture of awareness and ownership is really the best way to ensure engagement.

The medical device initiative requires Brown and his team to work closely with the research and development team, which continues to demonstrate a strong commitment to security. According to Brown, the process has gone smoothly because his own team is working collaboratively and openly. "We don't say 'no you can't do that'. We work to find a secure solution in support of the business. Of course, patient safety and confidentiality is always paramount."

TALKING CYBERSECURITY TO THE BOARD

Brown briefed the Boston Scientific Board of Directors after six months on the job. "It was a fantastic opportunity to give the BOD and several members of the Executive Committee an assessment of the security posture of the company, provide insights into what is happening in the cybersecurity world, discuss the data protection initiative and expound upon the company's strategy," Brown says. He adds, "There is a real importance in working with our executives on security. In today's world many governing bodies, including the SEC, are holding executives and BODs accountable for understanding security threats and risks to their organization."

Brown is researching the best way to leverage current and future tools to clearly communicate with leadership in a concise manner. In support of that, Brown has begun the process of employing solutions that can not only ingest and correlate information and minimize manual processes, but also provide customized dashboards that can present relevant information at the appropriate level. "Whether it is third party vendor management, incident data, training metrics, or compliance information, there is a value in customizing and providing a continuous flow and access of information to the various partners and organizations within the company," Brown states.