PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SEAN WALLS

CISO, Visionworks

HEADQUARTERS: San Antonio, TX

EMPLOYEES: 8,500+

ANNUAL REVENUE: $947.4 Million

SIZE OF SECURITY TEAM: 15+

Sean Walls began his cyber security career in the late 90's but had his first serious opportunity to develop a well-rounded understanding of security and IT governance in 2002 while working at Black Box, an international technology solutions provider. During this time, publicly traded organizations were required to implement section 404 of the Sarbanes Oxley Act, and through his work on this, Walls had his first exposure to true security from a structured framework and governance perspective, including policies, procedures, and standards. After moving on from Black Box, Walls spent almost ten years at Presidio, providing security consulting services to organizations through extensive work with security policy, standards, process, compliance, PCI, HIPAA, as well as penetration testing, social engineering, and risk assessments. He went on to lead their external security practice, as well as lead their internal Information Security Office as Sr. Director of Information Security (CISO).

Walls comments, "While I was at Presidio, I was tasked with leading their cyber security division, which was an external facing consulting practice, but I was soon promoted to their CISO-equivalent. I spent about nine years at Presidio running their external facing cyber security division, as well as their internal facing security programs, including Governance, Risk Management, Compliance, Incident Response, Security Awareness, and so on."

After leaving Presidio, Walls worked at Eurofins, an international organization operating in 49 countries with over 55,000 employees. He held the title of Vice President of Cyber Security at Eurofins, and then moved to Texas to take on his current executive leadership position as Vice President and Chief Information Security Officer at Visionworks, one of the largest optical retailers and healthcare provider in the United States with over 700 locations nationwide.

SECURITY AS AN ENABLER TO THE BUSINESS

Joining Visionworks meant Walls had the opportunity to work for an organization where security is viewed as an enabler to the business and an integral part of the security strategy. Leaders at the organization believe technology and security should play an important role in helping meet and protect goals and priorities of their business strategy. Walls saw great opportunity in working for an organization where IT and security play an integral part of business strategy.

Walls comments, "Security needs to be an integral and valued part of any business strategy. And we need to manage cyber security risk the same way we manage financial risk, operational risk, strategic risk, and all other aspects of a business. We need to be doing the same thing for security. What we're seeing is a trend where more and more organizations are allowing their CISO to sit-in and present at board meetings. As a result, board members are getting visibility into the importance of security, compliance and cyber risk management; however, I read an article a few days ago, Enhancing the Brand and Creating Value Through Cyber Security

"Security has traditionally been thought of as a hindrance to business. I would propose that it can be the opposite. Of course, it's there to preserve value and sometimes it does slow things down, but it can also be a creator of value, not just a preserver. And you can do that, for example, by certifying to SOC 2 or ISO 27001 and becoming a preferred partner to other businesses and customers in your market, demonstrating your commitment to security and privacy for your customers, and using that as a brand enhancer. Being able to have a well-tuned compliance program can also create value when you move into new markets. Whether it's overseas or a regulated market like California which has CCPA, you can ramp-up and become compliant quickly, helping to increase your company's speed to market and earning the company money because you're able to get into the market at minimal risk and fully compliant as quick as possible." - Sean Walls

that 38% of Fortune 500 companies still do not have a CISO appointed, which is a shocking statistic to me. We have many large organizations lacking a dedicated security executive in charge of managing risk and the security program. However, what I do see is a trend in the right direction, where security is becoming an important part of the business strategy."

Just over three months into his CISO role at Visionworks, Walls has focused on key goals to help him align security to the business and set himself, and the security program up for success. His goals include ensuring security has buy-in from executive leadership, understanding the business, and gaining clarity into risks, controls, technology, and governance, while ensuring that compliance requirements are being adequately met.

He comments, "I've meet with the various Vice Presidents and Senior Vice Presidents, along with the functional group leaders and other folks throughout the organization to understand not just what they do, but more importantly, how it's important to the business. What are the priorities for the business? How does the business function? What are the critical assets for the organization? And when I say assets, I mean not just technology and applications, because those are obviously important, but also the data, people, resources, and processes that run the business. In order to protect the business, you must understand the business and what's critical to its survival. So, that was the first thing, but there was a lot of things happening in parallel including understanding the technology stack, compliance gaps, and risk profile."

BUSINESS GOALS AND DIGITAL TRANSFORMATION

Being on the executive leadership team has enabled Walls to speak with other leaders to understand their priorities and goals. He says first and foremost, the goal is to improve the end-to-end customer experience. He explains, "Our goal is to make the customer experience as smooth and seamless as possible and to maximize customer satisfaction. And my role in this process is to leverage technology to enable the vision, and to ensure we control risk and meet compliance obligations in the process."

Furthermore, Walls says they are focused on growth and expansion, including increased market share and strengthening their competitive advantage. Visionworks is currently undergoing a full-scale digital transformation, something Walls has an opportunity to be a part of. He says they are adopting certain emerging technologies, business analytics tools, as well as migrating some systems to the cloud. This transformation will enable them to be more efficient, competitive, resilient, and nimbler, but also provide visibility into the market, their customers, their performance, and how they can improve their service offerings.

Walls believes many CISOs struggle to be involved in strategic planning discussions around digital transformations, but since enterprise architecture is rolled under Walls, he strives to ensure technologies properly align with the future state reference architecture model, which focuses on standardizing and consolidating the technology stack. Walls and his team ensure architectural reviews are performed for infrastructure, data, application, and security on all new projects. He advises other security leaders to ensure these four core areas be addressed at the design phase of any technology project, and to make sure they tack and align with the business goals and standards all the way through the SDLC.

In regard to security being involved in the early phases of digital transformation planning, Walls says, "If you own enterprise architecture like I do, then it's easy because you just change the process so that you inject yourself right at the beginning of every project. This allows enterprise architecture to review all projects to ensure standards are followed, security and compliance requirements are met, and the project aligns with business objectives. If you don't own enterprise architecture, then I would recommend meeting with the enterprise architecture team to make sure that they have a security architect on staff. If they don't, offer to let them use your services, if bandwidth permits. Often, enterprise architecture will look at a project and focus on infrastructure, data, and applications, since most think that's the core of enterprise architecture, but they're missing a really important aspect, which is security."