BILLY SPEARS

CISO
ALTERYX

HEADQUARTERS: Irvine, CA

EMPLOYEES: 1,500+

REVENUE: $495.3 Million

Billy Spears is currently the CISO at Alteryx, a software organization that unifies analytics, data science and business process automation in an end-to-end platform to accelerate digital transformation. As the first CISO in the organization, Spears has an opportunity to work with business leaders who support and value security as a key component to help drive the organization's technology offering forward. His focus has been on improving the security protection strategy to support overall business objectives.

SECURITY PROGRAM FROM A FUNCTIONAL PERSPECTIVE

Spears looks at his security department from a functional perspective, containing information security, cybersecurity and application security components serving the needs of the organization.

The information security program includes security-related governance, risk and compliance functions. Spears explains, "The governance function manages programs like business continuity and disaster recovery, insider threat detection and response, security awareness and training and security-related policies, standards and procedures. Our risk and compliance function are focused on security sales enablement, security risk management, third-party vendor security risk management and compliance with security-related frameworks, industry standards, internal policies and laws."

The cybersecurity program focuses on ensuring the protection of devices, networks, applications and data from threats. This program has two primary focuses - enterprise and product or application security. Spears says, "Enterprise cybersecurity includes areas like security information and event monitoring, network security, identity and access management, vulnerability management and incident response."

He continues, "Our application security team focuses on ensuring a 'security-by-design' philosophy is integrated using a 360-degree approach to proactively managing security of our internally developed products."

KEY FOCUS AREAS

Spears key focus areas include mitigating risks associated with security threats and vulnerabilities, modernizing the policy portfolio, supporting digital transformation and proactively managing security hygiene.

From Spears' perspective, CISOs are transformational leaders. He enjoys serving as a change agent working with cross-functional areas of responsibility matching the speed of digital transformation initiatives with agile, forward-thinking security strategies that consistently transform with the business to

> *"Over time you'll establish credibility within the organization and gain positive momentum as people begin to integrate security from the ideation phase and support the movement."*

deliver reliable system performance with security throughout its ecosystem amid constant and changing threats.

Companies are continuing to increase reliance on remote workforces. The work from anywhere concept has established an interesting opportunity for CISOs to consider strategic approaches for managing non-traditional security risk. He is always aiming to expand the security architecture and accelerate integration of new technologies to increase visibility and subsequently boost data protection capabilities.

To up level their policy portfolio, Spears and his governance team established modern security policies that align with industry standards and outline critical controls to protect the organization from risks. They actively partner with business stakeholders, collaboratively ensuring security requirements are utilized as guiding principles setting the tone for a positive security culture. Spears says he is fortunate to have positive support from the executive leadership team demonstrating their organizational commitment to information security as a component of the overall business culture.

Lastly, managing security hygiene is a critical component for reducing risk associated with known vulnerabilities and a key focus area for Spears and his team. They concentrate on cyber resiliency and have adopted a mindset that centers around increasing attacker costs while improving remediation responsiveness. His team gets excited about improving their cyber innovation and strategizing new approaches for reducing security risks while supporting organizational priorities.

COMMUNICATION: THE KEY TO SUCCESS

Spears says when building or strengthening a security program, it is imperative to develop strong relationships to understand the core needs of the organization. He believes it is important to work with respective business leaders and create alignment on mutually beneficial opportunities for the security team to support organizational objectives while improving security posture.

He remarks, "If you integrate too much change rapidly, you may unintentionally disrupt the ecosystem of company initiatives. Security professionals see a great deal of opportunities for improvement and naturally want to remediate everything, all at once." Spears suggests developing a risk-based prioritization of what should be accomplished then working with business leadership to build support for those initiatives spread out over a defined period. He doesn't often hit the brakes when building security programs, however he says that he has learned to take his foot off the accelerator at times to ensure success.

He also believes in embedding security into the cultural DNA of the organization. According to Spears, "Security leaders should focus on education and awareness to ensure all personnel are able to recognize and appropriately react to security risks such as email phishing or other security events." He understands the importance and value of a strong security program. Spears comments, "It's important to have a little bit of resiliency as a security leader. Each time I speak with leaders I provide some insight or a tip about a specific security theme enhancing the value of proactive security measures. Over time you'll establish credibility within the organization and gain positive momentum as people begin to integrate security from the ideation phase and support the movement."

CITIZEN DATA SCIENTISTS & PREVENTING FUTURE CYBER ATTACKS

As workers everywhere become more comfortable working with data, the ability of businesses to deliver value in data processing and analysis increases exponentially. Spears believes their ever-expanding skillset increases value by delivering actionable insights from terabytes of otherwise impenetrable data to help the company forecast, mitigate risk and fraud, deliver relevant products to their customers and improve cybersecurity defensiveness.

Spears states, "Effective cybersecurity threat hunting has always been built around the constant pursuit, near capture and repeated escapes of adversaries attempting to infiltrate a corporate network. Using a powerful analytics platform that enables machine learning capabilities is crucial to detect and address cybersecurity threats more rapidly by providing security departments with the ability to examine large volumes of data to uncover trends, identify patterns and deliver actionable intelligence."

With the further democratization of data, citizen data scientists will play key roles in helping security teams enhance and simplify their cyber defense technologies by precisely detecting future attacks, proactively identifying security blind spots across the network and protecting valuable company information.