PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BILLY SPEARS
CISO, lOANDEPOT

HEADQUARTERS: Foothill Ranch, California

EMPLOYEES: 6,000+

ANNUAL REVENUE: $1 Billion+

EVOLVING INTO A BUSINESS STRATEGIST

Billy Spears believes his knack for strategic problem solving combined with strong communication skills from a young age prepared him well for his career in cyber security. Currently the CISO of loanDepot, a fast-growing national consumer lender that matches borrowers through technology with the credit they need, Spears is focused on helping with continued innovation and growth.

He began his career with a strong technical understanding as a solid foundation for his cyber security experience. During this time, Spears worked on tactically solving problems, growing his understanding of business challenges, and becoming a dependable resource for organizations. He then grew into a business strategist, melding his technical skills with the skills necessary to improve productivity, increase morale, and take the strategic corporate vision and help execute it through his security program. He says, “In order to become a business strategist, I had to learn how to be a leader, not just a manager and not just a deep technical expert. I learned from a lot of mentors and I think I’ve been fortunate throughout my career to have phenomenal mentors that continue to grow me, even when I didn’t think that I needed growth.”

He continues, “I learned early on that I could make impactful changes. I could get a breadth of experience in places that I wouldn’t otherwise be exposed to and I could learn how to accomplish these very tough concepts in other vertical sectors. On my resume, you’ll find that I’ve worked in almost every vertical sector and accomplished significant things. That was the allure for me. I wanted to go places where I could make a difference, where my skillset was a benefit, and where I could work on challenges that hadn’t been solved before.”

IMPACTING INNOVATIVE TRANSFORMATION

Joining loanDepot provided Spears the opportunity to work at an organization with futuristic and innovative ideas. He was sold on the idea of being able to build something that didn’t already exist. Being in the mortgage industry, Spears recognized that historically the industry was very manual driven, with not much technology and no way to speed up, create efficiency, or lower the cost of a loan. Working at loanDepot enables him to be part of a team who strives to use

> *“THE BEST ADVICE I CAN COMMUNICATE WITH LEADERS IS THAT CLARITY IS KEY. A GREAT LEADER IS SUCCINCT IN THEIR MESSAGING, STRATEGICALLY NEGOTIATES FOR MUTUAL OPPORTUNITIES, AND LISTENS FOR ALIGNMENT.”*

technology to disrupt the mortgage industry and establish a new digital transformation that allows customers to increase their speed to market and improve their ability to acquire services and products.

Spears believes that aligning security with digital transformation requires agility and a true understanding of the company culture. He explains, "If I need to advise the business about a security related risk, if I need to talk to the board, or if I need to talk to the CEO, they are all very supportive, which provides a unique opportunity to establish rapport and influence how other leaders approach problem solving within their areas of responsibility. This softer approach allows the infusion of cyber security and privacy at the beginning instead of the middle or end where it's much more costly to revise plans or start over."

He continues, "The misalignment with executive leadership tends to come from not understanding the culture of the company, and it is imperative to stop yourself because it's a natural reaction for security professionals to just dive in and understand the detail surrounding cyber risk. It can be overwhelming to consume by business executives so you must build an institutional baseline before communicating these types of risk. You must understand what the company's about and what are their market conditions? What are the internal structures and politics that affect change around the business? What type of corporate services or products do they sell? They might have a different audience. And then lastly, what are their technologies and core systems?"

STRATEGIC GOALS FOR IMPROVEMENT

Spears lays out his top goals for the next twelve months including efficiency, maturing the information-governance posture, and improving awareness. The top goal for Spears is improving strategic alignment with the threat landscape and business priorities. He considers the social and economic factors driving change outside the business, then establishes his strategy for success, and scopes these changes to the ever-changing business priorities that come from the senior most executives.

Another goal is maturing the information governance posture to ensure it is defendable, repeatable, and sustainable. He believes this provides the business with comfort that core capabilities are implemented to proactively manage risk. He seeks to constantly improve as technology evolves into more of a digital ecosystem.

In the governance layer, Spears wants to improve awareness, training, and outreach. He explains, "It's important to speak to people in a way that they'll receive information well, instead of the traditional lectures or just e-learning courses. You should never deliver training once a year and check the box complete as your staff population will not retain the knowledge and perform associated actions according to company requirements. It is vitally important to engage staff continuously to simplify the message. I love the idea of a universal resource hub where new content is created weekly and customized for role-specific needs across the business. This allows more versatility to develop user heat maps and understand risks by channel while supporting targeting investments with low performing areas. It is also important to include calls to action within your messaging strategy that directly result in higher engagement and longer knowledge retention. Lastly, make learning fun. I love gamifying the experience across the company."

He also wants to increase efficacy around the security architecture integration across critical functions and improve security operations. He says, "You should be integrated with product development, DevOps, the identity and access teams, legal, HR, product development, marketing, etc. And then obviously your networks, you want to understand what's coming in and out and you want to understand how traffic moves east and west. For security operations, you must have precise intelligence gathering, which increases performance for everyone. You want to automate your security operations group and ensure active monitoring increases the speed of discovering risks while naturally decreasing dwell time and reducing noise."

CLARITY IS KEY IN THE BOARD ROOM

When addressing the board, Spears says, "I heard a quote once that the words a leader speaks are important, but how they're delivered makes the difference. Security leaders don't tell stories. They come in with a lot of numbers and they're looking for boards to give them answers. The best advice I can communicate with leaders is that clarity is key. A great leader is succinct in their messaging, strategically negotiates for mutual opportunities, and listens for alignment. Tell them the story, give them a highlight of a couple of things in terms of themes that are important. Provide options such as A, and B, here's the implications of both, and then offer a recommendation for a strategy to mitigate the associated risk."

Spears believes in showing how the program is doing, where it should be, the gaps in place, and the future strategy. By following this approach, CISOs are able to gain support, improve their audiences understanding for cyber risk, achieve confidence from key stakeholders about their ability to be successful, and manage organizational risk in a more cohesive way.