ALEXANDER BERMUDEZ

CISO & DPO
FISKER, INC.

HEADQUARTERS: Manhattan Beach, CA

EMPLOYEES: 850+

REVENUE: $736 million cash balance at the end of 2022

PROFILES IN *Confidence*

Alex Bermudez is currently the Chief Information Security Officer (CISO) and Data Protection Officer (DPO) at Fisker Inc., an electric vehicle manufacturer focused on design, sustainability, and innovation.

Alex's career began in Information Technology, first working in an IT support desk role then progressing into opportunities with increased technical exposure and complexity. In the early 2000s while working as an IT systems engineer, Alex had an opportunity to transition into information and technology security, his first official role helping to develop a cybersecurity program while leading a team of security professionals for a large subprime lender in California. Although he had taken on minor security responsibilities in previous roles, he was excited for the opportunity to take on a bigger role and contribute the field. He explains, "My transition into security was a matter of being in the right place at the right time, I went from an IT systems engineer to being an IT security manager, with an opportunity to build out a team and work across multiple security domains including administration, engineering, and architecture."

After growing his security experience within the healthcare, manufacturing, and finance industries as an individual contributor and hands-on manager, Alex moved in larger leadership roles as Director, then Vice President, and eventually Chief Information Security Officer. After working as Director of Global Cybersecurity Risk Management at Panasonic Avionics Corporation leading enterprise and product portfolio security for several years, he was promoted into the Panasonic Corporation of North America, Vice President and Chief Information Security Officer role. He comments, "I had an amazing opportunity to work with, and alongside, very talented engineers for one Panasonic's largest subsidiaries. During my time with Panasonic Avionics Corporation, they were serving approximately 70-to-80% of the world's airlines, developing their inflight entertainment systems and global communication suites. I had the opportunity to travel the world in support of customer accounts. My was responsible for digital and data risk management across enterprise and product systems."

After spending seven years growing his experience and leadership skills at Panasonic, Alex had the opportunity to join Fisker Inc. He ultimately decided it was a great step forward in his career and presented an exciting opportunity to help shape the cybersecurity and privacy program for an innovative electric vehicle manufacturer.

FOCUSING ON CORE SECURITY PROGRAM AREAS

According to Alex, a strong security program starts with emphasizing core foundational areas. He maintains that by focusing on strong governance with alignment to established frameworks, threat monitoring and response, awareness, supply chain surveillance, and continuous risk assessment, so organizations such as Fisker can achieve their objectives and undergo rapid transformation. He comments, "I strongly advocate for aligning the security program with the business, which must begin with a robust governance program. A governance program acts as a guiding principle and ensures that policy mandates from the executive team are clearly understood and followed. Governance is responsible for defining policy standards and guidelines to support the security program. It also establishes key performance indicators (KPIs) and key risk indicators (KRIs) to measure progress and ensure that the program is effectively reducing risk. By having a strong governance program in place, the security team can make data-driven decisions and confidently demonstrate their value to the organization."

Alex emphasizes the importance of integrating security considerations into all business decisions, and not just treating it as an afterthought. He says that secure product development lifecycles should be followed rigorously, from conceptualization to production and beyond. Whether it is a new cloud-based initiative or the launch of a marketing system, the security team must ensure that security is embedded in every phase of development. This involves assessing potential risks, implementing security controls, and monitoring for vulnerabilities both during and after production. By prioritizing security throughout the development process, you are able to ensure the products and services offered meet the highest standards of safety and reliability, while also safeguarding the interests of the organization and its stakeholders.

REDUCING RISK AND SPEAKING IN BUSINESS LANGUAGE

To ensure security is continually aligned with the business, Alex recommends being persistent and speaking in business terms, so threats and vulnerabilities are clearly understood across the enterprise. By focusing on the same terms, it reduces confusion, and you are not reinventing language every time issues are brought up to the board or executive stakeholders. This creates a universal way to discuss risk across the business, especially as it relates to the threat and vulnerability landscape. He comments, “I firmly believe in establishing agreed-upon methods for discussing risk with other departments within the organization. By doing so, we can provide valuable insights on how we analyze risk and help them make informed decisions based on their risk tolerance levels. This collaborative approach not only enhances risk management practices but also promotes a productive and forward-thinking culture within the business. As security professionals, our role is to educate and inform other departments about potential security risks and the potential impact on the organization’s overall objectives. By fostering a culture of risk-awareness, we can better mitigate and manage risks and ultimately drive the business towards greater success.”

He continues, “As a CISO, accountability is a top priority for me. I maintain comprehensive risk registers and record all decisions made within the business regarding risk. To drive enterprise and product security decisions, I have been an active member of steering committees and ensured that relevant stakeholders, including thought leaders, are involved in the decision-making process. To ensure that all decisions are well-informed and properly documented, I maintain a detailed risk register that is reviewed and updated regularly. By taking this approach, I ensure the organization has a clear understanding of the risks they face, the decisions made to mitigate those risks, and the stakeholders involved in the process. Ultimately, this approach enables us to make more informed and effective risk management decisions, which in turn leads to better overall security posture for the organization.”

TRANSFORMING AT THE SAME PACE AS THE BUSINESS

The nature of Alex’s industry means he must continually keep an eye on changing regulations, while at the same time educating the workforce on the security landscape. He explains, “I recognize that there are always areas for ongoing development and improvement. For instance, we recently attained certification of our Cyber Security Management System (CSMS) for UNECE WP.29 R.155 compliance and it is imperative the team is well-informed and continues to adhere to the highest security standards. To achieve this, it is critical that everyone understands their roles and responsibilities in relation to compliance and risk management. To address this need, we’ve implemented a security education and training awareness program specifically designed for the engineering and software development teams. Through this program, we aim to ensure that every team member is aligned with organizational security goals and understands their role in maintaining compliance. By taking proactive steps to educate and train our teams, we can enhance their security awareness, strengthen our overall security posture, and ultimately better protect the organization against threats.”

> *“I believe in leading my team from the front with a servant-leadership approach. This means I am always willing to roll up my sleeves and work alongside my team, and I would never ask them to do anything that I wouldn’t do myself.”*

Due to the nature of transformation as it relates to the electric vehicle manufacturing industry, Alex says he is continuously looking for ways to improve security in the cloud. He plans to optimize existing technologies while investing in others that will enable Fisker to get a strong handle on rapid changes occurring in the electric vehicle industry. From cloud-based vehicle backends providing software defined functionality to cloud based software distribution to hyper connected vehicles, security technologies like cloud security posture management, cloud workload protection, and XDR, will help enable effective cloud protection processes areas such as threat hunting, monitoring, detection and alerting.

LEADING FROM THE FRONT

Alex says he chooses to lead his team from the front in a servant leader style approach. He explains, “I believe in leading my team from the front with a servant-leadership approach. This means I am always willing to roll up my sleeves and work alongside my team, and I would never ask them to do anything that I wouldn’t do myself. My hands-on approach enables me to provide support and guidance to my team whenever they need it.”

Alex is a highly experienced and skilled Chief Information Security Officer and Data Protection Officer with a strong background in enterprise and product security. He has spent over 20 years in the industry, working with many high regulated and complex sectors such as healthcare, automotive, aviation, and finance. Alex advocates for a strong governance program that supports the security program, aligns the security program with the business, integrates security into all business decisions, and speaks in business terms to reduce confusion. He emphasizes the importance of building and maintaining a strong security foundation grounded in globally recognized standards for excellence and risk management principles. Alex’s expertise and dedication to the security field has helped companies such as Fisker Inc. build a robust security program, protect their digital assets, and maintain trust with their customers.