JACOB COMBS

Chief Product Security Officer/Senior Director Medical Device Cybersecurity

INSULET

HEADQUARTERS: Acton, MA

EMPLOYEES: 2,500+

REVENUE: $1.3 Billion

PROFILES IN *Confidence*

Jacob's career in technology and security has spanned many different industries including telecommunications, defense, financial services, and healthcare. He explains, "I've worked across different critical infrastructure sectors that have extremely high requirements for cybersecurity. This gave me an abundance of experience because I'm not formally trained in cybersecurity, I had to learn by doing to succeed in those industries. And in doing so I realized my love for identifying and mitigating cybersecurity risk."

Jacob is currently the Chief Product Security Officer/ Senior Director Medical Device Cybersecurity at Insulet, an innovative medical device company improving the lives of people with diabetes and other conditions through its Omnipod delivery system.

SECURITY BY DESIGN & KEY RESPONSIBILITIES

As Chief Product Security Officer/Senior Director Medical Device Cybersecurity, Jacob and his team's responsibilities include security of Insulet's Omnipod 5 Automated Insulin Delivery system, as well as legacy medical device products. His team ensures strong security is holistically designed into their products from start to finish. He explains, "We have a large ecosystem that's built around the devices we manufacture and sell. And we are laser focused on security by design, especially when it comes to security architecture, risk management and testing, across embedded devices, mobile applications, cloud services, and data. Along with that comes the global risk management of these products across the full product lifecycle especially from a cybersecurity perspective."

With a continually changing landscape of global regulatory requirements, Jacob ensures his team keeps the organization's devices and patients safe across the globe by managing privacy and ensuring their data is protected.

Jacob continues, "Different product platforms may move into different territories, use different technologies, or integrate with data differently. We have to build a secure ecosystem around our product that gives the business the ability to be agile and address patient needs as they arise. Since security is built into the product, the business can pivot quickly to meet market or regulatory demands."

BUILDING FROM A RISK MANAGEMENT PERSPECTIVE

Insulet's mission is to build security into products using a risk-based approach. Jacob makes sure all stakeholders align to this mission from not just a technical perspective, but also how security protects patients and positively impacts the business.

To achieve this, Jacob says it starts with securing a seat at the table. He believes in regularly meeting with executives and the board to inform them on the status of the security strategy, the current security posture of the products, and how the security program is faring in regard to regulatory changes. Providing risk-level information and how it impacts the company and product lines is vital. Aligning cybersecurity risk to business goals such as the security of next generation products, builds strong communication lines and ensures leadership understands the value of security. He comments, "The foundation is all about risk. I always approach issues and proposals from a risk perspective, talking in terms of business opportunity, brand equity, or customers satisfaction.

"We have to build a secure ecosystem around our product that gives the business the ability to be agile and address patient needs as they arise."

I express it in the terms that mean the most to the to our customers."

Having a business-focused approach enforces positive dialogue that goes beyond technical jargon and instead emphasizes the importance of security's impact on the overall business. Jacob says this also builds credibility for what security is delivering for the business and results in stronger buy-in for future projects or initiatives.

To further solidify the secure by design approach, Jacob says it is important to implement organizational policies around security in product development. He explains, "By engaging early with product development teams using structured and rigorous security assessments, security requirements and design are baked into the product from the beginning. Building this cybersecurity muscle within the organization ensures that secure design happens from the beginning on every single new feature or new product being developed. It has been quite effective in finding issues early and designing a strong security foundation. The business case for security by design is undeniable."

FOCUSING ON MATURITY AND COMMUNICATION

The top focus area for Jacob and his team is expanding and maturing many of the product security policies and procedures that have been developed over his tenure. Launching an innovative medical device is hectic and processes must be regularly updated to ensure their efficiency and effectiveness. Jacob comments, "It is important to iterate over your processes to ensure you are moving from baseline maturity to the next level. In an area like vulnerability management where a baseline process only tracks vulnerabilities, the next level would be ensuring that product development teams are decreasing their time to patch identified vulnerabilities. By maturing these processes during the development and maintenance lifecycles, we are making sure security patches are delivered to the field at a much faster rate. This protects our customers and our business."

Security automation is also something Jacob plans to continue to invest in. He says, "In the medical device industry, our quality standards require rigorous design verification processes. Since these processes statically verify requirements, we have designed into the system, they are a ripe target for automation. The product security organization continues to expand its automation capabilities and I have worked tirelessly to build automation into our DNA. I target security engineers with software development backgrounds and require that automated test cases accompany every security requirement that emerges from our security risk assessments."

He continues, "The last area I'm focused on this year is continually re-evangelizing security. I create training presentations for both technical and non-technical groups within the business. I believe it is important to speak with teams at all levels of the business to bring them up to speed on regulatory changes as well as the modern security landscape. Continuous training and communication ensures that security risk is part of the decision-making process."

"There's a lot of thinking, analysis, review, communication, and collaboration that has to happen to enable secure product delivery at scale."

KEEPING UP WITH REGULATIONS AND TRANSFORMATION

Jacob says he faces two main challenges, both very common across the medical device industry. The first is addressing increased scrutiny from regulators. He jokes that he used to read interesting fiction books for his own enjoyment, but now only reads articles and books covering standards, laws and regulations. He said to be successful in his role, you must always stay up to speed on any changes coming from regulators. He has developed a forward-looking product security program, so they are ahead of the curve when any new regulations are published.

The second challenge, similarly faced by many industries, is security's ability to keep pace with business transformation. Businesses are growing rapidly, expanding their product lines, adding regions, and often undergoing digital transformations at the same time. Jacob comments, "Our products are leading growth in the diabetes technology market and the demand continues to be high. So being able to scale and keep up with that increased demand from a security by design perspective is key. There's a lot of thinking, analysis, review, communication, and collaboration that has to happen to enable secure product delivery at scale."