PROFILES IN *Confidence*

DOUG INNOCENTI

CISO
MOONPAY

HEADQUARTERS: Miami, FL

EMPLOYEES: 300

REVENUE: Private Company

Doug Innocenti has a strong IT and security background in the banking industry, working a combined 28 years at Legacy First Union, Wachovia, and Wells Fargo (which acquired Wachovia in 2008). He then worked at Navan (formerly TripActions) before landing at his current organization, MoonPay.

Doug says security has been ingrained into everything he has done throughout his career, giving him wide exposure to many aspects of the industry. He became passionate about security projects early on, so his career naturally moved from IT-focused roles to more security-focused roles.

At MoonPay, Doug had an opportunity to combine his financial services background with his passion for working at innovative, forward-thinking organizations. MoonPay is a Web3 infrastructure company building end-to-end solutions for payments, custody, world class design, and enterprise-scale digital asset and smart contracts minting.

"Coming to MoonPay was almost like coming home for me," he said. "I've always loved innovation, building new technologies, and working at the cutting edge of new tech. When I saw what MoonPay was doing, it was the perfect model of what I was looking for and interested in. I had an opportunity to help move the needle forward for the next level of technology and expand the fintech space. I feel that I'm at the cornerstone of something new and innovative."

He initially joined MoonPay as Director of Information Technology, running the IT program and working on projects like building the foundations of a zero-trust model, hardening corporate systems, and laying the foundation for the overall security controls. At the time, his team partnered with the security team, which made his move into the CISO role a seamless next step.

As CISO of MoonPay, Doug oversees the strategy, architecture, and governance for IT and security, and is also in charge of implementing and integrating SaaS, contact center, support, and infrastructure platforms. He considers his role a strong combination of information technology and security.

"I have different teams that handle a lot of the traditional IT engineering, and I have my cyber defense team, I have my security operations team, I have my technical operations team, and so on," he said. "The way I look at things is that all of us are responsible for security. I hold them all accountable for how they are going to ensure they're not only implementing secure and robust systems, but they're also caring for the overall topology of security at MoonPay."

FOCUS ON STRONG 2024 INITIATIVES

MoonPay recently earned its ISO 27001 certification, a large accomplishment considering the amount of work and time Doug and his team invested over the better part of the past year. The benefits of this certification will help MoonPay improve overall program maturity while continuing to reduce risk in a proactive manner. Doug says his team is also working on finalizing their SOC 2

"The way I look at things is that all of us are responsible for security. I hold them all accountable for how they are going to ensure they're not only implementing secure and robust systems, but they're also caring for the overall topology of security at MoonPay."

Type 2 certification. They finished their SOC Type 1 earlier this year, and their Type 2 will soon close out after nine months of evidence.

As Doug's team moves into 2024, they plan to achieve their ISO 27018 for PII data in the cloud environment.

"I really think it's going to identify and allow us to extend our overall security posture along with the traditional things that every CISO is looking at right now when it comes to zero trust and defenses around the perimeters," he said.

To accomplish these certifications, Doug leverages his own team along with auditor partners who help level up and ensure they are meeting specific criteria. His internal team takes the lead on day-to-day work that needs to be done to deliver compliance, and in turn the auditors help them deliver on those.

In the past two years, Doug and his team have worked tirelessly on retooling their environment to better understand what investments they have, sunset anything they are not using, and ensure their strategy aligns with the products in their environment.

"Functionally, I think we're in a really great space," he said. "We're going to spend the next year making sure we're getting the most out of the platforms we have, and optimizing them so that we're positioned for our continued growth as an organization."

To ensure executives remain up to date on security plans and goals, Doug has employed a strong communication strategy to share data upstream in a productive and proactive manner.

"On a weekly basis, I produce reports from my team and myself that roll out to the executive team, so we are constantly sharing our security posture, what is underway, what we need to look out for, and what our next steps would be," he said. "This is all combined with our ongoing OKRs at a company level, to really ensure that we're communicating everything upstream on a weekly and a biweekly basis. And really, the culture itself at MoonPay, and the ability to communicate and share information so widely, ensures that not only the executive staff, but the company as a whole is aware of what's going on and how we're delivering to help support not just MoonPay but the employees with staying safe."

TRENDING AREAS AND CHALLENGES

The limited talent pool in information security is something Doug believes to be an ongoing challenge for the industry. Although he feels lucky to have limited attrition within his security team, he says there is always a need to continuously bolster the skill sets of his team members.

"We're focused on leveling up the skill sets of the team in conjunction with completing their daily work," he said. "I'm focused on reinforcing the need to grow their skills, to grow their certifications, and ensure they're continuing to uplift themselves and the program. It's a balancing act, but I've been lucky enough to have a great team that's been able to deliver on both of those."

The changing landscape of threats continues to be a challenge faced by many, and Doug believes teams must be dynamic in their approach to keep pace and ensure their organizations remain secure.

"Staying ahead of threats is all about having the right tooling, the right places to monitor the perimeters around, not just our platform itself, but our endpoints, our corporate systems, and having the right proactive monitoring and notifications in place," he said. "And then obviously the ability to review those on a daily, weekly, monthly, quarterly basis to identify the trends."

Artificial Intelligence (AI) poses another challenge, something Doug and his team are staying informed about in order to better understand the changing market.

"AI is an ongoing challenge for all CISOs to consider, and not only looking at what it's doing but also the fact that it changes the landscape of how you see cyber defense," he said. "The ability for AI to do things that individuals were doing before, but also protecting the data that we have, is important. We need to make sure that if we're using AI, the data we're producing into those large language models are being secured and protected, which is an area we've done a tremendous amount of work on. I think it's evolving and moving faster than anything I've seen in my career. The simple TDoS or DDoS attacks of the past were easy to deal with. Now you're dealing with things that you wouldn't even have fathomed five years ago."