PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHN HEASMAN
CISO, Chegg

HEADQUARTERS: Santa Clara, California
EMPLOYEES: 1,000+
ANNUAL REVENUE: $255 Million

John Heasman has had three chapters in his career so far, starting with the first chapter working as a cybersecurity consultant advising companies on how to build secure products and services. His second chapter was his career at DocuSign for five years, working his way from more technical-geared roles building out the application security team, to eventually becoming the Deputy CISO. During this time, he learned how to build, lead, and manage teams, and grow his influence as a leader. The third chapter of his career has been the CISO at Chegg, an education technology company that provides student services such as homework help, online tutoring, test preparation, scholarship searches, internship matching, and college application advice, as well as both digital and physical textbook rentals.

He says, "As the CISO of Chegg I'm putting into practice all of the skills I've learned both on the technical and the leadership side. The thing that really attracted me to the role at Chegg, beyond Chegg's mission, was this opportunity to lead a small but talented security team where I would be responsible for both the hands-on work because we're a small team, but also thinking strategically of how I could build out the team and put in place the foundations to get the team to the next level."

> *"As the CISO of Chegg I'm putting into practice all of the skills I've learned both on the technical and the leadership side."*
>
> - JOHN HEASMAN

REACTIVE TO PROACTIVE SECURITY

Heasman focuses on being proactive and solving problems by anticipating challenges as the company rapidly grows. He is tasked with building out the risk management side of the information security program in order to have a framework for identifying, categorizing, and prioritizing risks. He comments, "Without a framework to do this, it's easy to become distracted and chase the newest shiny object to go work on and then suddenly the whole team is working on that thing. This is something I was very keen to avoid. I went through a period of fact finding, talking to as many people and leaders in the company as I could and getting them to talk candidly about areas that we needed to improve upon. Then my team started to form a prioritization for our risks so that we could really boil it down to what are the key things we need to get done in the next six months."

By establishing this framework, he says it will allow him to have strong communication with the C-level staff and board on what they are doing to improve security. It provides the ability to drill down initiatives and projects to the right level of detail for those audiences. By articulating their top risks and what the plan to address them is, he will be able to demonstrate progress and that they are moving the needle in a meaningful way.

AUTOMATION AND SELF-SERVICE FOR SCALE

"One of my ideas coming into this role at Chegg was that I wanted to build a security organization that is relatively lean and relies heavily on automation and self-service. We need to put foundations in place for when the company is at a much greater size than it is today, so that we can scale with the needs of the business. Everyone must realize that simply adding more people in security, for fast growing companies, is not scalable. It's hard to find those people. There's a cost in time and money of training them up," explains Heasman.

For example, Heasman explains that a system to scan for vulnerabilities when developers deploy code historically required the security team to run the tool, analyze the findings, and email back and forth with developers, or create a ticket. He says this kind of process does not scale, but by leveraging static analysis companies that tailor findings to developers rather than security teams, the security team is no longer responsible for taking a large list of vulnerabilities and trying to work their way through it. He says this self-service approach is scalable but still has certain challenges, namely other teams may require training and the tools themselves require constant tuning to minimize false positives. When Heasman and his team integrate new security tools, he always considers how he can make the product or service available to other users outside of the security team that may benefit from having direct access to the data.

CLEARING THE PRODUCT CLUTTER

When addressing the cluttered security product market, Heasman focuses on understanding exactly how the solution will fit into the broader program and specifically what gap the solution addresses.

Heasman says, "There are a few key things I always look for in technologies. A few years ago, having products with API was a "nice to have" but nowadays I feel API support is an absolute necessity. An organization like ourselves, we're often not running these tools in isolation. They're often not run by humans, they're orchestrated by other processes and we want to pull the results down, manipulate them, store them elsewhere, and aggregate them with other tools. That's something I will always ask a vendor. I like to see vendors that have really considered their API and really understand how customers like us are going to use their product."

Heasman also speaks with Venture Capital companies and always asks for references from any security product he is interested in purchasing. He seeks references from companies of similar size and scale to understand how the product will address his specific challenges.

ALIGNING TEAM GROWTH AND LEARNING

Heasman fosters a team environment of continual learning, and in turn encourages his team to always share what they learn with one another. He believes it is everyone's responsibility to level-up the team, regardless of them being in junior or senior roles.

He explains, "Often a team member will come to me and have a certification, conference, or seminar in mind. I will ask what value that individual is going to get out of it, how that aligns with what we're trying to do as a team, and how that will help the company. That's the key thing. I want to make sure that our training efforts are aligned. I want the individual to get new knowledge out of it that will help them in their career development. But I also want them to share their newfound skills with the team and for this to help us on our mission."

The Huge Potential of the Education Technology Space

"When I consider a role, I'm looking for a company with a very clear mission. DocuSign and Chegg both have very clear missions. And, digital transformation, when it comes to the education space, historically it's been lagging behind other industries and I feel we're on the cusp of that changing. The education tech space is going to undergo massive growth. One of my goals here is to build the foundations of a program that will enable Chegg to scale and expand, whether that be through acquisition or expansion into international markets. The ed tech space has huge potential, but then of course this brings security and privacy challenges along with it. I'm really excited about the company's plans and the interesting security challenges that come along with those." - John Heasman