KELLY HAYDU

Vice President of Information Security and Technology
CarGurus

HEADQUARTERS: Cambridge, MA

EMPLOYEES: 900+

REVENUE: $551.45 Million

When Kelly Haydu was asked by a recruiter to take a meeting with CarGurus's CTO, she initially went into it thinking it would be a good networking opportunity, however once she learned more about the organization, she knew it would be a great fit for her career. Kelly says, "I really wanted to understand, what was their vision, what was their strategy? Is it a place that I would want to work? I talked to many individuals and with every conversation I was impressed with their culture; the people were just outstanding. Everyone I spoke with was genuine and wanted to do the right thing. Integrity is a core value of CarGurus which is important to me. I knew it was a place I could be happy."

She continues, "CarGurus has such a great group of people. Leaders in security roles aren't always welcomed to the table. They have invited me with open arms. I am grateful for that and the executive support I've received."

CarGurus is an automotive research and shopping website that assists users in comparing local listings for used and new cars and contacting sellers. As an innovative, rapidly growing company, Kelly says that during initial conversations it was clear the organization recognized the importance of a mature security program. With new digital tools and additional transactional capabilities including their Instant Max Cash Offer (IMCO) and the acquisition of CarOffer, ensuring seamless and robust security was a necessity. Kelly comments, "I think the company understood that in order to expand beyond a listings business, they were going to need additional security around those existing and new product features."

Before her tenure in the security space, Kelly worked in Quality Assurance including lead automation roles across markets and verticals. She served in various previous roles as Director and Senior Director in Information Security prior to taking on the Vice President of Information Security role at CarGurus. In August of 2021, IT was brought under her department, and she became the Vice President of Information Security and Technology.

CREATING STRONG SECURITY AWARENESS

Kelly's first and foremost responsibility is to educate all employees about their responsibility to the overall security of the organization. Creating a strong awareness and educating the workforce is key for her to ensure security is baked into their everyday culture. She explains, "Creating awareness and education across the whole employee base is really important. Once people start to understand what those security best practices are, I often hear them say they had an 'aha' moment when they're working in their particular department and they're handling personal data or they're handling confidential data, or they get an email and they're not sure if they should click on that link. It causes people to think about security in a different way and to sometimes pause. My job is to educate, but also to make

sure that you get to a point where employees carry those best practices into their personal lives."

The security program under Kelly includes risk & compliance, application security and security operations. IT remains as a separate department but both teams work closely together. By focusing on these core areas, Kelly comprehensively focuses on both risk reduction and increasing security maturity.

Under risk and compliance, the security team focuses on streamlining the vendor risk assessment process to enable the business to move quickly while still gaining visibility across vendors and partners. For their security team, understanding security risks and evaluating them has been a large project, which goes hand in hand with understanding all end user applications they use on their machines.

For application security, Kelly and her team focus on the Software Development Lifecycle (SDLC) process and how they can instill the 'shift left' mentality and approach. She explains, "We've tried to build security architecture reviews into our SDLC process. We are still building the program. We want to make sure that we are providing recommendations for secure coding and collecting feedback from the product and engineering teams. It is important for the application security team to gain insights earlier into that review cycle when the ideas are incubated to understand what are the necessary security protocols and what are the risks."

One of the biggest focus areas for security operations is around automation. Kelly says they have already started building a golden AMI pipeline so they can hone-in and have an automated strategy for patching their infrastructure systems. Her background working as an automation engineer has provided her ample exposure to ensure their automation goals are met.

The IT program is in the process of hiring an Identity & Access Management engineer to help orchestrate identity solutions across the entire organization. This involves a deep understanding of what they have today in order to streamline and consolidate to avoid redundancy of multiple systems.

INDUSTRY BENCHMARKS AND TYING BUDGET TO THE BUSINESS

When planning and strategizing for budgeting, Kelly recommends reaching out to your network of CISOs to better understand how to approach this sometimes daunting task. Kelly states, "My advice would be if you're going to go out and do an industry benchmark, make sure that you're benchmarking against your industry, including public and private companies. That is important for not only where you are today, but if you're a growth company, where you're going to go. You must make sure you are telling the story and showing them the picture of where we you are and what the risks are to your business."

"A lot of times employees might not understand how security ties back to their work or their function. If you can start to talk about how that ties back to the strategic initiatives or the products or programs that they're running, you'll get better buy-in."

By getting ahead of the curve and demonstrating the long-term benefits of having the appropriate staff and budget, you avoid playing catch up or being behind. Kelly says what is key to remember is tying it back to business and strategic initiatives to exemplify how security provides value to the organization.

According to Kelly, conversations with executives about budget are most successful when CISOs have invested time in educating the business about the importance of security. She suggests putting a roadshow together that includes roadmaps with major initiatives or projects and to get in front of each business unit to show them what the security team plans to accomplish. She explains, "A lot of times employees might not understand how security ties back to their work or their function. If you can start to talk about how that ties back to the strategic initiatives or the products or programs that they're running, you'll get better buy-in. You must form the relationships through something like a roadshow. People that are solely focused on the technology will sometimes fail in that area because they haven't been able to socialize why their function is important and how it relates to the other business units. So, getting that roadshow going and meeting with other stakeholders is important. Be careful not to give too much information to people in your first meeting, though. Security can be overwhelming to those that have had little to no exposure to it."