ANDREW SMEATON

GLOBAL CISO
DATAROBOT

HEADQUARTERS: Boston, MA

EMPLOYEES: 1,100

REVENUE: Undisclosed

Andrew Smeaton is a career security professional with over 25 years of technology experience working in government, banking, healthcare and now his most current role as CISO for DataRobot, the leader in enterprise Artificial Intelligence (AI). Smeaton comments, "DataRobot is known for its unique approach to AI and machine learning that appeals to a broad mix of users, including data scientists, business analysts, data engineers, software developers and executives. Our proven combination of cutting-edge software and world-class AI implementation, training and support services empowers any organization - regardless of size, industry or resources - to drive better business outcomes with AI. Some of the very best data scientists in the world work for DataRobot. Certainly, some of the smartest people I've ever worked with. That makes it so interesting for me and our team, we are working with giants in the data science industry."

Smeaton has a passion for building world-class security programs while focusing on business enablement. He says, "I must say, I love security, it's the first thing I think about when I wake up. I truly love what I do. Over the years, offers regularly presented themself to serve as a CIO, but I have never been interested. My passion is security and that's where my career started, working for the government 32 years ago. Over the years I think my Liverpudlian sense of humor, constant willingness to learn and passion has postured me in good stead."

COMMON SENSE APPROACH TO STRONG SECURITY

Smeaton takes a common sense approach to security, with efforts equally focused on doing the basics flawlessly, recruiting a strong workforce, utilizing artificial intelligence, security data analytics, leveraging automation, ensuring there is a sound security architecture and providing a platform to be successful.

Since becoming CISO over 16 months ago, Smeaton has reviewed the organization's risk model, created a culture where users want to engage proactively, improved processes and worked across relevant departments to attain DataRobot's strategic goals.

Smeaton comments, "As our team has grown, so has the need to formalize and mature existing security, compliance and privacy processes that reach throughout the organization. Our entire company has been incredibly supportive of our initiatives to drive security forward over the past year and we plan on taking that into 2021."

He continues, "We have worked very hard to build strong relationships across DataRobot and have seen huge wins from this teaming. We have become closely aligned with our Engineering teams, Human Resources, Sales and Legal staff and we plan on focusing even more on this in order to deliver the

best possible products to our customers."

FOCUS ON AN INNOVATIVE TEAM

Keeping pace in a fast-moving environment means Smeaton must always focus on business alignment, innovation and his team's success as top priorities.

Smeaton comments, "Strategically, I think one to two years ahead while recognizing how to stay aligned with business objectives. It's very important that a CISO has a seat at the executive-level during strategic or business discussions. As a CISO, relationships are incredibly important. The language of the boardroom is business language, so I always talk in business terms and about the cost of business."

As a leader, Smeaton measures himself by the growth of his team, and believes there is nothing more rewarding than helping other people grow and inspiring them to reach new goals.

He says, "The first step in driving innovation is to build an innovative team and find rock stars. Sometimes you must recruit, other times you can find natural rock stars within your organization. It is important to identify and recruit innovators and people who think outside of the box, because that is what it takes to be great at security. These are the big ideas people, who think beyond incremental innovation and have broad interests, diversified backgrounds and present not only their hard skills, but also their soft skills. I identify mavericks and non-conformists, people who are not afraid to break the rules and existing paradigms."

The next step to an innovative team is creating open, honest dialogue. He explains, "I create an environment where people are not afraid to blow things up and start again. As a CISO, don't be scared to be challenged and open to thinking differently. CISOs shouldn't dictate to their team, they should create an environment where every idea is utilized in one way or another. Every year I tell my team that it's a blank piece of paper and to think differently. Individually, we come up with ideas, and together we evaluate as a team and prioritize initiatives."

The security team at DataRobot is comprised of experienced professionals who have worked across the globe in a multitude of sectors. Smeaton ensures he allocates budget for innovation to provide his team the time to work on projects and their ideas. He states, "After you've done all the hard work in hiring and creating the right environment, the next step is exhilarating; it's letting the horses run. Of course, as a CISO you still have to manage, but as a leader you have created the environment for success."

SEAMLESS TRANSITION TO REMOTE WORKFORCES

When workforces went remote this year, DataRobot was poised for success as a cutting-edge SaaS organization. Smeaton says that when their employees began working remotely, they took their laptops home and had the same work environment as they would in the office. While many organizations struggled with on-prem solutions, datacenters or limited VPNs, DataRobot was seamlessly prepared.

Smeaton explains, "From a team perspective, we didn't skip a beat to be honest. The team was fully functional with very little productivity loss. From a security point of view, it made us fast forward some of the strategic partnerships that we had already gone forward with which gave us more security intelligence. We also focused on education around the pitfalls of working from home, concentrating on the executive team to make sure they had secure networks to work from."

LOOKING FORWARD: TOP SECURITY TRENDS IN 2021

Smeaton focuses on these trends to look out for in 2021:

Ransomware will change yet again. Smeaton says The Department of Treasury and FBI have indicated that ransomware funds are ending up in the hands of individuals and regimes sanctioned by the United States. He believes this will force the underground economy to shift their tactics and not necessarily run adversaries out, but we may see yet another evolution in ransomware.

Proprietary CPUs will help level the playing field. With the introduction of Apple's M1 chip and Microsoft's Pluton chip, a huge leap in more control and greater security will take place according to Smeaton. He says there will be less interdependence on vendors, undoubtedly leading to greater software security.

Zero Trust. Another top trend for Smeaton is Zero Trust, rooted in the principle of "never trust, always verify". He says Zero Trust is designed to protect modern digital environments by leveraging network segmentation, and organizations should prioritize focusing on building a strong Zero Trust program.

Location-agnostic security operations. Smeaton says these should be designed to support customers everywhere, enable employees everywhere and manage the deployment of business services across distributed infrastructure.

Hyper automation Security Orchestration, Automation and Response (SOAR). According to Smeaton, SOAR helps accelerate incident response and maximize security tools while standardizing processes and should be another focus area for security leaders.