PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MICHAEL COATES
CISO, TWITTER

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 3,600

ANNUAL REVENUE: $2.5 Billion

Many CISOs begin their careers as technologists, yet it is the combination of technology and business strategy that ultimately drives their interest in information security. Such was the case for Michael Coates, the CISO of Twitter. Coates says, “The exciting thing about information security is that it is not just a technical challenge. The truth is, the best technical security answer could potentially drive a business into the ground. The challenge of finding security solutions that work strategically for the business is exciting.”

Coates says he was drawn to the CISO role at Twitter because of the organization’s greater role within the world. “Many organizations need security to be effective, such as banks and government agencies. At Twitter, security is absolutely vital for a safe user experience. Twitter is a platform that allows people to speak truth to power all over the world. For that reason, we need to ensure a safe and secure experience for each and every user.”

As a business, Twitter is only successful if users trust the company’s security efforts. This reality motivates Coates and his team everyday. It also elevates security within the organization, as a basic core of the platform’s mission.

> “The key is to explain the risk as it relates to the business and get prioritization and buy-in from leaders across the whole company”

“Twitter has a massive amount of public information. We enable people to share incredibly mundane and also incredibly important information. With that we maintain a large amount of private information that our users give to us, such as contact information and their location. We are only in the position we are in because we maintain their trust that we can protect their private data. Our role as a security organization is to protect that data while maintaining the speed and real-time design aspects that are key to the user experience.”

In the two years Coates has been CISO at Twitter, he and his

team have elevated the role of security. It now holds senior leadership visibility and support. The company continues to win awards for its security efforts, and is regularly named to the top spot of the Online Trust Alliance Honor Roll.

MAKING SECURITY A COMPANY-WIDE POLICY

One of the most important aspects of Twitter's award-winning security program is senior leadership involvement and company-wide awareness.

Coates says, "Awareness of security is an important topic because security can be a funny thing. If there is no problem today, others might say, 'well what has the security team been working on?' But if there is a security issue, then still others will say 'well what has the security team been doing?' That is why it is always important to be communicating about security efforts and programs."

Coates suggests finding ways to measure ongoing programs and take a quantitative look at security metrics and business risks. Coates believes it is important to bring in other business leaders outside of the security controls organization to understand and measure security. At Twitter, the Security Committee, which is comprised of key business leaders and heads of organizations, takes a quarterly look at overall security efforts as they relate to business performance.

This approach has enabled the team at Twitter to tackle longstanding risks that were previously deemed too daunting. "The key is to explain the risk as it relates to the business and get prioritization and buy-in from leaders across the whole company." Coates recommends starting with a problem that has a clear path to success to build a reputation and show what can be achieved with cross-organization efforts.

HIGH RETENTION RATES IN A COMPETITIVE MARKET

"One reason I wanted to be a leader was I felt I could accomplish more by aligning a team on an objective," comments Coates. Based on his successes with retention and job satisfaction, it seems that the approach is working well for Coates.

Without a doubt, one of the biggest factors in Coates' success at Twitter, and Mozilla before that, is his ability to retain his team of security engineers in a hyper competitive market. "When given a choice of where to work, people stay with me. That makes me very excited. I'm very proud of being able to hire and build security organizations where people enjoy what they do and want to stay here." Coates believes some of the success comes from growing his team internally, rather than having to fight for security talent in the market.

"We have found success in growing our own security engineers. Creativity is an important quality for a security team member, and certain technical skills are needed, but security knowledge can be taught. We take employees with base foundational skills from another team and then teach them about security. What we found is enterprise or network security engineers can come from network or IT backgrounds and web developers can make excellent web and application security engineers. These people have deep knowledge of how the organization runs and how systems work. They know how people do their jobs and how security measures will impact the job. This knowledge is extremely valuable when building security programs that can be effective and not constraining for the organization."

SECURITY START-UP SPACE

The security start-up space is hot and growing. In fact there has been a 300% increase in venture capital investment in security vendors. It can be tough for CISOs to navigate the crowded and noisy market.

Coates believes many security starts-ups are focused on the big news issues, whereas enterprise organizations still have to worry about more traditional security concerns. He says, "I welcome continued investment and experimentation in the security industry. We need a lot of failures to find success. Many start ups are going after challenging areas and it is just not practical. Why worry about a burglar parachuting in when you left the porch door unlocked? Security needs to be scalable, fast and effective at addressing real problems. Security technologies that create a lot more work for already over burdened security teams are not helpful. If I can trust a security solution to do its job then I can focus my team's efforts on one of the many other issues we face."