PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAVID HAHN
CISO, HEARST

HEADQUARTERS: New York, NY
EMPLOYEES: 20,000
ANNUAL REVENUE: $10.7 Billion

DIGITAL TRANSFORMATION BRINGS NEW SECURITY CHALLENGES

Four years ago, as the historic and venerable Hearst Corporation underwent a digital transformation, it became obvious to company executives that a more strategic, centralized security effort was required. David Hahn arrived on the scene as the company's first Chief Information Security Officer. Now, Hahn's task is to drive a more strategic, centralized approach to cyber security for Hearst's more than 300 unique operating businesses.

Hahn works closely with Hearst's Chief Technology Officer to map security to business strategy for the entire organization. "Security starts with business strategy," says Hahn. "Business strategy sets what you need to get done. For our industry in media, the world has changed. Technology has evolved and the needs of viewers and readers have changed. Hearst went through a real transformation to become a digital company. As a result of the transformation, we face new threats that make security a much bigger priority. For us, security is all about protecting and enabling availability for our media properties. We need to protect our data while operating without disruption."

"Due to strong CTO relationships, it is easier for me to work with the business partners and explain how security can help them. The important thing is making sure the business partners understand that we want to enable them with security."

- DAVID HAHN

Prior to Hahn's arrival four years ago, security was handled at the individual business level. Information Security Officers (ISOs) at each organization ran unique security programs. With Hahn in place as the central CISO for the global conglomerate, the business ISOs are tasked with more operational and tactical security efforts. Hahn and his team run what is essentially an information security services team at the enterprise level, setting strategy for the company. It is a geographically distributed model that ensures corporate data is protected, standards are met, and individual business needs

SECURITY COSTS RISE WITH THE CLOUD

> “The cloud is transforming IT and it will certainly change operations. While it is seen as a cost-saver for IT, it is not yet that for security. In fact, it’s a reason security costs will continue to rise,” predicts Hahn. “It is another thing for security to have to cover. Every business still has on premise systems, we cover legacy systems, data centers, infrastructures and networks. Now we are also figuring out how to secure the cloud - this requires even more capabilities from our team. Nothing gets eliminated when you move to the cloud, things just add up from a security perspective. In the long run the cloud strategy will save millions, but today we are not there.”

are addressed.

The sheer size of Hearst and its organizational structure are both a challenge and inspiration to Hahn and his team, who took the position at Hearst seeking to expand his expertise. “The challenge was how to build a successful security program with more than 300 different businesses. We are in media, healthcare, financial services. We have 33 TV stations, and for them, availability is everything. There is no one simple security solution to address everything. It is very fulfilling work to be on the front lines of security protecting a business like this,” says Hahn.

Hahn prioritizes understanding the company’s goals, and understanding management and their expectations. He continues, “My role is to be strategic. I cannot get too tactical, but at the same time I must have a broad program. We are always moving forward. I do not want to try to predict the future, but I always need to examine my objectives against what has changed. In a digital transformation, and in cyber security, things are always evolving, so we constantly need to be looking forward to make sure we are addressing things appropriately.”

“No one ever hires a CISO when everything is perfect,” Hahn points out. “But you cannot come in feeling like a hired gun and install a bunch of solutions to fix problems without first understanding business strategy.”

DISTRIBUTED ORGANIZATION WITH A DEEP TEAM OF EXPERTS

Like many CISOs, Hahn says the secret to a successful security program is the team in place. The unique model at Hearst equips Hahn with several skilled team members, a deep bench of ISOs, and a large network of CTOs and business partners at each distinct organization.

“One person cannot do everything,” says Hahn. “But I do believe that one person can make a difference. While I focus on strategy and where to go in the future, I am very grateful to have a large team of contributors who are focused on the right areas and the particular controls that we need.”

He explains, “I spend a lot of time with the CTOs at our various business units. The CTOs really understand what I am doing and together we look for effective integration points. Due to strong CTO relationships, it is easier for me to work with the business partners and explain how security can help them. The important thing is making sure the business partners understand that we want to enable them with security.”

Security awareness is high at all of the Hearst organizations. “Today, every company, no matter how big, is focused on security. No one is immune to the internet. Every business leader is looking to me for guidance on what to do. What can we control, how do we make changes to protect and enable our business? There is no resistance, we work smartly together as partners.”

Hearst’s organizational structure provides much autonomy to the business units, and some of the ISOs report into their own CTOs. “As an enterprise we are connected via shared services, so I provide security services out to the businesses. While the ISOs focus on business specific challenges, such as managing HIPAA or compliance requirements, I focus on the back end infrastructure, the network and enterprise security. If a business unit has a legacy product in place that is working well, then they continue to use it. When it is time to overhaul or introduce a new security technology that is done by my central team.”

Hahn reports up to his own CTO, who reports directly to Heart’s CEO. “I produce a monthly Key Performance Indicator (KPI) deck. Right now it is 50 pages because we try to show all the different pieces. The KPI deck works to educate the team, and let them know what we are handling. They are not interested in hearing about the problems, they want to know how we are managing the problems. For example, it includes our mean time to detections and mean time to resolution,” explains Hahn. As Hearst continues its digital transformation, Hahn’s security team is laser focused on detection and resolution of security incidents, to enable business growth.