PROFILES IN
CONFIDENCE

TIM MCKNIGHT
CISO, THOMSON REUTERS

HEADQUARTERS: Toronto with offices globally
EMPLOYEES: 45,000
ANNUAL REVENUE: $11.2 Billion

"Someone called me the CISOs' CISO, just because I have been at it for so long," says Tim McKnight, CISO at Thomson Reuters. In an emerging field, where as many as 80 percent of CISOs are in the position for the first time, McKnight stands out as a veteran with a multitude of best practices to pass along. He says, "I've been a CISO for 16 years and before that I was a special agent with the Federal Bureau of Investigation." McKnight even helped create the first high tech crime unit, the precursor to cyber security, for the FBI in Philadelphia.

In his career, McKnight has seen the role of the CISO progress dramatically, from a back office position to a critical role in the company, helping to map strategy and align security with business goals. He says, "In the early days, the CISO was more of a network security person in middle management. But now we have progressed to have a seat at the [executive] table, and an important voice with the CEO and the Board. It feels like the progression happened over night, but that's not true."

After nearly a decade in the FBI, McKnight took on CISO positions at Northrup Grumman, Fidelity Investments and GE. He has been the CISO at Thomson Reuters for a little more than three months.

"What drew me to the position at Thomson Reuters is the growth trajectory, both for the company, and for myself professionally. The team at Thomson Reuters recognizes that security is on the forefront of enabling growth. Our customers include big banks, accounting and law firms. These are institutions that honor trust and demand integrity. At Thomson Reuters, trust is highly valued and information security is critical for our customer. For me, there is an opportunity to raise the bar and make security part of the value proposition to our clients."

A PROVEN PROCESS FOR THE FIRST 90 DAYS

McKnight has a standard process he deploys when approaching any new CISO role, and in his first 90 days at Thomson Reuters he's worked through that methodology. "It's a traditional approach – people, process, technology, in that order," says McKnight. "In the first 90 days we put a focus on the leadership team and the skillset of our overall team. What are the gaps we have in our skill set? What are our needs for the future, such as the cloud? We did a market analysis of the competition. What do we need to do to attract, retain and develop talent? All of this is a catalyst to move our security team forward."

" The greatest business advice I ever received was from a 92-year-old founding partner at a Financial Services firm. He said to me, 'Tim, you can never know the influence or authority of a person based on where they are in the org chart. There are folks in every company who drive the company. Seek out those folks, they are not just the executives in your line of sight. "

He continues, "Then we look at our processes and answer a series of questions. How do we prioritize risk? Are our processes mature and value add? Do these processes mitigate risk to the company? What is the role of the team in risk management? What do our lines of defense look like?

"Lastly we look at the technology portfolio. Where do we have duplication? Does our technology align with our future strategy? Are we getting the greatest use out of our investments? Once those questions are all answered, then we go into planning for the year."

ADVICE AND CAUTIONS FOR NEW CISOS

While this is not McKnight's first transition into the CISO role, he is still cognizant of the challenges new CISO's face. He says there are three especially difficult aspects to taking on the CISO role for the first time:

1. LETTING GO
"So many CISOs come into the role from a technology or network backgrounds where we are hands on technically. It can be hard to let go of the technical functions. But, the CISO position requires management skills, communication skills and business strategy acumen, so it's a real shift in focus for a lot of first time executives."

2. LEARN TO TRUST YOUR TEAM
 "When you move from a tactical day-to-day mindset to a strategic view you have to trust your team to keep the daily efforts moving. A CISO's role is about framing challenges, identifying resources and funds, developing strategy and communicating with the larger organization. "

3. COMMUNICATION AND TRANSLATION
"You can't speak like a technologist anymore. CISOs need to translate cybersecurity issues into business risks that CEOs, CFOs, General Counsels and the Board can understand. "

For new CISOs facing these challenges and the daunting work of starting in the role at a new company, McKnight offers this advice, "Identify your key stakeholders across the company, what I call the "super nodes". Those are the

people who can torpedo a project without notice or help you become successful."

McKnight continues, "The greatest business advice I ever received was from a 92-year-old founding partner at a Financial Services firm. He said to me, 'Tim, you can never know the influence or authority of a person based on where they are in the org chart. There are folks in every company who drive the company. Seek out those folks, they are not just the executives in your line of sight.'"

McKnight recommends adding those individuals with special influence to an information security counsel or committee so that they are "part of the parade, not sitting in the stands."

The more traditional executives, such as the CIO, CEO, CFO and General Counsel make up McKnight's "Sphere of Influence". These are the people any CISO needs on their side in order to be successful. McKnight recommends approaching them with specific goals in mind. Ask for their support, and request their help on two or three specific initiatives.

THE IMMEDIATE FUTURE OF INFORMATION SECURITY

McKnight says that there is always the next thing to figure out in security, it is not a problem that is ever solved. As a CISO you must embrace change now more than ever before. Organizations are going through significant transformations and CISOs need to be in the driver's seat of this change.

McKnight believes the cloud continues to be a massive trend that requires a large investment from security. His team is constantly reviewing how to better secure the cloud, limit gaps and improve automation related to cloud security. According to McKnight, other big trends for the next year are artificial intelligence and analytics. The Internet of Things will continue to be a large focus as people, cars, homes and life are increasingly connected. Security and privacy efforts will continue to converge, creating new challenges for organizations and their clients.