# STEPHANIE FRANKLIN-THOMAS

**SVP & CISO**
**ABM Industries**

**HEADQUARTERS:** New York, NY

**EMPLOYEES:** 100,000+

**REVENUE:** $6 Billion

Stephanie Franklin-Thomas' career in IT and security spans over 25 years, garnering her keen business and technical skills to strategically mature security programs and continually protect organizations. She leads her teams with a focus on open and authentic communication, creating collaborative environments poised for success.

Stephanie does not have a traditional technologist background and did not initially set out to work in IT or cybersecurity. She says, "I'm a product of being involved in a number of different engagements and activities throughout my career that led me down the cybersecurity career path."

Right out of college, Stephanie joined a large oil and gas company as part of their customer service operations center, and one of her first assignments was to work on a large enterprise resource planning (ERP) implementation. This was her introduction into the world of technology, and she quickly recognized how much she enjoyed and excelled at this type of work.

After moving into more IT-focused roles, she found herself working at one of the Big Four accounting firms at the same time as Sarbanes-Oxley was gaining traction. This enabled her to lean into compliance-focused cybersecurity functions assisting organizations managing through the new reporting regulations.

For the past year, Stephanie has worked as the SVP and CISO at ABM Industries, with a focus on driving IT strategy and transformation, building a strong security culture, and delivering impactful security solutions.

## TRANSITIONING INTO LEADERSHIP ROLES

As Stephanie progressed in her career, she was able to move into cybersecurity leadership roles, by leveraging her strong business background to achieve success. She explains, "I came from an environment where I was working in the business. I became the liaison between the business and technology teams, conversing with technical people about their work and then turning around and translating it into business speak for our leaders. Having the ability to essentially speak two different languages is a strength. Thus you are quickly elevated into those roles that are more leadership-facing to create understanding."

After spending the majority of her career in oil and gas, she was excited to transition to ABM Industries where she would have exposure to different businesses which look at cybersecurity in various ways. She comments, "ABM was interesting to me because it has five industry groups and the approach that could be taken to support these areas. I always use the analogy when I talk to leaders that we are trying to protect what's important to us – so we don't want to build a million-dollar fence to protect a $20 horse. In cybersecurity

you want to understand what is most important or what is most valuable. Once those variables have been identified, the focus becomes clearer on what goes into building your cybersecurity program and addressing the needs of the organization. At ABM, the real assets are the people, unlike manufacturing organizations where there is a keen focus on the products. Our people are the assets we are protecting. This was an opportunity and an approach to a very different aspect from my previous roles."

## BECOMING A BUSINESS ALLY

Stephanie believes successful and strategic CISOs should always strive to have a seat at the table with business. She says there are still many organizations who view cybersecurity as the police, she analogizes – when you need them you call them and they come and everyone is happy, but when they pull you over for speeding, you don't want to see them. She continues, "At times, the business sees cybersecurity through that lens, thus the teams are not invited to the table. It is important, whether it is a transformation effort or otherwise, that cybersecurity has a seat at the table and a voice when projects are in development. You do not want to get so far down the path and implement something that is not secure, or it is going to get held up to ensure necessary security features are enforced to protect resources."

At ABM, cybersecurity has a seat at the table to truly understand what is happening in the organization and to provide guidance for any innovative projects, according to Stephanie. She comments, "It goes back to creating rapport with the business. Establishing that connection shows them what your teams have to offer, and leaders have the ability to bounce ideas off you before they move forward with projects. With the recent launch of ELEVATE, our long-term strategic priorities, we know our focus will be on elevating the client and team member experiences, and ABM's use of technology and data. The collaborative efforts between the business and technology teams will strengthen our efforts around transformation. Our unified goal is for ABM to continue being a leading provider for integrated facility services in the near-term and future, and cybersecurity will be a strong ally for our organization and clients."

When presenting cybersecurity updates and key data to boards, Stephanie tailors her presentations to match her audience. Her extensive experience presenting to boards and executives enables her to ensure meetings are productive. She explains, "Leaders receive information in different ways. The key to success is getting to know your board or your audiences and approaching them with the content that resonates best with them. Some leaders may be most interested in the narrative, others may want to focus on data visualization and some executives may just want to dialogue with you about what we are currently facing. The tried-and-true way to have effective communication is by adapting your message as needed."

> *"The key to success is getting to know your board or your audiences and approaching them with the content that resonates best with them."*

## PEOPLE: TOP ASSET, TOP THREAT

Stephanie says an organization's greatest asset is their people, which may also be their biggest threat. She believes it is the way in which people interact with their environment that poses significant threats. She explains, "Most of your security vulnerabilities happen because someone did or did not do something, it all drives back to an individual."

When asked about the balance of people, process, and technology in addressing threats, Stephanie says, "All three are equally important, as you must have the policy and/or standard in place, educate and train employees on best practices and implement the technology to support. Your underlying automation is the guardrail, so processes are enforced, and no workarounds are available."

## CELEBRATING WOMEN AND DIVERSITY IN CYBERSECURITY

"I recently attended a CISO meeting and at one point I looked around at the attendees and thought to myself, 'WOW, every person in the meeting is a woman.' I was so accustomed to being the only one in the room, either the only woman or the only minority, that I had a moment of amazement. To see all these different women working in the cybersecurity world, I'm impressed with how far the industry has come in recent years and in awe of the diversity I see within my own team," says Stephanie.

Women now account for 25% of the cybersecurity workforce (according to ISC2), but Stephanie believes more could be done. She recommends that leaders striving to develop more diverse teams should consider creating an environment where all members at the table have unique differences. For potential talent looking to join an organization, being able to identify with someone who resembles them could be a factor in their decision to accept an offer. This also extends to how companies engage with students or young professionals, especially women and minorities, about opportunities in the technology space. This awareness could open the doors for someone who never knew this could be a path to a successful career. Stephanie hopes more women and minorities will step into CISO and other IT leadership roles in the future.