PROFILES IN *Confidence*

KAREN HIGGINS-CARTER

Executive Vice President, Chief Information and Digital Officer

GILBANE, INC.

HEADQUARTERS: Providence, Rhode Island

EMPLOYEES: 3,100+

REVENUE: $6.3B annual revenue, Gilbane Building Company; $8.5B total development, Gilbane Development Company

Karen Higgins-Carter, CISSP, NACD.DC is an engineer by training who spent most of her career working in information technology. She mainly focused on roles in the financial industry, gaining deep exposure to cybersecurity as it relates to protecting data, maintaining trust with customers, and adhering to regulatory requirements. After 20 years in finance, Karen decided to make a transition to join Gilbane, Inc., a family-owned company that provides real estate development, global integrated construction, and facility management services.

Moving her career into a new industry was exciting for Karen, and she felt the transition to Gilbane would enable her to continue to grow professionally. She explains, "I felt from a values perspective, Gilbane made sense for me. It has a family-owned culture that really cares about people, and also a culture of safety, which is very similar to cybersecurity. Gilbane has built some of the largest and most complex projects on the planet. I am truly impressed by our team of experts, and how they build these complex buildings. From a technology perspective, it's easy to work with stakeholders who know how to build things and also appreciate the need to manage risk."

As the Executive Vice President, Chief Information and Digital Officer, Karen is responsible for optimizing the value of innovation, digital, analytics and AI, technology, and cybersecurity. The role was newly created one year ago to ensure a single point of accountability for these related areas in the company, with a focus on digital transformation at the center. The structure of her responsibilities is comfortable to Karen because risks related to digital strategies are cybersecurity in nature and to have one executive oversee those areas, it is easy to make risk-adjusted strategic plans and execute through a risk lens.

COMMUNICATING RESPONSIBLY AND EFFECTIVELY

Karen is responsible for reporting on cybersecurity to the executives and the board. She comments, "To effectively communicate, you must put yourself in the shoes of the audience and understand the responsibilities of the board. I sit on the board of another company, so I think about the board member perspective and how they are stewards of the company and its future. Boards care about the shareholder value over the long-term, ensuring there is the right strategy, resources, and risk management approach in place."

She continues, "My advice to CISOs is to not speak in terms of technical controls and what you do every day, but communicate how cybersecurity risk is realized as any other type of business risk. In fact, we manage risks related to confidentiality, integrity, availability, and related control failures and those manifest themselves as operational risk, operational losses, reputation impacts, legal, and compliance risk. A mentor once told me that a risk is not the absence of a control. Framing the message in terms of how would the absence of that control impact the business can be a powerful way to communicate the value of our efforts."

"My advice to CISOs is to not speak in terms of technical controls and what you do every day, but communicate how cybersecurity risk is realized as any other type of business risk."

When anticipating questions from board members, Karen suggests being prepared to speak on emerging risks, things they might have read about in the news and apply those to what is relevant to your own organization. When working with the board, Karen likes to share management's perspective and welcomes board insight and advice.

RISKS RELATED TO DIGITAL OFFERINGS

A top focus area for Karen and her team is to proactively mitigate and identify emerging risks related to digital offerings the organization is developing. It requires managing both how they compete with the digital offering, and how they concurrently manage risk in the offering.

She explains, "Our innovation team has developed a methodology for experiments and what we call the experiment canvas. Through that tool, we identify not only the potential of an idea, but some of the inherent cybersecurity risks we would need to control through the experimentation process."

Karen continues, "It's tempting to work with startups, but many are not 'enterprise ready' to safely manage sensitive data. It's important to balance the potential rewards of innovation and experiments with the cybersecurity risks. As a control function leader, you need to also serve as an enabler. You have to understand what the business goal is and how you enable success in a controlled way. With that in mind, you can come up with collaborative efforts to reach business strategies and goals while managing risk."

LEADERSHIP AND HIRING

Karen's team manages everything from innovation to cybersecurity, and to ensure she maintains effective leadership, she believes in being hands-on, which includes visiting actual construction sites in person, or the "frontline" as she calls it. She says, "I've been out to our construction sites on a regular basis over the past year. You learn a lot about how technology is used in the field. On our job sites, our teams are managing construction work performed by our trade partners. You really must walk in their shoes and experience their work environment to understand how technology is being leveraged, what the cyber risks are, and if shortcuts are being taken. It's important to bring their perspective into how to help them protect and manage risk."

When looking at the cybersecurity team and the abundant lack of talent in the industry as a whole, Karen believes in developing people to combat this skills gap. It comes down to efficient training, development, and coaching, in order to grow individual skillsets in the cybersecurity realm. Karen comments, "You're kidding yourself if you think you're going to hire yourself out of a skills gap, you have to develop it. You can find people who are good developers and encourage them to move into cyber. You can find people who are good process leaders who can help with the risk management aspects of cybersecurity because all controls operate within the context of a process. If you find a good process person and teach them about risk and enterprise risk management concepts, they can be helpful. Staffing cybersecurity teams can be a struggle if you're looking for a unicorn that doesn't exist. I find that part of my responsibility as a leader is to put together the team, that should collectively have all the skills. Then I can coach and develop the team in areas where individual team members may need support."

"Our innovation team has developed a methodology for experiments and what we call the experiment canvas. Through that tool, we identify not only the potential of an idea, but some of the inherent cybersecurity risks we would need to control through the experimentation process."