PROFILES IN *Confidence*

DONNA ROSS

CISO
RADIAN GROUP, INC.

HEADQUARTERS: Wayne, PA

EMPLOYEES: 500+

REVENUE: $250 Million

As early as Donna Ross can remember, she was interested in taking things apart and fixing them, and this curious mindset has helped in her extensive and successful career in cybersecurity.

Her career in security happened somewhat by chance, when she was volunteering at a food bank and met someone who worked in security, and who eventually became her mentor. Through this mentor relationship, Donna was offered her first security job. She explains, "I was in marketing, I had a degree in economics. But I met someone who worked in security and I asked him if he would be my mentor. He agreed. And we started working together and maybe three months into that mentorship, he invited me to join his team, and I said to him, 'I know nothing about security, but I'm eager to learn.' Subsequently I've gone back to school and achieved some key security certifications."

She continues, "My life lesson and my foray into security was: first asking for help, but secondly, when someone in a leadership role sees something in you, you may not see it in yourself. So take that job, take that role, and be the best you can be, because I think a lot of times women career-limit themselves when they see a job description. I know there have been studies on this, we tend to look at it as a checklist. I can do this. I can do that. I could do this. I can't do this, so I won't apply. Where men will look at that same job description and are happy if they meet 60% of the skills and they'll go ahead and apply for that job. I guess in my case, I realized my mentor believed in me. I liked him. I knew I could learn from him, so I quickly realized I should take the job. And that's how I got into security - I didn't choose it, it chose me."

Her background in marketing, economics, and a business school degree helped Donna make an easy transition from technically focused roles into more leadership driven roles. Currently the CISO at Radian Group Inc., a mortgage insurance and real estate services company, Donna is responsible for the overall information security program, protecting the data that is entrusted to them by customers, partners, employees, and counterparties. Her team is broken into three distinct groups, as she explains, "I have an information security technology team and a leader that runs that reporting to me. We also have an information security operations team, focused on operational tasks and incident response. And then I have an information security governance risk and compliance team that really is focused on assurance, compliance, awareness and training, and all those non-technical components."

WHAT CISOS ARE FOCUSING ON

Donna says cyber leaders should be focused on four things looking forward. One is reducing the attack surface and considering a zero-trust model where you trust no one by default and are continuously verifying access. Another area is focusing on ransomware readiness and cyber resiliency, including incident response readiness, backup and recovery strategies, and employee training. The third area is cloud security, specifically because regardless of what kind of cloud, it's a shared responsibility model. It is important for CISOs to better understand what their responsibilities are and what the service provider's responsibilities are in those cloud instances. Lastly, supply chain security is key, with a focus on having a rigorous vendor risk management program and process looking at single points of failure and continuous monitoring. There have been a barrage of data

"My life lesson and my foray into security was: first asking for help, but secondly, when someone in a leadership role sees something in you, you may not see it in yourself. So take that job, take that role, and be the best you can be, because I think a lot of times women career-limit themselves when they see a job description."

breaches within supply chains that could impact anybody that uses that product or service, so it is really important to ensure you are prepared and proactive in your approach.

By focusing on these four areas, Donna believes CISOs and security leaders alike can help advance their programs in a mature and risk reducing manner.

EFFECTIVE COMMUNICATION WITH EXECUTIVES

Donna believes in transparent and honest conversations. She comments, "I am highly transparent whether I'm reporting to any of our internal committees or whether I'm reporting to the Executive committee or even the Board of Directors. The key is being honest, being transparent, and talking in terms of risk. What I talk about is not necessarily information security, it is all about how we are managing risk, and then to keep it simple I avoid talking to them in technical terms. I try not to talk in zeros and ones, I try to make it more of a conversation. Anytime you're in a technical area, you know you do a much better job when you can speak in business language. It is important to speak in terms of dollars and risk to the business."

Throughout her career, Donna has had the privilege of briefing the board, whether it was annually, quarterly, or monthly. She says the best approach is always to do your homework – research current events or things they may have read in the Wall Street Journal, and to know who the members are. She shares, "I need to know other boards they are on, so I'll do some research leading up to the board meeting. Have any of their organizations been in the paper? Has there been an event, have any regulations changed that align with their area of expertise? I spend a lot of time in the months, weeks, and days leading up to the board meeting, doing my homework to avoid surprises. My first advice is to know your board, know what they do, know what they care about, and know what's going on in the news. And the other thing is if they ask me something and I don't know, it's okay to say I'll get back to you. I'm very honest and open with them."

PROACTIVELY APPROACHING CHALLENGES

For the cybersecurity industry as a whole, Donna believes outside of budget and people, that CISOs should focus on external factors that could impact their program such as the threat landscape or geopolitical factors. She says to think about what is going to happen with the US election, what are the different scenarios should one candidate win versus the other? Donna also shares that it is important to consider evolving areas like Artificial Intelligence and how it might be used by bad actors. The compliance landscape is another challenge – to better understand how it is changing and how to be one step ahead of these changes.

THE VALUE OF MENTORSHIP

Donna considers herself a visionary leader, someone who prioritizes not just her needs, but those of the company and her team to ensure their development and well-being is considered. She learned a lot from her early mentor and strongly believes in finding a mentor to help guide you in your career journey. She

"I am highly transparent whether I'm reporting to any of our internal committees or whether I'm reporting to the Executive committee or even the Board of Directors. The key is being honest, being transparent, and talking in terms of risk."

comments, "Find that mentor, that coach, that advocate, and make sure you can articulate a really clear vision. Through mentorship you are able to create a commitment aligned around shared goals and shared growth that encourages innovation and forward thinking. I've mentored many people over the years and my goal is to help guide them in achieving the goals they have set for themselves."

She always looks at how she can motivate and influence her team to drive better results and create an even stronger culture. To continue to grow as an individual, Donna seeks feedback, is constantly learning, participates in networking, and engages in self-reflection and self-assessment.

Donna belongs to a number of professional groups including CISO and analyst communities. She also has an extensive group of CISO peers she can call up and problem-solve with. She explains, "We don't talk about anything like technology pricing, we talk more broadly about the problems we are facing. We share things like how we solved certain problems, lessons we learned, how we would have done things differently, and other relevant things. Having this amazing Philadelphia CISO network that I'm part of has been rewarding because we are all incredibly interconnected. We have known each other for a long time. Most of us have been around for years, so even if I'm going to a conference, I have a distribution list on my cell phone with everyone's number and I'll just check who's at the conference and ask, "Do you want to meet up later and talk about what we learned?" So, we're very fortunate in this community and in the Philadelphia area where the CISOs and the security folks are very tight knit and we support each other and help each other out."