PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MEG ANDERSON
CISO, PRINCIPAL FINANCIAL GROUP®

HEADQUARTERS: Des Moines, Iowa

EMPLOYEES: 15,000+

ANNUAL REVENUE: $13.9 billion in GAAP revenues, $1.5 billion in non-GAAP revenues, $2.4 billion net income

> "I am constantly challenged and busy here, and enjoy that pace and energy. We are currently number four on the Forbes list of America's Best Employers (2018) and I truly believe it is a wonderful place to work. I am surrounded by an engaged and diverse team who understand how they impact our customers and business. Given the cybersecurity talent gap, the fact that our team has an average tenure in the 15+ years range is amazing."
>
> **- MEG ANDERSON**

Meg Anderson, CISO at Principal Financial Group®, a global financial investment management and insurance organization, possesses a unique background and exceptional leadership experience. Anderson began working at Principal® in 1987, working her way up the organization while holding a range of IT roles. In these roles, she handled a diverse set of IT issues and strongly built up her business practice experience. Her initial glimpse into information security occurred when certain components of her responsibilities exposed her to a variety of regulatory aspects of privacy and HIPAA, some time before information security became widely prevalent in organizations. In 2008, Anderson was approached about an opening for the CISO role, something she somewhat blindly agreed to, without understanding every facet of what the job entailed.

Anderson says, "I had no idea what I was getting myself into. My experience with HIPAA and privacy laws helped me understand some components of security, but I didn't understand the full breadth of information security at the time. However, having some business unit background allowed me to consider the impact of our evolving security program on our business strategies and to be in a position to use that context as we strengthened the program in the face of increasing external threats." Throughout her career, she has experienced tremendous growth as a business leader and evolved into a well-versed information security expert.

Anderson links her 30+ year tenure at Principal® to the strong company culture and fast-paced, challenging nature of work. She comments, "I am constantly challenged and busy here and enjoy that pace and energy. We are currently number four on the Forbes list of America's Best Employers (2018) and I truly believe it is a wonderful place to work. I am surrounded by an engaged and diverse team who understand how they impact our customers and business. Given the cybersecurity talent gap, the fact that our team has an average tenure in the 15+ years range is amazing."

Longevity at Principal® offered Anderson advancement in both a personal and professional capacity. She explains, “From a personal perspective, I’ve learned how to interact with executive management better, up through the CEO, board and audit committee, something I didn’t have exposure to before. Professionally, I’m at a point where these audiences are asking questions and engaging with me more than ever before.”

CUSTOMER TRUST AND INNOVATION

Customer trust is a core component at Principal®, and the information security program holds a prime position to ensure this remains consistent. Anderson states, “Like many companies, we have lots of pressure to make sure we are not the next company in the news. Aside from reputational risk associated with a breach, we operate our business on customer trust by making sure we keep their data and money safe. The amount of investment security receives has increased, which is partially fueled by our digital business strategies.

For Anderson, one aspect of digital transformation is improving customer experience to offer faster and more seamless interactions and the ability to quickly resolve any needs. She comments, “I would describe digital transformation using words like velocity and agility. Things are moving at a fast pace as we innovate and use data in new ways. We need to think about things like providing solutions that scale for larger customers, and offering secure and innovative solutions to grow revenue and our customer base. The bottom line is continuing to earn customer trust throughout this transformation.”

While many CISOs experience struggles to ensure security is involved in initial planning and conversations about digital transformation, Anderson believes in security being an enabler of innovation to solidify that speed and trust are baked in. She says, “We need to work security into the process from the start, make sure it’s built in by design and not a bottleneck on the backend. Doing so saves time and money.”

To accomplish this level of alignment and enablement, Anderson says you must understand why the organization is deciding to innovate or create new products and services for the marketplace. She believes once you understand this, it is easier to help those driving innovative initiatives in the organization. In doing so, you can demonstrate how the information security component will ultimately help them get to the end goal quicker, or avoid having to redo any aspects of their project. Anderson explains, “You cannot throw information security policies at someone and walk away. You must understand their business objectives and what they are trying to accomplish. There’s flexibility in collaboration, which leads to quicker achievement of the goals”

BUSINESS-FOCUSED METRICS

As a seasoned professional with many years of experience reporting and presenting to the board, Anderson relies on specific, business-focused metrics. She does not think Boards want CISOs to report every incident to them, but instead, barring any significant events, share select minor incidents so they gain a sense of what is happening, why it is happening and the response process. She says, “The board needs to be confident that if an incident occurs, we have a comprehensive process in place that includes the right people.”

Anderson uses board discussions as opportunities to educate members quarterly on any relevant news of interest. She explains, “For example, if ransomware is increasing in the news, we help the board understand what it is, what we are doing to protect ourselves ,and give them a level of confidence that we are doing what we should be doing.” She suggests other relevant topics to educate the board on may include identity and access management, the regulatory landscape, threat intelligence, and supply chain risk.

EMPOWERING TEAM MEMBERS

As a leader, Anderson believes in a strong company culture and enabling her team to feel empowered, to instill passion and commitment. She comments, “We embrace diversity and flexibility. Most team members can work from anywhere. We also empower our team, they are encouraged to have two-way conversations and a voice of their own. I’m a big believer in healthy debate and open dialogue for problem solving and to show people they are valued.”

Anderson puts a heavy emphasis on building the next generation of leaders. She values recognizing the need to develop successors and prepare cyber leadership for the future within her own company. By doing so, she aspires to make an impact on the upcoming group of information security leadership.