PROFILES IN *Confidence*

HUGH TOWER-PIERCE

CISO

MILLENNIUM TRUST COMPANY

HEADQUARTERS: Oak Brook, IL

EMPLOYEES: 1,000+

TOTAL ASSETS UNDER CUSTODY: $55 Billion

Hugh Tower-Pierce has over 23 years of experience in both technical and people management roles, with the majority of his career spent working in health insurance, health/tech and financial-related businesses.

Hugh currently serves as Chief Information Security Officer (CISO) for Millennium Trust Company, a leading provider of health, wealth, retirement, and benefits solutions, serving over 5 million customers nationwide. He has been in this role for four months and pursued the position because of the unique opportunity to work at a company that helps people plan, save, and invest. Due to his background in both finance and healthcare, Hugh felt this company and role would give him exposure to familiar verticals, but also introduce a new set of security challenges and opportunities to explore.

Organizational support is important to Hugh, as he believes a security program is more successful when it is backed by not only the executives, but across the business as an intrinsic part of the company's culture and shared goals.

RESPONSIBILITIES & FOCUS AREAS

Hugh is responsible for typical security program areas including security operations, incident response, governance and policy, due diligence (inbound and outbound), application security, identity, and compliance. To accomplish the security program goals while continuing to support the business, Hugh has identified major focus areas including assessments, identity, and application security.

For assessments, Hugh notes, "We spend a lot of time on the assessment piece. There is a lot of due diligence for acquisitions, which take time, and we focus on assessments related to compliance like PCI, SOC, and HIPAA. The due diligence we do on vendors looks conceptually and procedurally similar to customer assessments, which also relate to compliance assessments."

Application security is another area of attention. "We are partnering on customer identity issues, and also focusing on how authentication works across multiple product areas, the architecture of products between our mobile and web properties, and making sure we engage with our product team," says Hugh. To ensure security is baked into the SDLC, Hugh focuses on transparency, engaging with the product teams on an on-going basis. This results in better communication and more understanding in the value of security as part of the development process, avoiding any surprises or delays.

One challenge Hugh and his team face is security inherent to acquisition activity the organization has been involved in. Hugh explains, "There's some version of independent environments that present strategic and tactical challenges. You must think through them from a security and business perspective when it comes to both the user and employee experience and having a common set of standards across those environments. If we acquire a business, we must make sure we are looking at the distinct risk challenges and how we can operate as one company and apply one set of standards across the board. There must be a consistent security strategy to support this kind of rapid growth."

AI POTENTIAL & RISKS

Hugh believes there is a huge potential for business opportunities, occurring across both big and small use cases when it comes to AI. He explained, "The individual could benefit on a day-to-day basis with small but frequent use of AI for particular tasks, while there are also opportunities at a larger scale doing such things as data analysis to optimize services. Regardless of what security issues or risk may surround AI, we must adapt to it."

He also acknowledges what to look out for, and comments, "One of the main things to be aware of is the potential for data leakage which may exist as an acute concern

when early in adoption lifecycle. Right now, because of the way companies have been slow to react, lots of people are using generative AI services outside of any framework. The resulting fear is that this unmanaged use can lead to data exposure. At Millennium Trust we're taking steps to manage these risks while investigating how best to incorporate AI services to the benefit of our employees' productivity and value we provide clients. Beyond data leakage, there are ethical and bias concerns with AI. Broadly speaking many organizations are finding themselves behind already, with their workers using it in an ad hoc fashion, and companies scrambling to identify what their specific opportunities and risks are."

Hugh also believes vendors are late to enter the AI discussion. He describes an 'AI arms race,' and has been in discussions with security tooling vendors about AI-related threats. However, he feels most don't have strong answers yet, they're still late in identifying what those risks might be to their products. An outcome of this might be that AI resistance or AI features become part of the vendor selection criteria. Hugh plans to continue to bring the topic up with vendors and ensure he remains vigilant with research and trending data around AI.

LEADERSHIP APPROACH

"My philosophy is that if I can hire and develop good people and give them the space they need, they tend to succeed. I will always make sure I'm there as a safety net if something happens, so I can provide a more hands-on approach or guidance as needed. I am normally naturally calm and like to bring stability to situations, which I've found helps in certain types of work like incident response. I also prioritize trust, a big factor in how I lead and build a team," Hugh says.

As a part of his own growth, Hugh discovered the importance of self-awareness and vulnerability as a way to connect with others and develop as a better leader. He focuses on receiving feedback in a non-defensive way and leaving (professional) fear at the door to continue to develop as a leader. He emphasizes being authentic and honest with people and staying grounded as much as possible. Mentorship has always been important, and Hugh believes in seeking the help and guidance of others to better oneself, as well as providing mentorship to those who can learn from his perspective, experience, and skills.

Activities outside of work also help ensure Hugh is a strong and successful leader. Long distance running in the 50-to-100-mile range helps him spend time outside and process the variety of interesting or challenging issues that come with the job. He's found that the extreme physical and mental effort involved tends to strip away and identify the things in life that are truly inconsequential, leaving only the things that matter. In gaining this kind of perspective, it helps Hugh refine his priorities, whether that be at work or within his personal life.

COMMUNICATING WITH EXECUTIVES

As a security leader who interacts with many non-technical

"In discussions with leadership, and other non-technical executives, I try to meet them where they are and offer them as much as they're interested in engaging on risk and security, while avoiding too many technical terms."

people, Hugh says he must ensure he understands what the business is doing in terms of priority. He explains, "When I'm talking to someone on the finance, product, sales, or customer service team, it's important to empathize with what their challenges are, what they're trying to solve, and what the term "success" means to them. It's also important to interact with them from the perspective of the business, and not only focus on security. As a security team we can't operate in a vacuum, we don't exist in the company just to practice security for its own sake; we exist to enable our colleagues to do what they need to get done in a safe way and to foster trust with our customers."

He continues, "In discussions with leadership, and other non-technical executives, I try to meet them where they are and offer them as much as they're interested in engaging on risk and security, while avoiding too many technical terms. I try to put myself in their shoes and meet them on common ground. Security needs to have a positive perception in the company so that we can be most likely to succeed doing our part to foster business growth. It's important to me that we are viewed as partners rather than a source of friction. We must give the right level of feedback and provide trusted and informed counsel on risk where we need to, to mitigate that risk and help continue to build success."