PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JO BENTLEY

CISO & SVP ENTERPRISE RISK MANAGEMENT, BOSTON PRIVATE

HEADQUARTERS: Boston, MA

EMPLOYEES: 764

COMPANY ASSETS: $8.1 Billion

"For us, our biggest priority and challenge right off the bat was stabilizing the relationship between the enterprise and regulatory environments to ensure a sensible approach to security."

- JO BENTLEY

"There is an underlying principle in security to do the right thing," explains Jo Bentley, CISO and SVP in Enterprise Risk Management at Boston Private. She continues, "We are not tasked to do what is convenient or what is easiest, but to do what is right for the organization."

From her first days on the job, this principle formed the foundation for Bentley's approach to security at Boston Private. She explains, "I understood that, like any financial institution, we faced security concerns. We see that quite often in security, where CISOs are hired because there are significant risks that must be addressed."

CREATING AN INFORMED ASSESSMENT

With years of experience understanding the goals and processes of CISO responsibilities, Bentley's first step after joining the company was to evaluate the environment and gather her own understanding of the challenges the organization faced. She stated, "It is important to identify the issues you can see, not as much what you hear, but what you can see from your own analysis. This is how you develop a good baseline for the program."

Armed with support and a strong team, Bentley approached establishing a solid and foundational baseline with a standard as a backdrop (SP 800-53) through leveraging three components. These included interviews, product analysis and review of regulatory outputs.

Bentley suggests concise conversations with various stakeholders as the first step in the process. These conversations should not focus on specific problems, rather on an overview and examination of the environment. Next, she says, "Perform a quick analysis of the products that are a foundation of the program. Understand what products they

are, the problem(s) they solve and their coverage." Finally, since the company is in a heavily regulated environment, Bentley and her team reviewed all audit and regulatory outputs to gain an understanding of what external parties see. She explains, "You can create a decent assessment of the security posture of the environment with those three elements."

IDENTIFYING GAPS IN A REGULATORY ENVIRONMENT

"Once the initial assessment is done, you can verify and validate the findings. From there you can identify the gaps to help you lay out a roadmap of where you need to go," continues Bentley.

She points out that many of Boston Private's initial challenges stemmed from a familiar issue for financial services organizations. "As you can guess, in many financial service companies, security starts from a compliance perspective. Since many CISOs come to security with a risk management approach, this can create fundamental issues when you start interacting with simple processes."

"For us, our biggest priority and challenge was stabilizing the relationship between the enterprise and regulatory environments to ensure a sensible approach to security."

Bentley reports into the Chief Risk Officer, a reporting structure that facilitates the company's move towards a risk-based security program. She explains, "I understand that many assume the CISO will report into the Head of Technology, but to me the Risk Officer makes more sense. Technology is a peer and stakeholder of mine, but security is not just about technology. Security provides the foundation for the enterprise to operate in terms of business functions, processes and interactions. We enable trust and safety in business using a mix of technology, process and people. So, while technology is very important to security, it is not the only entity in the stack."

TAKING A PRACTICAL APPROACH TO THE BOARD

Bentley possesses a strong background of interacting with executive and board members, which continues to evolve as she furthers in her career as CISO. She believes CISOs and security teams consistently hold an important role and perform an overall vital function in Board meetings. She feels the current industry assumption that Boards are elevating cybersecurity to a higher level may be overstated. She explains, "As much as we, as an industry, talk about aligning closely with the Board and collaborating with the Board, we have to remember that we are not the only gig on the block."

She suggests CISOs remember that while cybersecurity may sometimes be an uncomfortable topic for the Board, it is not the only topic they will cover in any given meeting. Bentley explains, "It's not really all eyes on you. Yes, we have an entry into the Board now, but I do not think we necessarily have the spotlight. In most cases there are multiple topics and risk areas the Board will discuss each meeting. Cybersecurity is just one of the things that they care about."

Given the time and bandwidth constraints of the Board, Bentley suggests letting the Board chart the course of the conversation. "In most cases, what the Board wants to talk about may not be what I want to talk about. It is my job to find ways to work that in, while being respectful of time and opportunity. Is the Board interested in what we have to say? Yes, of course. But let's not give the impression that this is easy. Cybersecurity is not the Board's only concern."

While the Board sets the agenda for their conversations, Bentley always comes prepared with reports and metrics outlining the security program's progress. She explains, "We have particular parts of our program that go to the Board for approval. Those include policies and specific programs. The Board is judicious in its review of these items, and they ask detailed questions which demonstrate they have understood and reviewed what is presented to them. They look for updates and progress on the strategy and a go-forward plan. They have informed opinions on strategy."

Bentley explains how recently, her organization's Board and executive teams expressed increased interest in understanding how security may support and enable digital transformation. The crux of the issue is speed. Bentley says, "The executives want to understand how they can embrace digital transformation in a secure environment. They ask, 'as I am trying to go fast, what will slow me down?' They wonder if security will impede the transformation."

Bentley alleviates executive concerns about security constraints by keeping her team focused on enabling the organization to move forward. "We anticipate requirements that are two to three years ahead of the rest of the organization. We listen to their priorities and clear a path forward for them. In this way, we are able to provide the organization with world-class structures and foundational elements so that the company can achieve the level of excellence expected from the overall business strategy."