PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DEB BRIGGS
CSO, NETSCOUT

HEADQUARTERS: Westford, MA
EMPLOYEES: 2,500+
ANNUAL REVENUE: $910 Million

"Security can't be the department of 'no', it can't be shutting down everyone's projects. You want to protect your company and the data and people but at the same time you can't prevent the company from moving forward."

- DEB BRIGGS

From a young age, Deb Briggs expressed a strong interest in learning how things worked and how to take things apart, and this curious, problem solving mindset helped carve her a successful career in security. Her first job out of college was at GTE Government Systems, where Briggs first began understanding how to protect data in the organization. This sparked her interest in privacy of data and is where she gained a strong understanding of the importance of protecting data. She followed a well-defined path to security through IT infrastructure, all while focusing on solving complex problems.

Briggs spent the past sixteen years working at NETSCOUT, where she spearheaded the focus on security, eventually leading her to the CSO role. She explains, "When I got to NETSCOUT I was responsible for all of the IT infrastructure, and security was just piece of it. Security was part of my role, but it's hard when you are doing everything in IT and trying to balance security, risk, and strategy when help desk also reports into you. As the company grew, I was given the opportunity to take off all other hats and just keep security. I've been able to grow the department significantly since then."

Since becoming the CSO, Briggs expanded the security team and has experienced the increasing importance of a strong security program. Briggs discusses the shift of the security industry from being focused on perimeter to now focused on the expanding, constantly moving workforce. She comments, "Today there are so many more people who don't work in brick and mortar offices, they are now working from home and outside the office. NETSCOUT has over 2,600 human firewalls and each one is an active point into my network. There was a strategic shift of what we are protecting and how we are protecting it, and our old tools needed to change and keep up with this shift."

STRONG ALIGNMENT AND COMMUNICATION

The executive leaders at NETSCOUT are very engaged in security and the overall risks to the organization. Briggs has worked hard to ensure security is constantly aligned with the business, and that she is always communicating risk in a cohesive, understandable manner.

Briggs says security cannot be an inhibitor to the business and compares security to the brakes of a car, because without security people may not move as fast as they want to. She explains, "Security can't be the department of 'no', it can't be shutting down everyone's projects. When people come and ask for your support on a new project or initiative like moving things to the cloud, the security team must learn to balance being both agile and secure. You want to protect your company and the data and people but at the same time you can't prevent the company from moving forward."

The key to this approach is putting yourself out in the company and solidifying strong relationships with your business counterparts, something Briggs has worked hard at over her sixteen-year tenure at NETSCOUT. She believes being a strong communicator helps explain risk to the business and business users in order to gain enough budget.

ALIGNMENT AND UNDERSTANDING WITH BOARD MEMBERS

Briggs considers the drivers and projects important to NETSCOUT in order to understand how security can support the overall company strategy. By doing so, she sets herself up for success when discussing progress or initiatives within her security program.

The NETSCOUT board is comprised of some technically-minded members, allowing her to go into deeper program details than most CISOs would during board meetings. Briggs says CISOs should always remember that the board is looking at them to set the tone for the direction of cyber strategy for an organization. She says CISOs must know how to relate to board members and understand what questions they may ask. Briggs continually ensures she is polished, has thought about questions they could potentially ask, and thoroughly understands the needs and concerns of each member.

When updating the board on progress, Briggs leverages an agnostic third party that provides risk scores based on vulnerability scans. She explains, "I don't control the risk score from our third party, but what my team does can impact it. We can do things to affect that score, but I can't just call up and make it happen. Our board has faith in that third-party assessment because they get a sense of how we are doing from a vulnerability and risk perspective."

Whether she's asking for additional headcount, a new technology, or consulting service, in order to justify budget, Briggs starts with discussing the risk involved. She says, "As an example, I went to the executive cyber board and told them we had two customer inquiries for us to have Soc 2 Type 2 completed. I told them we should do this because customers have started asking for this. We are now in the process of getting that accomplished and it is part of our strategy for the next 18 months."

NETSCOUT sells into Fortune 500 and 1000 companies, who want to ensure they are protecting their data. Briggs says, "I don't recall a recent customer in the last two years who hasn't asked for a security amendments or equivalent audit."

ASSESSING CURRENT TECHNOLOGY BEFORE MAKING NEW INVESTMENTS

Briggs believes in conducting an annual assessment of their current investments. She says, "You can go out and buy tools today and most likely some will overlap with what you already have, some will be best of breed, and some may fall short. In my annual assessment, if a product is coming up for renewal, I will evaluate if it should be replaced. I will evaluate if there are other tools out there that offer more, or it could mean getting rid of two to three of my current tools. It's important to understand what tools we have, the function and data we have from these tools, and if we can combine or get rid of certain tools. We have all heard from vendors that they have AI and ML. We need this, we need to see indicators of compromise earlier in the kill-chain. Tools need to be providing this to us. No one can afford to have a bad actor on their network for 100+ days."

LOOKING OUTSIDE OF SECURITY FOR TALENT

With a competitive hiring market, Briggs looks for potential team members in unique places. For example, an open security compliance role could be filled with someone who has a finance degree and is highly trainable and interested in security. She says, "I look for people in unique places and I try to bring two to three interns in every summer. For interns, they are given the opportunity to get real world experience and it also allows me to get exposure to people I may want to hire in the future. You don't have to just look at people in security, it's important to have the ability to train people with different backgrounds."