# PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

## TONY MEHOLIC
CISO, THE BANCORP BANK

**HEADQUARTERS:** Wilmington, DE

**EMPLOYEES:** 500+ Employees

**TOTAL ASSETS:** $4.3 Billion

"I always try to highlight the contributions of team members, as it is their work that makes the bank secure."

**- TONY MEHOLIC**

## CISO WHO SPECIALIZES IN BUILDING PROGRAMS

Like many CISOs, Tony Meholic, the CISO of The Bancorp Bank, moved to the information security industry from another career entirely. Backgrounds in military service, the intelligence industry and IT are common among CISOs, but Meholic might be one of the few CISOs to get his start in the hospital emergency room. Meholic shares, "I was studying for the advanced cardiac life support test and found flow charts for treatment modalities in the back of my prep book. I had always dabbled with programming, so I realized this too could be charted out in a program. To help in my study prep, I wrote a model that simulated cardiac arrest. When the emergency room residents saw it, they wanted to use it, too." Meholic aced the cardiac exam and, at the same time, found a new career path.

"In 2000, I joined First USA Bank as an application developer in their application security group. My job was application security and helping with secure coding, code reviews and training, so that I-banking, which was new at the time, was done securely," he explains.

Meholic steadily advanced at First USA Bank, taking on a managerial role leading application security for the entire organization, not just the information security team. When the bank was acquired by JPMorgan Chase, Meholic created the first team of ethical hackers. Meholic explains, "It was a hard sell to hire hackers at the time. It was considered an unorthodox approach, but I was able to bring in talented people who quickly proved their worth. We saved $360,000 that we would have spent on external

penetration testers, because we had our own hackers on the team."

From JP Morgan, Meholic made a jump that he says, "is not typical, and not always advised." He left the international banking giant, where budget was not an issue, for a regional bank. While the regional bank did not have a global reputation, it represented a step up in responsibility and title for Meholic. He says, "It was my first CISO role and an opportunity to create a security program from the ground up. It was also a chance to work more closely with C-level executives and get exposure with the Board of Directors."

## TAKING THE CISO REINS AT THE BANCORP BANK

After establishing the security program at the regional bank, Meholic joined The Bancorp Bank. He recalls, "I was attracted to the CISO role here because it provided an opportunity to build the security program from scratch again, but this time with an international component."

At The Bancorp, Meholic inherited a team of one. He says, "Now we have 8 people and a well-established security program. I am proud that we have recently mapped our program to the NIST framework. This is important because we are now able to show our full security program in an audit-friendly manner."

As he considers his career trajectory, Meholic realizes he is especially adept at building out new programs. He shares, "I helped develop the application security program at First USA, established the technical consulting and ethical hacking teams for JP Morgan Chase, and then the complete security program for The Bancorp."

## KEYS TO CREATING A COMPREHENSIVE SECURITY PROGRAM

Given his expertise in building out security programs, Meholic has specific advice for CISOs who are new to the role. He suggests starting with these three steps:

1. Understand Staffing Levels - "We have to look at the support system in place, whether that support comes from within the organization, or IT or business units, we need a team of people supporting security efforts."

2. Identify and Review Existing Policies - "It is important to understand current policies as they are written and applied. Do they meet requirements for privacy, security and compliance?"

3. Know the Data - "Data classification is key. We cannot expect security awareness from the staff if we have not classified the data. We need to identify confidential data, understand where it resides and build protection around it."

Once the basics of his security program are established, Meholic follows a few guiding principles to take his security program to an appropriate level.

- "Let the professionals do their job." - Like other CISOs, Meholic keeps his team motivated through education, training, mentorship and advancement. Importantly, he says, "I am a hands-off manager. I clearly communicate corporate and team goals. Our tasks are well-defined. I know my team has the skills to get the job done, so I give them the freedom to work in the manner that's best for them."

- "Choose the right technologies." - The market is flooded with new security technologies, and it can be hard to find the best solutions. He says, "I rely on my peers. Nothing beats an unsolicited review from a trusted colleague. I also rely on Gartner, although Proof of Concept is still the best way to determine if a solution will do the job for our company."

- "More tools do not equal better security." - Meholic reports The Bancorp runs 8-10 security tools. "It's not the number of tools that will make you secure, it's the way they are deployed in practice," Meholic explains. He prioritizes security solutions that can report on their own performance and measure return on investment.

Meholic works closely with other C-level executives at The Bancorp, and he meets with the Board of Directors on a regular basis. "Sometimes the Board wants a five-minute, high-level overview, and other times they have one hour's worth of questions. Usually interest is driven by bank initiatives or external news."

No matter the focus of the Board's inquiries, Meholic is careful to position security as a team effort. He comments, "I always try to highlight the contributions of team members, as it is their work that makes the bank secure."