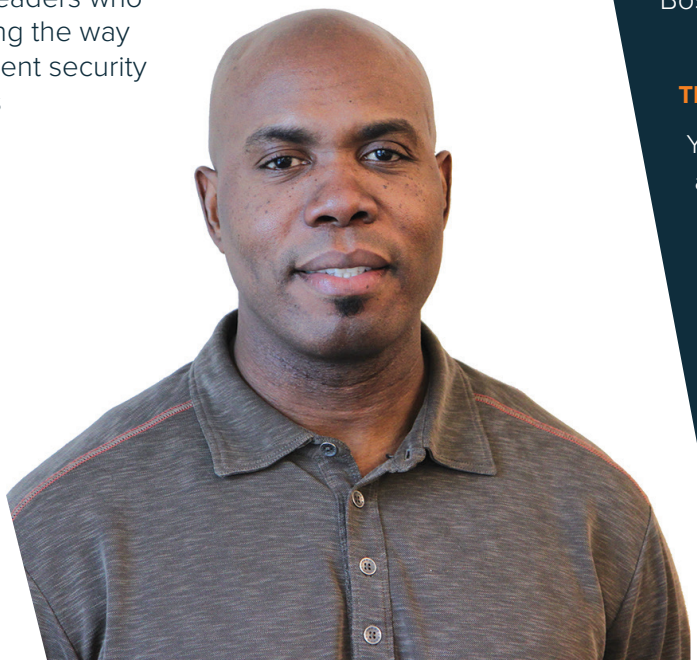
PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs



YALMORE GRANT

Head of Security
Boston Financial

THE START

Yalmore Grant's early career was in the data center at Boston Financial. He describes himself as a "real data center guy. I was about servers and hardware: the big physical stuff. But then, a light bulb went off. I realized that all the data in the data center, which was moving from one company to another, was inherently insecure. I quickly realized that securing that data was the future.

APPROACH

Coming from the data center, Yalmore admits that in the beginning he was interested in all the shiny new tools of security – the technology. But a conversation with a major client early on in his time as a security leader changed all of that. "Immediately after I was handed the reins of the security department, I received a call from a client. They were coming to Boston to do due diligence, and they wanted to talk about data security. I thought we would talk about proxy servers and firewalls. When we sat down together I quickly learned they had no intentions of discussing anything technical. All they cared about were our processes. What our clients care about is the processes, vision, and strategy. What will happen with their data when they entrust it to us?"

This was a major revelation for Yalmore and would shape his entire approach to running his security organization. "I had to think differently. I would no longer focus on technology, but on the business. I turned my focus to the management of the processes, policy, procedures, and governance."

He continues, "We had policies and processes in place, but they were not communicated well to the employees they impacted. Security is more successful when you have buy in from the people using the systems. When people are aware of security it is easier to implement policy and procedure, and it makes the entire company part of the security team. With the right knowledge, they are essentially another pair of eyes watching out for the safety of our critical data."

THE CRITICAL FIRST WIN

Increasing the company's security awareness required Yalmore to get outside his office and the IT department and make connections one business unit at a time. "I sat down with each of the SVPs of our different business units. I listened to them talk about their business processes and their work. What systems did they use most often? Which ones were most critical to their processes and what would be the impact if those systems fail."

"My first interaction was with a gentleman who runs a major organization within the company. He has a lot of responsibility, and relies on a number of critical systems and 25 servers to ensure the productivity of his team. My challenge was to deliver technical information to him about the security of these systems in a manner that he could relate to as a business mind. We talked about one system in particular that played a large role in the company's ability to reach its revenue goals. He knew if that system went down that it would seriously impact his team and the company. I showed him how the system rated on a Vulnerability Test I had performed. We talked about how a negative incident with the system could impact the end customer. From there he knew I was different. I wasn't asking him to buy a security technology; I was talking about making his team more efficient. We talked about how security awareness could improve the productivity of his team, and our end product."

After that conversation, Yalmore had his first department on board with security. That led to other organizations within the company embracing the approach as well.

COMFORTABLE IN THE BOARDROOM

Since taking over control of the security organization, Yalmore has had several opportunities to meet with the Board of Directors. He comes to these meetings from a position of strength because the Board is largely clued in to his security efforts before the meeting takes place – thanks to constant company-wide communication and education.

"My meetings with the Board are positive because we are not there to discuss fall out from a breach or a catastrophic security failure. In fact, we are not even talking about specific security efforts, because they are covered in company-wide meetings that occur several times a year. Instead we talk about our security posture and how it compares to the industry and to standards. We also talk about our customers and how our security programs can positively impact the services we are delivering to them."

"Security is a series of decisions. That is why it is about the people, more than the technology. Think about it, we are all awareness-oriented people. We make decisions based on awareness and security every day. Lock your car. Dress for the elements. Look both ways before you cross the street. So much of Information Security is about applying this same innate awareness to your business processes. Sure, technology is important as part of the framework, but the most important element is that everyone be aware."

- YALMORE GRANT

FUTURE DIRECTIONS

Yalmore points out that his security program, like all security programs, is constantly evolving and must always adapt to change. He does not get caught up in worries about future attacks, as he knows they are inevitable for every organization.

Instead he says, "Detection and response is just as important as the protection layer of security. We must have good incident response. We must act quickly to remediate issues when they do occur. This will minimize any discomfort we would feel from a malicious attack. That is how we can help drive business forward, and so that is what I focus on when I talk to the Board and the company about our security programs."