PROFILES IN *Confidence*

# FREDERICK WEBSTER

## INFORMATION SECURITY OFFICER
BLUE CROSS & BLUE SHIELD OF RHODE ISLAND

**HEADQUARTERS:** Providence, RI

**EMPLOYEES:** 760

**REVENUE:** $1.7 Billion

Fred Webster says the first few years of his career began at the ground level, working on help desk support tickets, fixing desktops, and troubleshooting laptops. He then moved into server administration, application support, database administration, and other highly technical areas. It was in this work that he gained exposure to project management, a field he felt compelled to explore because he was able to apply a consistent methodology across a variety of problems. His work as a project manager at a managed service provider provided a gateway into information security. He began learning the basic principles of information security before taking on his first official security role as Vulnerability Management Program Manager at CVS. He ran the vulnerability management program and applied project management principles to information security domains. His job expanded to include configuration assessments and positioned him in a managerial role taking over large components of the security operations department.

After leaving CVS, Fred worked at NTT delivering their managed security services to clients in North America. As a senior leader, Fred was a key management contributor responsible for the successful delivery of all managed security services.  After spending over four years in this role, Fred moved over to Blue Cross & Blue Shield of Rhode Island (BCBSRI) as Director of Information Assurance, Business Continuity where he was exposed to the policy, risk and governance oversight, something he feels was missing in his previous experience. He was then promoted to the Information Security Officer (ISO), reporting into the Chief Risk Officer.

## INFORMATION ASSURANCE AND SECURITY OPERATIONS

As ISO, Fred has two main programs he oversees – information assurance and security operations. From an information assurance perspective, Fred leads third-party risk management, security awareness and training, information security risk and governance, cyber threat and security incidents, and policies and standards.

Managing third party risk management includes assessing vendors and monitoring vendor risk. Fred explains, “We want to make sure our third parties are following best practices and they meet our contractual requirements. We are able to calculate a risk score for all vendors that receive sensitive data. We also use a third-party vendor that monitors the infrastructure and footprints of our vendors for potential risks and security threats.”

BCBSRI’s security awareness program comprises training on an on-going basis, whether it is onboarding a new employee or ensuring associates with privileged access understand their responsibility to keep corporate data secure. Fred says they engage with employees throughout the year, with a heavy focus during cybersecurity awareness month. They collaborate with the compliance team during compliance week, and regularly with the human resources department to ensure they work on various projects with shared goals.

> “I want to enable each team member’s strengths while helping them develop their weaknesses. My approach, and I think this mirrors the overall BCBSRI approach, is we trust that our associates are making the right choices and doing right by the organization.”

To ensure the security program engages in shifting left, Fred and his team have oversight into the RFP or RFI processes as they relate to information security. He explains, “In an attempt to shift left, we want to be at ground level so we can inject security requirements but also help the business assess vendors that are being selected. We want to make sure the business makes informed decisions, and we help them do that by identifying risk within vendors.”

Fred and his team manage security risk and governance in accordance with all policies and standards, providing advice to leadership on risk levels and acceptable thresholds. Also, the cyber threat and security incident process provides external threat intelligence, countermeasures within their environment and management of the third-party SOC that receives all logs and triages alerts. This team investigates any security incidents reported internally. Lastly, policies and standards related to information security are regularly updated and drafted by Fred and his team, where they work closely with the business to ensure goals are met and security is maintained.

Security operations includes managing all security tools and platforms from multi-factor authentication, vulnerability scanning tools, antivirus, or anything that has a security agent. They are responsible for making sure those agents are doing their intended jobs and running smoothly.

## FOCUS ON THIRD PARTY RISK, IDENTITY, AND RETENTION

Some areas of focus for Fred and his team include third-party risk, an area most security programs are currently concentrating on due to heightened and ongoing risk posed by vendors outside of an organization. Fred says, “We have lots of confidence in the core components of the program but every time there is a third-party breach or security incident, I look back and we might have given them a good score so we try to understand what other components we can add. This will help show us indicators of increasing risk or potential risks that we might not be seeing today.”

Identity and access management is an area Fred and his team plan to continue to focus on. He explains, “You’re not talking about servers and firewalls anymore, you’re talking about someone’s identity and the privileges that that identity has. So identity and access management is an area where there’s an opportunity for us to provide more governance and more oversight.”

The ability to retain and grow their team is another top priority for Fred. He comments, “We did well retaining people over the last two years. It comes down to our culture and the environment we have cultivated. But there is always more work to do, and I want to make sure our staff is fulfilled, and they are doing the work they want to do.”

## ASSESSING RISK

Fred explains, “We communicate risk to executives through our enterprise risk management program. Cyber has been the top risk of organization for last three years. As part of that risk program, we assess the various components of cyber risk on an annual basis. Our goal is to always improve, and we continue to tweak that process. For example, we might go back through our scoring techniques to really highlight the underlying risks and map them back to what risk means to the organization.”

## LEADING WITH TRUST & EVANGELIZING SECURITY

Fred says his approach to leading a team is based on being a good coach and providing support as needed. He says, “I want to enable each team member’s strengths while helping them develop their weaknesses. My approach, and I think this mirrors the overall BCBSRI approach, is we trust that our associates are making the right choices and doing right by the organization. That’s a key component to my leadership style. My primary job is to support them while I keep an eye on the business results in driving the business outcomes that we want. I am fortunate to have a strong team so it’s really just guiding the ship that is already heading in the right direction.”

Fred adjusts his approach when he is speaking with executives outside of his department. He says he focuses on being an evangelizer for information security, discussing it across the business and making sure everyone understands the value. He shares, “It’s important to not only communicate in terms the business understands, but in terms they care about. Some groups might not care as much about cost, but they care a lot about reputational impact, so understanding the audience and mapping back to the business conversation is important.”