CHIEF RISK OFFICER
BLUE CROSS & BLUE SHIELD
OF RHODE ISLAND

JON FREDRICKSON

HEADQUARTERS: Providence, Rhode Island

EMPLOYEES: 760

REVENUE: $1.7 Billion

When Jon Fredrickson was a child, he was fixated on exploring the limits of computers as soon as he had a computer with a modem. His high school was part of the Cisco Networking Academy, providing students the opportunity to take classes that counted towards achieving the Cisco Certified Network Associate (CCNA) certification. Because he participated in that program, he was hired as an intern at American Power Conversion upon graduation.

He explains, "I began my internship working the help desk, answering the support line, and helping with similar duties. I maintained this internship through college because I went to University of Rhode Island, a short walk from American Power Conversion. I was able to come and go as I needed to with classes. Halfway through my junior year, a position opened up on the networking team. That started my information security career. Back then people weren't cybersecurity analysts or engineers, they were network engineers. So that's where I received exposure to things like firewalls and web proxies."

After working in security leadership roles at CVS Health and Southcoast Health, Fredrickson moved to Blue Cross & Blue Shield of Rhode Island (BCBSRI). With two CISO roles under his belt, he recently transitioned to Chief Risk Officer (CRO).

THE BENEFITS OF RISK + SECURITY RESPONSIBILITIES

When Fredrickson first started at BCBSRI as Information Security Officer (ISO), he oversaw the information assurance program, comprised of a team responsible for governance, risk and compliance, some incident response, and threat intelligence with limited technical responsibilities. Shortly after, he added the title of HIPAA Privacy Officer because of his extensive experience working in healthcare. Then, security operations was brought in under him, along with enterprise risk management and most recently business continuity. He has since transitioned from CISO to CRO, now responsible for the entire risk portfolio. Today, his programs include enterprise risk management, business continuity, information assurance, security operations, and privacy.

While adding the responsibility of privacy poses unique challenges, Fredrickson welcomed the opportunity to strengthen his knowledge in that area. He explains, "HIPAA guides a lot of our privacy program. The privacy rule is complex and fact specific, which can be challenging at times. There are a lot of nuances in the HIPAA privacy rule and sometimes I need help. I report to the General Counsel, so I have a team of lawyers, not at my disposal, but who I can quickly interface with for some of those tougher HIPAA legal questions. It is definitely a challenging area, but there are always opportunities to learn."

Fredrickson hopes more security leaders assume extended risk roles in the future. He comments, "You look at all of the more recent attacks and the old school, CIA triad: confidentiality, integrity, and availability. With the way ransomware's going with extortion, it's really all about confidentiality and availability right now. And I think that if you have that higher lens or report through something that's not just IT then you'd hopefully have a better view of the organization and the impacts if a cyber event were to affect operational capacity."

The enterprise risk management department is comprised of not only cyber or IT risk, but it also extends to the entire organization. The team manages any risks that have the potential to impact the strategy, operations, finances or compliance of the organization. Fredrickson explains, "Cybersecurity is one of a myriad of risks that we monitor, and we provide the business with a framework and report all the way up to the board on what our top risks are, how we're managing them, and what our inherent vs. residual risk portfolio is. So it's not just cyber-focused by any means."

BUILDING OUT PROGRAMS AND SUPPORTING CLOUD TRANSITION

For the enterprise risk management program, Fredrickson says the next twelve months include a build out capacity for operational risk management. He says, "Today at the enterprise risk management level, you're looking at things that have not happened yet that could affect our ability to execute on our strategy. Folks will come to me and say, hey, I've got this project that's going awry, and I need help with risk management. And I respond, well, have these things already happened? Because then it's not managing a risk, it's managing an issue. So I think that the organization is now needing an operational risk management program and we're going to help do that in the next twelve months."

On the privacy side, the program is moving at an incredibly fast pace. With states beginning to adopt their own privacy laws, it is always a challenge to keep up. Fredrickson states, "Our business is moving quite quickly with digital transformation, an omni-channel experience for our members. So a lot of that is around member privacy. At the end of the day, the member owns the data, we don't own the data and we need to make sure that we stay one step ahead of that, but also enable the business with member privacy in mind."

Both the information assurance and security operations programs are undergoing a fast push to the cloud, so Fredrickson and his team are working diligently to establish the necessary guard rails to take advantage of the speed the cloud offers. They also need to ensure they keep the organization as secure as transparently possible, with business continuity being a large part of that, especially as they continue to rely on third party vendors.

FOCUSING ON THE BUSINESS

"One of my security leaders earlier in my career, had a picture frame in his office and it said something like "it's not your job to say no, it's your job to say yes, but here's how," and I've really driven my team to follow that mantra. I think that's helped us with the business. You are a partner and you're here to enable the business to do what they want to do, but we have a responsibility to do it safely and with member privacy in mind. And reminding the team to consistently do that, has driven us to have successful relationships with the business," explains Fredrickson.

For security leaders looking to build programs, Fredrickson says, "I would start with, what does my company do? What is their mission and purpose, what are their current priorities? And then make sure the framework that you've adopted makes sense for the organization, both culturally and strategically. We've adopted the NIST Cybersecurity Framework. I think it's the right size and it maps well and easily into HIPAA. But if you're a government contractor, you need to align with their regulations. So make sure it's the right fit. And then I would do a third-party maturity assessment up against that framework. Some boards prefer an independent opinion. Folks can get more funding that way and then see where the holes are. For example, you may think you are strong at protecting the organization, but your "Identify" foundation in NIST CSF might be lacking. You then need to either make people or technology investments to be more robust in that area. I would work backwards again from the business, adopt a framework, and see where the gaps are."

PRESENTING TO EXECUTIVES

For Fredrickson, relevancy is key when presenting to business executives. He says business leaders are not typically interested in hyper-specific technical metrics; security leaders must understand their audience, what their goals are, and in what capacity the security program applies to them.

Topics at board meetings typically include questions around any newsworthy cybersecurity events, so Fredrickson always includes a slide that discusses the global threat landscape. This keeps board members up to date on any threats the organization could potentially face.

Fredrickson says, "Another question from board members which I really appreciate is if I have enough resources to achieve my mission. And that's a nice question to receive, I've had a lot of educated and pointed questions about ransomware and business resilience. Even to the point where we conducted a dedicated cybersecurity session for particular board members that wanted to go a bit deeper. It was a productive candid conversation with a subset of the board that I think was pretty successful."