CRIS EWELL

Chief Security and Privacy Officer
NRC Health

HEADQUARTERS: Lincoln, NE

EMPLOYEES: 500+

REVENUE: $133 Million

Cris Ewell had an eclectic background leading up to his career in cybersecurity. He dropped out of college and bought a restaurant, where he learned key customer service skills, before deciding to become a paramedic. He then became a director of paramedic service, responsible for protecting patient data and addressing access control, which spurred him to go back to school to finish his undergraduate degree in information technology. After achieving his degree, Cris continued his education and completed his graduate and Ph.D. degrees in information technology and systems with a concentration in information security.

Cris has over 25 years of experience in information security and spent over 19 years in CISO or equivalent roles. He held CISO positions at PEMCO Corporation, Seattle Children's Hospital, and University of Washington Medicine before joining NRC Health as their Chief Security and Privacy Officer. He has worked as an Adjunct Professor specializing in risk management and operational controls courses throughout his career. Currently, he teaches two to three classes per year and sits as an advisor to graduate students at City University of Seattle.

He says, "I love being a CISO. I love leading organizations and seeing how I can help them navigate the field of risk and threats. But I also know that I need to give back to the community and I need to train the people who will take over my position someday. It's great to see students learn. It's really exciting to see people I've had a small part in educating over the last 15 years, prosper and blossom in their positions."

RISK MANAGEMENT

When evaluating security programs, Cris always starts with understanding the risks and threats faced by the organization, something that should always be grounded in an understanding of how the adversary thinks. He explains, "It is important to know the difference between opportunistic attacks versus targeted attacks, and all of the controls in place for the organization, from your security operations to your development operations, to the systems teams. Then put those all things together with the current climate and the current resources you have available."

Cris believes in order for security leadership to appropriately address threats, they must have strong knowledge around risk management and quantitative risk analysis. He says, "It is important for CISOs to really understand quantitative risk analysis, so an actual risk and financial number on the level of risk for the organization. And that's the language of business that really resonates with CFOs and other executives. It also resonates with cyber liability insurance companies that may be taking a look at your organization's real financial risk. It's about understanding the whole insurance spectrum, understanding the real difference between qualitative and quantitative, you can't just put numbers on colors and call it quantitative."

Another focus area for reducing risk is situational awareness in relation to threat intelligence and understanding the adversary. Having a level of threat awareness that goes beyond what is happening locally, ensures CISOs know what is going on in the rest of the world. Cris believes situational awareness is a minimum requirement for CISOs to gain holistic risk insight and ensure they are proactively prepared.

He continues, "I spent 10 years researching and understanding risk management and it really has helped me deliver something that our business leaders and boards can understand. I think that's still a failing in the information security education department, in getting CISOs to understand everything about proactive risk management, especially with data centers, third parties, and risk assessments. How do you understand all of those intricacies to be able to come up with that risk management report?"

DATA VISUALIZATION

Cris says he is passionate about data visualization, especially when it comes to presenting to boards and executive audiences. In meetings, he provides a mixture of strategy documents indicating the overall strategy, key threat areas, and projects they are working on to mitigate risk and threats. He also includes visuals for an executive dashboard, often leveraging red, yellow and green indicators.

He explains, "I look at both the overall risk of the organization, and a view of what's the information security overall program risk. When I look at the program risk, it really is answering the question, is the organization resilient enough to be able to respond to the current threats and risks? It looks at all the different security domains and being able to say that you are prepared. It's measuring your ability and your maturity to information security controls. Then I look at attack vectors and our organizational asset risks. I always throw in compliance if you're an organization that has compliance, healthcare definitely is. I also include some very high-level performance measures. Those things make up my executive-level dashboard that I typically give to the board of directors so they understand the different components. Hopefully that will spur conversations about the information security program and risk from there."

CHALLENGES

For Cris, the most pressing challenges CISOs currently face are around data, legacy systems, threats, competing priorities, and human error.

Data: "The challenge comes in knowing all the areas that data is kept and which controls are in place. Most of us do really well with primary, secondary, and maybe even tertiary data sets. If you've ever done research and been part of academic medicine, academic institutions, or research institutions, there ends up being many copies of data sets and they can be difficult to identify. Whether it is limited datasets, healthcare-related, restricted or public data, or if you have PII for a financial institution, understanding where all that data is and understanding what controls are in place is essential."

Legacy systems: "A fact of being a CISO in 2022 is you have to have a plan to support the legacy systems still required by the business. These systems may not have the latest software version, latest patches, or the latest code development. These systems may not be at that highest level across the entire spectrum of things you have to protect, but you still need to provide information security controls that help to reduce the risk of unauthorized access or use."

Threats: "There is a rapidly expanding spectrum of threats to our systems networks and data assets. It is enormous, we have zero days that come out, we have code or exploits that are stolen or purchased that are now utilized against organizations. As CISOs, we need to have security practices that are robust enough to help mitigate these threats and understand – how do I continue to keep ahead of the threats?"

Competing priorities: "You can't fix a hundred percent of all your risk, it's not possible. We need to understand all the threats, vulnerabilities, and risks to the assets and data in an organization. The question then becomes how we prioritize the remediation with the limitation of the resources that we have underneath the control of the organization."

Human error: "How do we help our users understand the real threat? How do we help the user understand the world that we live in and, for example, where we have to question every single email that we receive or putting a pause in our actions before we post a change in a system. Simple actions by our users can decrease the risk to the organization - such as understanding their responsibility in protecting the data, not clicking on that link, not installing software, or not accessing our data without a VPN. Education and awareness is a very important element of our security controls and should not be underestimated in its importance to the overall program."

DIVERSITY

"Having a diverse team that has different life experiences is critical to your success. I don't want a team that just says 'yes', I want them to challenge my decisions when appropriate. If you have an incident or critical incident that is time critical, it might not be the time to challenge. It is the right time when you're talking about the right technology to use or strategies on how to implement zero trust. That's where having those different experiences is so important for the team and something that I have promoted over the last fifteen years. Where I am today, I've hired almost my entire team, and we have a very diverse team. There's just so much to learn at all levels from everyone's perspective. I believe that the diversity and ability to work together is a core requirement for what makes a really great team."