CHRIS HOLDEN

CISO
CRUM & FORSTER

HEADQUARTERS: Morristown, New Jersey

EMPLOYEES: 3,000+

REVENUE: $19.8 Billion (2020)

Chris Holden was interested in cybersecurity from an early age and decided to attain his Bachelor of Science degree in Cybersecurity and Information Assurance during college. After graduating, he applied for an internship with HP's Cyber Forensics department and was hired immediately, later finding out he was the only person who applied with a degree in Cybersecurity. After holding various cybersecurity jobs, Holden began working at Crum & Forster, a leading national property, casualty and accident & health insurer with a large, diversified specialty platform.

Beginning as Manager of Cyber and Information Security at Crum & Forster, Holden moved to Associate Director, before becoming the Chief Information Security Officer in 2020. Transitioning into a leadership role meant stronger alignment with the business. He explains, "The biggest change is the exposure to the business and how to efficiently and effectively implement security with the lowest impact possible. When you're early in your career working as a security engineer, your goal is to implement the most robust security control first, taking care to ensure it doesn't inhibit the business from being operationally effective."

REMOTE WORKFORCES AND CLOUD MIGRATION

Moving workloads to the cloud is a top strategic priority for Holden, with remote work exposing many new considerations for security. The organization already had significant initiatives to move to the cloud, yet when virtual became the new normal in 2020, Holden says it sped up the company's timeline. He comments, "We saw it was much easier to realize the return on investment of moving to the cloud while being remote. It provided us a lot more flexibility, as well as a better experience for our employees. We were fortunate that we had pre-existing infrastructure to securely support remote employees."

Another initiative Holden and his team are working on is the planning around shared office space. Crum & Forster is in a unique position where it owns several of its offices around the country, and because the employee base, in large part, works remotely, it has opened some of that floor space to other businesses in the local areas. With its strong cybersecurity guidelines in place, Holden says he and his team are mindful of all the considerations and, importantly, are ready for having nonemployees working within the company's walls for the first time. He says, "How do we segregate or prevent access to sensitive data, whether that's physical files and the file cabinets that we have around our office, or more strictly enforcing clean desk policies for some of our users, but also who can connect to the network and how we're facilitating those connections as well. I think those are our biggest and most interesting initiatives right now."

One challenge Holden says he faces is around designing and implementing many newer controls in ways that are feasible and adoptable. Holden notes at the forefront of all the company's and his team's initiatives is to build a culture of security, enabling Crum & Forster's entire workforce to conduct business in a highly secure manner. Since historically that was done when employees were all working in an actual office, the tools are now changing, including a portion of the company's technology, to bring colleagues into the new era of cloud and remote work. Employees are now working differently and interacting with different applications and systems. He knows his team is up to the task of getting a significant portion of the company's 3,000-plus employees used to securely working remotely.

BUILDING A STRONG CULTURE

For Holden, culture building starts with hiring. His main focus when hiring is looking for individuals who are passionate about cybersecurity, because they will end up being the ambassadors of the security program. He says, "They are the ones that are going to be designing the controls and implementing the change. They are the ones who are going to be working with our employees and our business groups when issues arise. If they are not excited about it, our stakeholders are not going to be excited about it either. That's the key driver there."

He continues, "The other thing that we have done is more frequent employee outreach. We initially started this a couple of years back, during Cybersecurity Awareness Month in October. Outside of our standard training, we often have speakers come who are focused on cybersecurity. We have had a couple of retired and current FBI agents talk about the threat landscape, not only from a work perspective, but also in their personal lives. We've also done more interactive training and "Ask a Cyber Expert" program, both of which have been huge successes."

This type of outreach has been received well by the workforce, and something the company is coordinating into a longer-term approach. Holden says they are not just doing this during the October Cybersecurity Awareness Month, but rather making regular outreach efforts and interacting with various business groups. This is done both formally and informally to provide training and feedback throughout the year on a consistent basis.

MOVING TO FINANCIAL-BASED RISK REPORTING

To track the progress of the security program, the first thing Holden did was align controls to an industry-recognized cybersecurity framework. This is key for measuring maturity and identifying gaps, to continually measure growth and make a strong impact on the organization. His latest efforts have moved to quantifying risks, which Holden says can be a cumbersome and incredibly time-consuming task. He comments that at the end of the day, "You often see it gets to a point of analysis paralysis, where you are putting a large amount of time into the analysis and defeating the purpose of identifying what the real threats and risks are."

Holden says he is seeing a significant shift throughout the industry of moving to financial-based risk reporting, which speaks to executives in business terms. He explains, "I've shifted the approach; I'm looking for two key things in all of my metrics and KPIs. One is the dollar value, and what we have found is that it is not always easy. The second most important thing that I put into perspective though, is time. Those are the two key things that the business can relate to. Time and money. From a time perspective, I am not necessarily concerned about the thousand vulnerabilities that have come up on my latest scan report, but how many of those vulnerabilities have I missed the SLA on remediating? Those are very tangible to illustrate how effective we are as a program."

IDENTITY: KEEPING IT SIMPLE

Holden approaches identity with a core focus on keeping it simple. He reveals, "There's a lot of potential for an identity and access management program to be a very bad experience for both your employees and your clients. Keep it as simple as possible. This will help with future provisioning, user access reviews and audits and a cleaner experience for your stakeholders. It is also critical when implementing to keep in mind who your stakeholders are. There have been a lot of great developments recently in providing flexibility with how they choose to prove their identity and access your applications and systems. Supporting a few different options will ultimately provide a better user experience as well as increased security if your users don't see authentication as a hassle."