PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

ANDREW BJERKEN
GLOBAL CISO AND CPO, CATALINA

HEADQUARTERS: St. Petersburg, Florida

EMPLOYEES: 1,300+

ANNUAL REVENUE: $640 Million

"Be yourself, be humble, be approachable, and be credible in your job. If you can be those things, you're off to a good start. When you don't know the answer, don't try to bluff your way through it, because no one expects you to know everything. Be confident in what you do know."

- ANDREW BJERKEN

Currently the Global CISO and CPO of Catalina, a big data company focusing on shopper history, Andrew Bjerken possess a strikingly unique background. Starting his career in the Air Force as an electronic warfare officer and then transitioning to the red team, Bjerken tested physical and cyber security controls across a multitude of bases and systems. Along with his team, they spent their time trying to break into networks and facilities to exfiltrate data. They would then brief commanders on what kind of unclassified/classified information they were able to either exfiltrate or piece together. This work exemplified Bjerken's first plays into information security and sparked his interest in replicating his Air Force work in his transition to the corporate world.

HONEST, STRATEGIC CONVERSATIONS WITH SENIOR LEADERSHIP

Holding previous CISO and Privacy roles in a variety of verticals strongly prepared Bjerken for making an impact and embedding strategic alignment at Catalina. Bjerken reports into the Chief Legal Officer who reports directly to the CEO, enabling him access and a strong working relationship with senior leadership and the board. He comments, "You have to be cognizant of your audience and what's important to them. You must make sure you deliver on your promises and you need to be careful that you don't falter early on, you can't misspeak or oversell, it's going to leave a lasting impact. You must establish your expertise early on and establish a trusted partner relationship."

Honesty ranks high on Bjerken's approach to communication with senior leadership. He is consistently open and honest about where challenges exist within his information security and privacy program and what his needs are to fulfill business requirements. Most importantly, he clearly articulates his strategic roadmap to show where they are and where they need to be so allocated budget does not get wasted.

When providing advice to other CISOs preparing for their board presentations, Bjerken explains, "Talk to other folks who have been in front of the board, so you know the audience and what's important to them. Be yourself, be humble, be approachable, and be credible in your job. If you can be those things, you're off to a good start. When you don't know the answer, don't try to bluff your way through it, because no one expects you to know everything. Be confident in what you do know."

REPORTING ON RISK METRICS

Bjerken does not subscribe to in-depth technical details and statistics when reporting to senior leadership on metrics. He comments, "For me, the most important metric is the risk profile. What is the risk of the organization and how are we tracking it? I show where our current level of risk is, broken down into five different categories of risk, then I show key things we need to do in terms of reducing risk. This allows for informed decisions to be made based on risk appetite. When married up to my overall strategic plan with project goals, one can easily see where the weight of my team's efforts are focused and in which risk category we are trying to affect. If they see a discrepancy later or wish to reprioritize based on changes to business goals, then we can adjust the roadmap."

He continues, "The board and senior executives feel more comfortable when I have a holistic plan in place versus saying something off-hand like I need a tool 'X'. When they can see why you need a SIEM, how it fits into the strategic plan, how it reduces risk, and what the anticipated ROI is, they have a greater sense of comfort in terms of expending those dollars. The ROI is often explained in laymen terms such as the tool 'X' gives me greater fidelity, which means the team can identify a threat quicker and we can mitigate them faster. The downtime for the business is going to be less as a result. Knowing our revenue generating lines of business and the associated business impact assessments allows me to give an educated answer associated with dollars, if our system goes down, that could be '$X' Amount an hour depending on the system but tool 'X' reduced that estimated downtime. Always driving the discussion back to the business requirements and goals. Bottomline, making that correlation so they can see the risk in true dollars has really helped me."

COMMUNICATION, STRATEGY, AND PASSION

According to Bjerken, key traits of success for CISOs include effective communication, a strategic approach, and being passionate.

Communication. "You have to translate between technical and non-technical. You've got to take the non-technical and tie it into business requirements. Today's CISO must speak business language more so than technical language, in many cases. Business language is PNL (Profit and Loss) and Risk. What is the risk to operations, to revenue, how much is this going to cost, what is the ROI, all of those things. We can't just talk threat, threat, threat."

Strategy. "We must be strategic in thinking, but we must be able to tactically execute on our ideas. I'm a strategic thinker in terms of having a roadmap and vision that enables the business, but when it comes to doing the work, I'm big on having goals that focus on the tactical tasks to ensure we accomplish the strategic objective. Diversity is key in any capability, as a CISO, I want to surround myself with a diverse group of people that are smart and take pride in their work. However, that diversity won't help the company if we're not willing to listen to them. That's how we grow. You have to listen to all voices. I don't like the doom and gloom messages that I hear sometimes, everyone is aware of the doom but a CISOs job is to identify the potential doom and determine the best courses of action to avoid or mitigate the potential negative impacts. CISOs must be willing to make the decision. Regardless of how much data you have, if you don't move forward and choose a direction, you will fail."

Passion. "One of the things that makes a good CISO is truly caring about the company they're with and really wanting to make a difference. I love my job, and I love what I do, therefore I want my team to feel the same way because when they do, they're much happier which means they work harder and inevitably they want to make a difference. When things go wrong and they have to stay late, they're not doing it necessarily because they have to, but because they want to; they feel a sense of responsibility in the success of security and privacy. If you can encourage and foster that type of environment in your organization chances are you'll have a high functioning team which increases your chances of success in your role. At the end of the day, without your team being successful, a CISO won't be successful."

GDPR FOCUS

"Shopper info from retailers are sent to us and we provide coupons back using real time analytics. We have lots of data from around the global to include the EU. As both the Global CISO and CPO, most of my time lately has been consumed with GDPR and ensuring security and privacy are aligned and of course that we're compliant by May 25th, 2018. We were building it from the ground up and are pleased with the final program. For any company or organization, the fines associated with GDPR are large enough to make your board and CEO, sit up and pay attention and want to know what's going on."