PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MARK FERGUSON
FORMER CISO, HONEYWELL

HEADQUARTERS: Charlotte, North Carolina

EMPLOYEES: 130,000+

ANNUAL REVENUE: $40 Billion

Formerly the CISO of Honeywell, Mark Ferguson has worked in a number of security roles over his 15+ year career in security. In 2004 he worked at an organization specializing in safety and control systems that was acquired by Honeywell. After obtaining his CISSP certification, he took on many security roles during his time at Honeywell, starting as an Infrastructure and Security Architect, working his way up to eventually become the CISO. He explains, “It was an interesting journey for me to become a CISO. In 2008, due to the economic downturn companies were doing less external recruitment and more internal hiring. So, I was able to benefit and the opportunities for internal candidates were there. I eventually moved out of my role as a Security Architect into the corporate global security team within one to two years. I had the opportunity to interface with the CIOs, the business CSOs, and business leadership. That helped me gain reputation and credibility, both externally within the business, but also internally within the security function.”

ALIGNMENT & TRANSFORMATION

Throughout his career, Ferguson has instilled security as a trusted advisor to the business, making sure he was constantly advising them on risk and continually ensuring he understood what the business was trying to accomplish. One challenge Ferguson and many of his CISO peers face is keeping pace with rapidly growing business transformations.

Ferguson says today businesses are transforming in many ways including digitization and moving to the cloud, something that enables the business to grow, yet security departments aren’t always equipped to keep up. He explains, “Security teams just weren’t ready for the cloud. They lacked either the capabilities or knowledge to keep up and you almost had a perfect storm. Security wasn’t capable of delivering on the business needs, and cloud took off leaving security teams scrambling to keep up. I discovered when I went through this myself and we thought we had a plan for cloud, but when you actually dig into it, you realize cloud is different. And how you provision, secure, and manage are completely different. I think a lot of security toolsets are sold as being cloud-enabled when really, they aren’t. That was one of the things we discovered. You find out they can operate in the cloud, but they’re not cloud aware. And that’s a big difference. These types of things keep the security teams from being able to move at the speed that the business needs to operate.”

SECURITY STRATEGY STARTING WITH THE BASICS

Ferguson says doing the basics and doing them well are always his top priority. He explains that if you do the basics such as patching, configuration management and managing identities, then you rapidly shrink the attack surface, and if companies do things such as these, they are much better positioned to avoid a significant cyber event.

He shares that any security plan must be founded on a strong and robust strategy for identity and data protection. He says, “You’ve got to be able to manage and secure your identities, and everything that goes around that including access and authorizations. Securing your identities is crucial. And then having a strong plan to protect your data, which I feel is a place we're failing in, securing data."

Agile technology and services are also important for Ferguson's security program, with a heavy focus on automation, scalability, and being frictionless. For him it means having technologies that are adaptable and if he cannot automate, then he does not invest in them. The same goes for his internal processes or services, which must be frictionless otherwise the business will just work around security.

Ferguson says culture and a strong awareness program help drive good cyber hygiene. He comments, "We did things like launching a global security ambassador program. Rather than having the corporate security team telling people how to practice good cyber behaviors, we brought employees on board and had them go and evangelize on our behalf. We found people that had an interest in cyber and an interest in security and wanted to get a little break from their normal day job. We equipped them with the knowledge and the messages to evangelize on behalf of security. It sounds better if it comes from somebody in the business rather than a corporate security person telling you. I'm a big believer that people are the weakest link in the chain, and why they're so often the target of the bad guys, so you have to try and equip them as much as possible with the knowledge to make the right choices."

RISK-BASED, THREE-TIERED APPROACH TO BOARD METRICS

When preparing and presenting to the board, Ferguson believes it comes down to knowing the personalities and finding a strategic balance of what to present. He created a three-tiered approach to metrics, with operational metrics or things that he works on every day at the bottom, then a tactical layer which is what he presents to functional leadership. Then there is the strategic layer at the top which is presented to senior leadership and the board.

For Ferguson, discussions with leadership teams must be risk-based and translated in meaningful terms. He says, "When we say risk, I mean risk to the business, not a cyber risk because that's meaningless to them. They want to understand what the business impact of that attack is, whether it's reputational, financial, or some other risk to the business that might impact operations."

He takes a stoplight approach with green, red, or amber colors to show trends and the impact of those on the business. Ferguson prefers having a qualitative dialog with leadership, backed up by solid metrics. He believes in making sure the board understands the impact of each risk and the plan to solve it in an impactful, business-focused manner.

Ferguson said he was often asked by the senior leadership team about how they benchmark. He comments, "You always get asked, "well, how does it compare?" It's difficult to baseline data. Most companies don't really share, but we're always ready with an answer on how we're positioned against the industry or competitors. We've participated in benchmarking surveys but there's so much context in the data and until you've understood that context, it can be a little meaningless. For example, we took part in one survey and it looked like we were spending a fraction of what some of the others were spending on awareness. But we just didn't know who we were up against, their risk appetite, or awareness strategy. It helps if you've got the full context to better articulate your position."

INDUSTRY TRENDS - HYBRID MODEL AND CRISIS MANAGEMENT

Ferguson says the security industry will eventually end up in a hybrid model, with humans and machine learning working together. He explains, "The humans will be there to do what they do best - add context to the answers machines are producing. I see AI and machine learning having so much potential in the security space. I don't think people are necessarily looking at it holistically, but all this is going to come together at one point. And if you look at the use cases from data protection to threat detection to email security to automating risk assessments, everything is going to be powered by AI, and then in this hybrid model, value and context will be added by the human element to drive better decisions."

Another important trend is crisis management, something that still concerns Ferguson. He says, "One thing that concerns me is whether organizations are really ready to handle a major breach. The ones that handle breaches well have thought about it and prepared. They've got a plan, they've tested it, but the ones that go badly, they haven't planned for it. Cyber teams are going to have to get smarter at crisis management, because when something bad comes up, the business will ultimately look to them for answers. You must also be engaged with your HR, legal and comms teams, and understand the decision-making process during a cyber event. And when the media calls, are you ready with a response, do you know who to call, who is going to own the message, and test for basic things like what happens if your email system gets attacked. How are you going to contact people? Do you know their phone numbers? Details and responses to these kind of questions should be in a playbook. I don't think a lot of teams have really worked through that."